Google Cloud

Cross-Cloud Network Hybrid Workforce Solution Brief

Cloud Native Secure Access Services Edge (SASE)

Secure user access to applications

Today's workforce requires the flexibility to connect securely to applications from any location on any device. Whether an employee is connecting over a trusted network from a company managed location or they are connecting over an unsecured public network, user connectivity must be secured to prevent incidents that exploit user access as an attack vector and, in particular, user access over untrusted networks or unmanaged devices as an expansion of the attack surface. The potential attack surface in user to application communications is further expanded by the need to connect to public applications that are mostly reachable over an untrusted network such as the internet.

To protect these communications, the security industry is continuously developing functionality to improve authentication and authorization of users, guarantee connection privacy, prevent data leaks, prevent malware propagation, and many other security functions that are particularly relevant to user communications over untrusted networks. The security stacks that deliver these important functions are offered as security service edge (SSE) managed services. SSE has been defined as part of the secure access service edge (SASE) solution framework.

The SASE framework proposes a combination of connectivity and security. Connectivity controls are required to ensure that user traffic is indeed steered through the SSE security stacks. SASE providers therefore offer last-mile connectivity solutions like software-defined wide area networks (SD-WAN) and build global mid-mile networks to aggregate last-mile traffic and deploy SSE enforcement points as close to users as possible. These global access networks must connect to the networks built by the cloud service providers (CSPs) to interconnect their global footprint of data centers. Reconciling these separate networks to optimize performance and security for the different application access flows is a complicated and expensive task, particularly since internet connectivity isn't always an acceptable path for application flows. Enterprises often implement a combination of SSE-managed connectivity and self-managed networking in diverse co-locations to meet their performance, privacy, and security requirements, effectively creating an additional network. By making SASE a cloud native service and consolidating these networks, the problem can be largely simplified and performance can improve significantly.

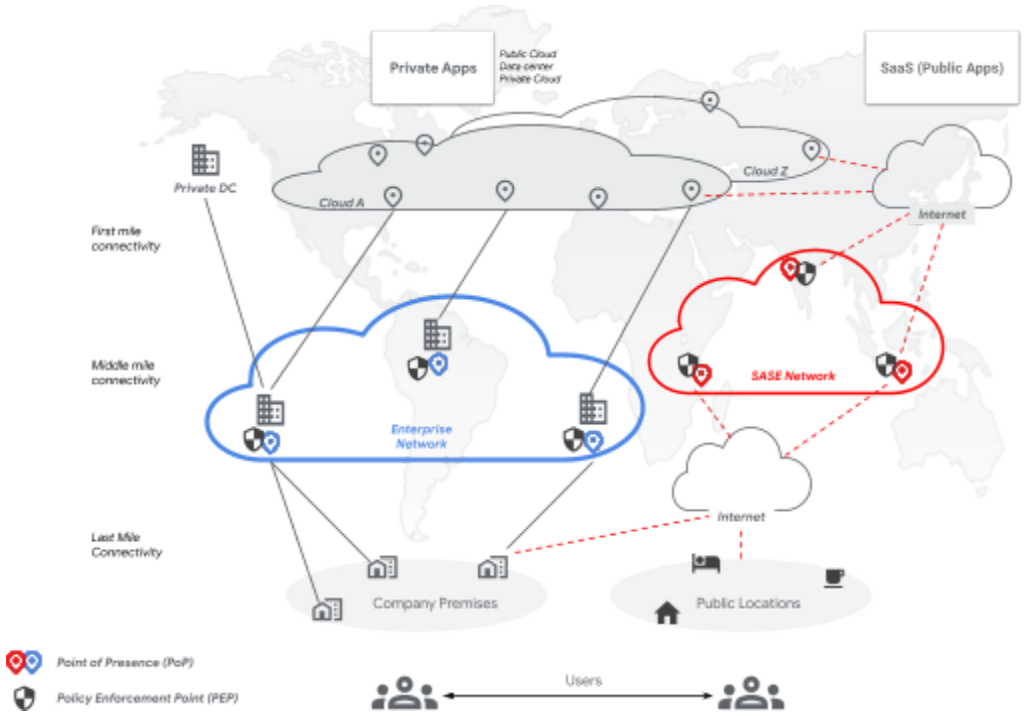
By offering cloud native SASE solutions in the Cross-Cloud Network, the connectivity required to access applications while also enforcing security can be consolidated onto a single network and workstream. Cloud integrations of the SSE stacks that have traditionally leveraged internet connectivity can evolve to use private connections within the cloud network to improve privacy, performance, efficiency, manageability, and cost.

