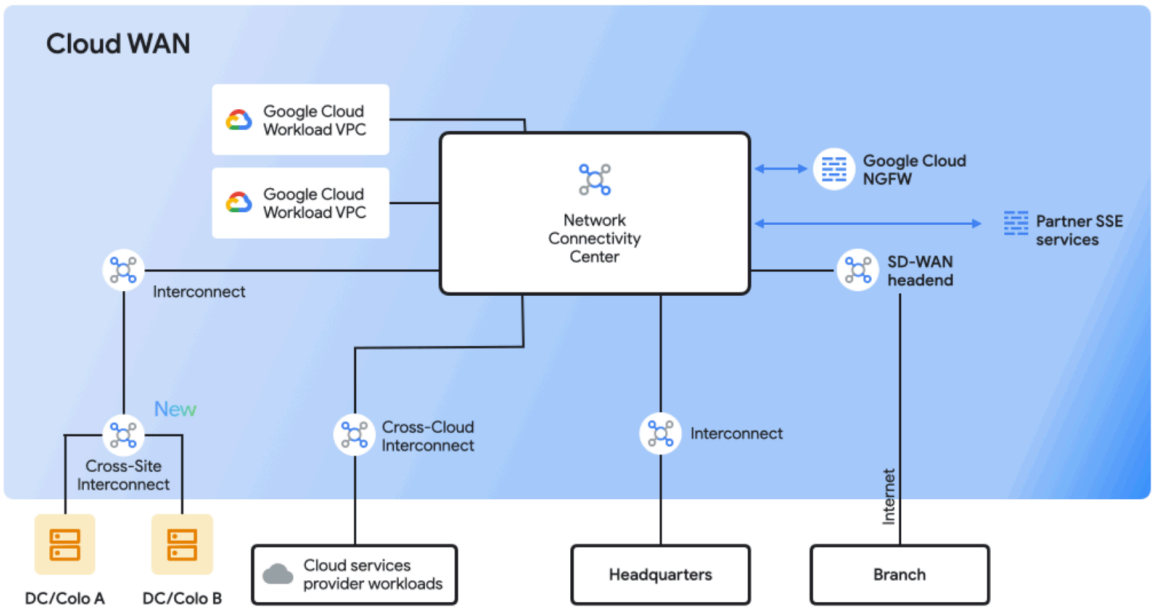
Google Cloud

Cloud WAN

Solution overview



For more information visit **cloud.google.com**

Connect Your Enterprise Securely & Globally

Cloud WAN enables secure, high-performance access to applications from any location by leveraging Google's global network and cloud-native security solutions.

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 over an unsecured public network, user connectivity must be secured to prevent incidents that exploit users as an attack vector and, especially over untrusted networks or unmanaged devices that expand 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 user authentication and authorization, 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 a choice of next generation firewalls (NGFW) and security service edge (SSE) managed services. Connectivity controls are required to ensure that user traffic is steered through the NGFW or SSE security stacks. SSE providers build global middle-mile networks to aggregate last-mile traffic and deploy SSE enforcement points as close to users as possible. Users deploying their own stack of NGFWs take on the task of building the middle-mile network themselves.

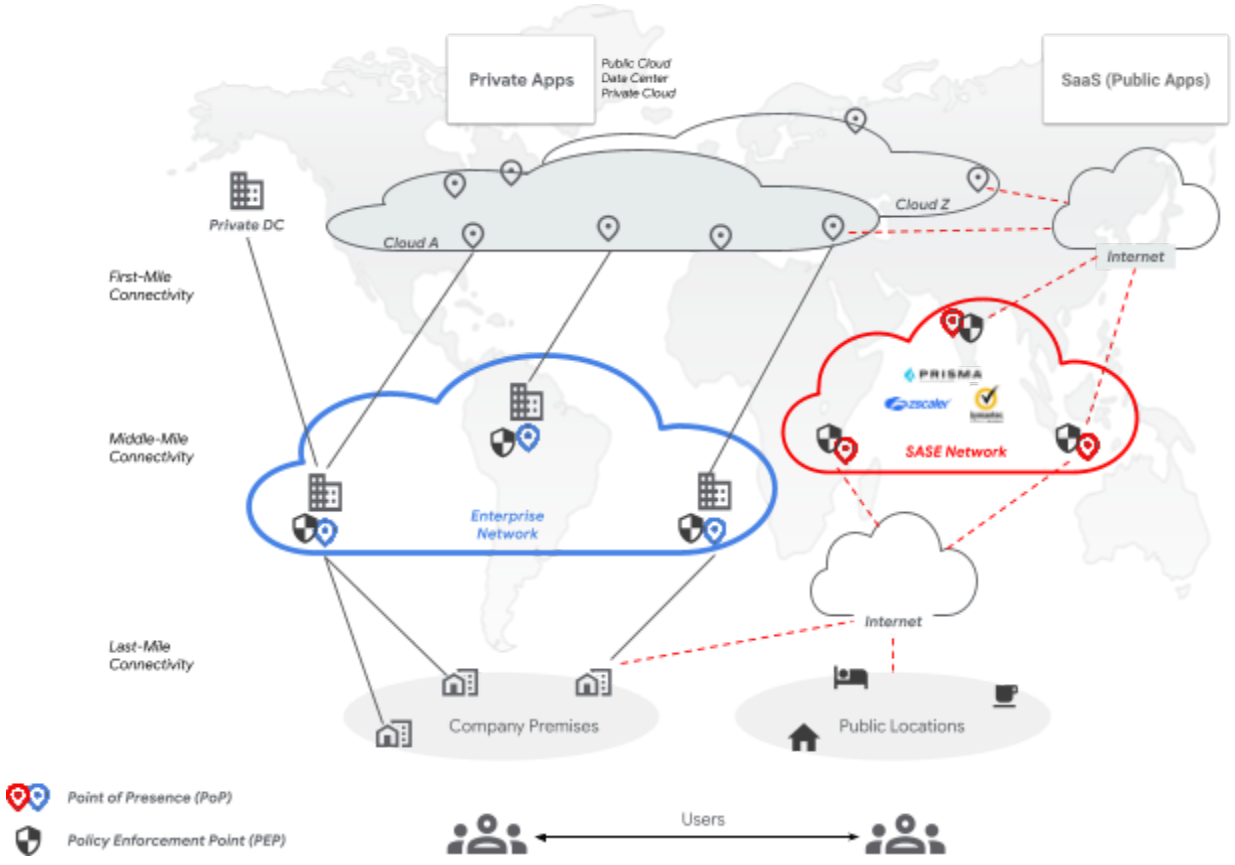
Enterprises often implement a combination of SSE-managed connectivity and self-managed networking in diverse co-locations to meet their performance, privacy, and security requirements, effectively creating an additional network. These global access networks must connect to the networks built by the cloud 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. By making the security stacks cloud-native and consolidating these networks, the problem can be largely simplified and performance can improve significantly. By offering cloud-native security solutions in 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 and costly encryption can evolve to use private connections within the cloud network to improve privacy, performance, efficiency, manageability, and cost. Expensive and operationally intensive deployments of network and security infrastructure at colocations can also be minimized. Cross-Cloud Network offers a

platform for the different security providers to offer their solutions for user access connectivity and security in a cloud-native model, 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 NGFW and SSE security stacks
- Improved throughput and latency for traffic subject to SSE stack security
- Leverage the performance, ubiquity, and reliability of Google's planet-scale network.