The Cross-Cloud Network offers a platform for the different SASE providers to offer their solutions for user access connectivity and security in a cloud native mode resulting in the following benefits to end customers:

- Reduce the required footprint of self-managed infrastructure in co-locations
- Provide on-demand access to optimal secure connectivity on a global basis
- Cloud native consumption and insertion of SSE security stacks
- Improved throughput and latency for traffic subject to SSE stack security.
- Optionality to combine components of different SASE solutions

Consolidation of the access network

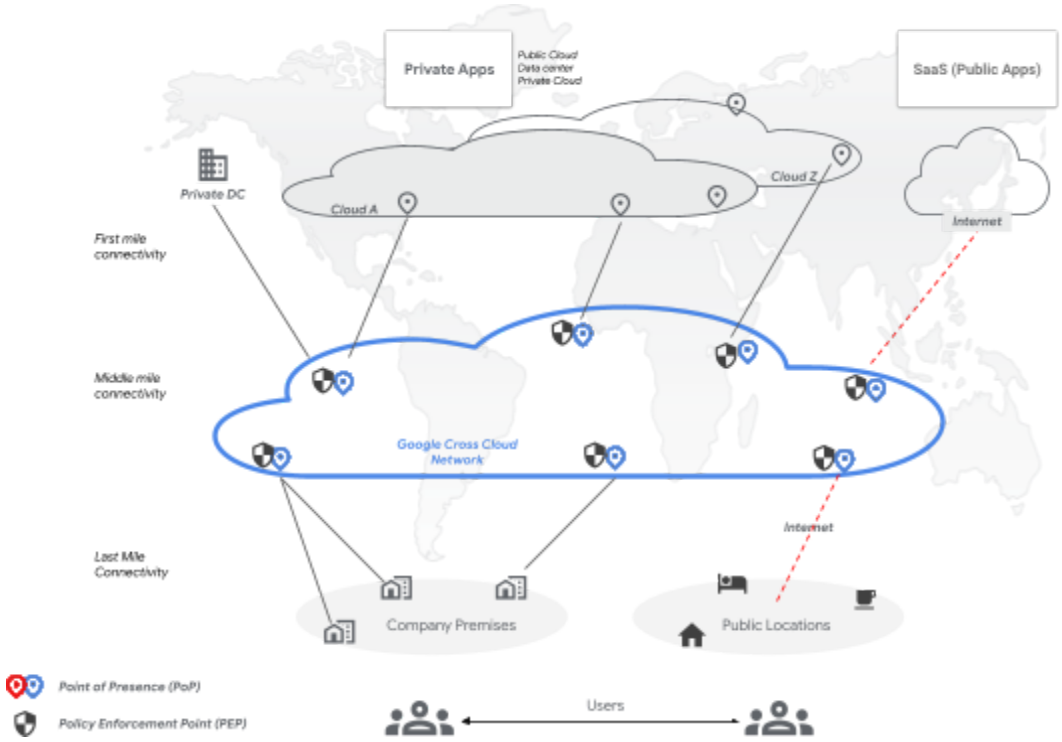
SASE solutions rely on a mid-mile network that offers a rich footprint of points of presence (PoPs) that are interconnected with high performance circuits. User traffic is aggregated at the PoPs, where the SSE stacks are deployed to enforce security on the traffic. For these solutions to be effective in bringing privacy, security, and performance guarantees, traffic needs to be brought to the PoPs as quickly and efficiently as possible. Thus, the mid-mile must have a pervasive footprint of PoPs that is as close to the users as possible.



A mid-mile network with a pervasive footprint of PoPs quickly becomes a large and expensive endeavor to provision and manage. In addition to connecting users, this mid-mile network must connect to the enterprise's private data centers and also to a series of regional data centers in one or more cloud service providers (CSPs). The CSPs already deploy their data centers on a global network designed to be shared by multiple tenants while ensuring privacy and performance for each tenant. Rather than building a separate mid-mile network, Google Cloud's Cross-Cloud Network can be used to deliver the mid-mile connectivity and PoPs with a planet scale network infrastructure that can be accessed pervasively around the world. Google's network is engineered for mission critical availability and has an actively expanding footprint of over 187 PoPs and presence in over 200 countries and territories.

By consolidating the mid-mile network into the Google Cross-Cloud Network, the problem is reduced to effectively using one network, a network that is already built and engineered for planet scale operations. In addition, the Cross-Cloud Network offers a very rich set of options for public and private connectivity to private networks and the internet. Google Cloud has a large ecosystem of internet service provider (ISP) partners and offers turnkey options for private and internet connectivity on a global basis. Custom connectivity to customer premises and other cloud service providers is available with Google Cloud's

portfolio of hybrid connections which includes Cloud Interconnect, Cross-Cloud Interconnect, Cloud VPN and an ecosystem of SD-WAN partners.



Leveraging the Cross-Cloud Network as the mid-mile for SASE services presents benefits to both the SASE providers and the end users of the SASE services. SASE providers can simplify their mid-mile network, expand their geographic reach and evolve their managed services offerings. SASE consumers can leverage cloud native SASE services and consume them elastically anywhere and at virtually any capacity without the need to plan, deploy and manage infrastructure in specific co-location facilities.

Cloud Native Security Stacks

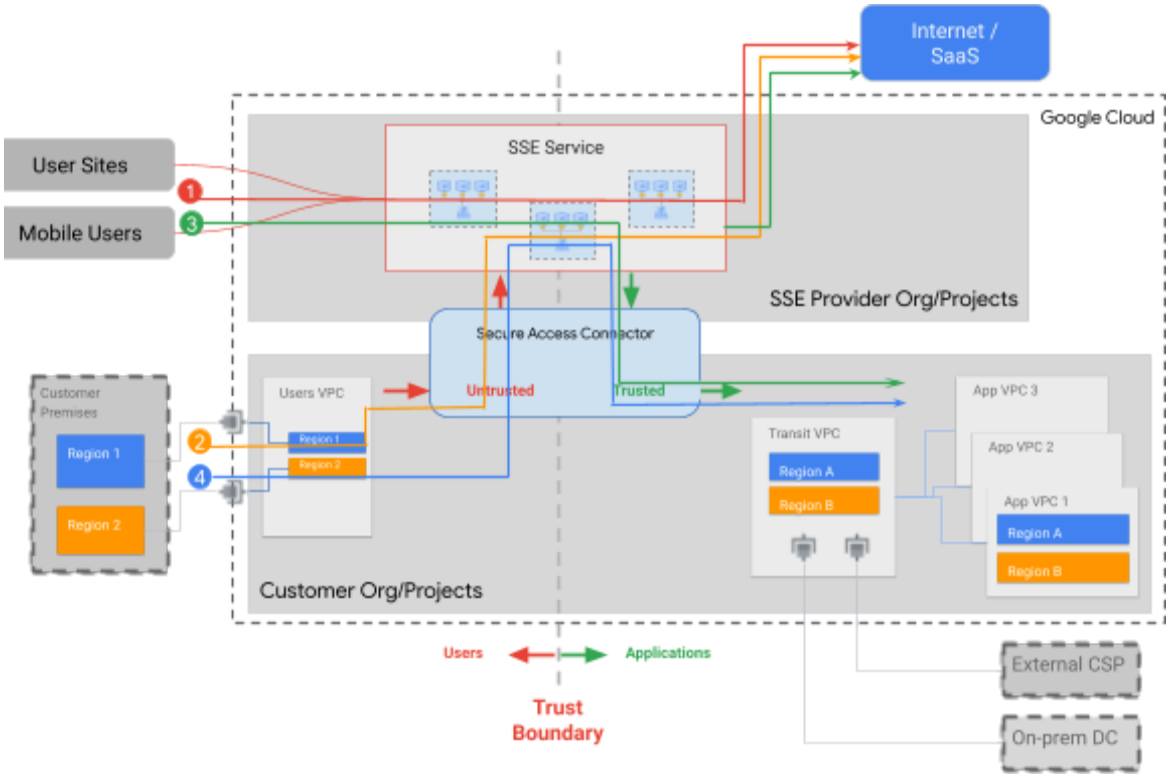
In the Cross-Cloud Network, SSE security stacks are implemented in a cloud native form factor to optimize their pervasiveness, resilience, performance and scale elasticity. End-users may provision SSE stacks on-demand in new locations quickly and reliably. SASE providers may fulfill this demand elastically while minimizing their investment in reserved capacity and pre-provisioned locations, which ultimately minimizes costs. The economies of scale that the on-demand cloud infrastructure enables translate into savings for SASE providers and SASE end-users alike.

An elastic deployment model also allows SASE services to optimize the location of the WAN aggregation nodes and SSE stacks. Traffic no longer needs to be concentrated in predetermined regions or PoPs, but can leverage the global footprint of the Google Cloud network. Furthermore, the capacity of any particular security stack can scale-out horizontally, making the cloud-native SASE solutions truly scale-up or scale-down to the needs of the end-user.

User traffic must be steered to the SSE security stack and then to the target applications in cloud or on-prem data centers. Once user traffic is processed by the security controls of an SSE stack, the privacy and integrity of the traffic must be preserved as it travels from the SSE stack to the application

over the internet. SASE providers guarantee this privacy and integrity by encrypting the traffic from the SSE stack to the destination applications. This encryption has an impact on performance, scale and operations. These artifacts can be avoided by natively deploying the SSE stacks in the cloud and maintaining the traffic inside a private network such as the Cross-Cloud Network in which privacy, integrity and service levels can be guaranteed without the need for encryption. The overhead and performance impact of encrypting traffic is not negligible and therefore having the ability to avoid it opens a much higher performance SSE option.

Managed SSE services hosted in Google Cloud benefit from the global reach and the pervasive set of PoPs and internet peering points of the Google Cloud network. These managed services are hosted in the SSE provider projects and must use the internet to connect to any customer projects. The Secure Access Connect (SAC) is designed to bridge this connectivity between the SSE provider and customer projects and insert SSE services in specific flows based on policy. The SAC is a resource present in the customer project which can steer traffic to or from the SSE service nodes. The SAC is configured to connect to the customer's specific SSE service instance and can be configured to send customer traffic to the SSE stack (on-ramp), bring traffic from the SSE stack to the customer cloud environment (off-ramp) or both.



The off-ramp function of the SAC allows users that already connect to the WAN portion of the SSE service to reach private applications hosted in the Cross-Cloud Network with privacy and high performance, without going out to the internet. (Flow 3 in the figure)

The on-ramp function of the SAC allows sites that require very high capacity connectivity to Google Cloud to access the internet via the SSE service. (Flow 2 in the figure)

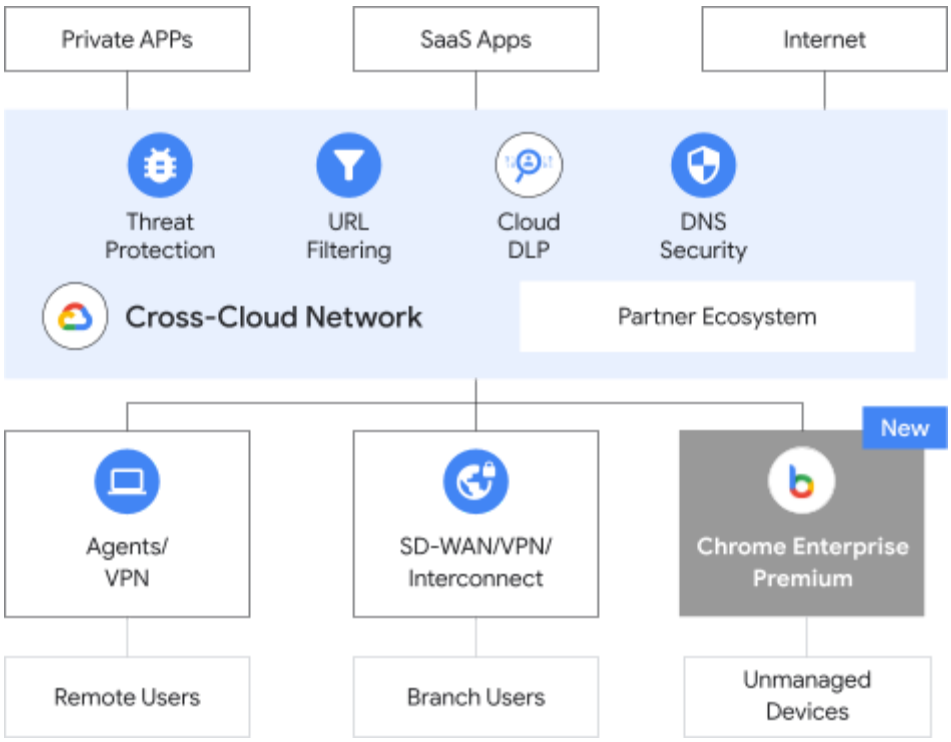
By combining both on-ramp and off-ramp, customer sites that are connected directly to Google Cloud over hybrid connections can access private applications hosted in the Cross-Cloud Network securely through the SSE stack. (Flow 4 in the figure)

By using the SAC in the VPC network, customers can streamline security for all user-to-application flows through the SSE service of their choice. The insertion of the SSE stack is based on policy and the stack instances are available elastically in Google Cloud throughout the globe. Optimal placement of security enforcement along with high bandwidth private connectivity leads to optimal application experience.

Secure user connectivity from any location on any device

A cloud integrated SASE stack enables secure workforce connectivity from any location. Users may connect from company premises where the network is private and secure or they may connect from public shared networks where privacy and security cannot be guaranteed. The Cross-Cloud Network expands the set of connectivity options for mobile users and provides the flexibility to connect over private wide area networks, VPNs over the internet, or SD-WAN. Different connectivity solutions can be combined while consolidating the security enforcement onto a common stack. Thus, an enterprise may use an evolving variety of connectivity solutions, all of which can be aggregated onto the Cross-Cloud Network where traffic can be steered to a consolidated SSE security solution.

The workforce may also be enabled to use devices that are not company owned. A secure enterprise browser (SEB) can secure connections from any device and allow users to securely use their own device without the overhead of making these devices managed devices that would require the deployment of mobility management solutions. Effectively extending the range of secure user connectivity options to include unmanaged devices at any location.



SASE Partner Ecosystem

The Cross-Cloud Network offers a broad choice of SSE solutions from leading SASE vendors. This growing ecosystem includes Broadcom, Fortinet, and Palo Alto Networks.

Summary

In the Cross-Cloud Network SSE stacks are integrated into the cloud traffic flows using a policy language that drives the selection of the traffic to be processed by the SSE stacks, but also drives the locations of the SSE stacks. As the Cross-Cloud Network creates a private, high performance network across the different cloud service providers and on-prem data centers, privacy, integrity and high speed connectivity are guaranteed for traffic destined to any workload in any cloud or private data center. The Cross-Cloud Network makes the experience and performance of deploying SSE security truly cloud native by making the consumption of the resources demand based and policy driven.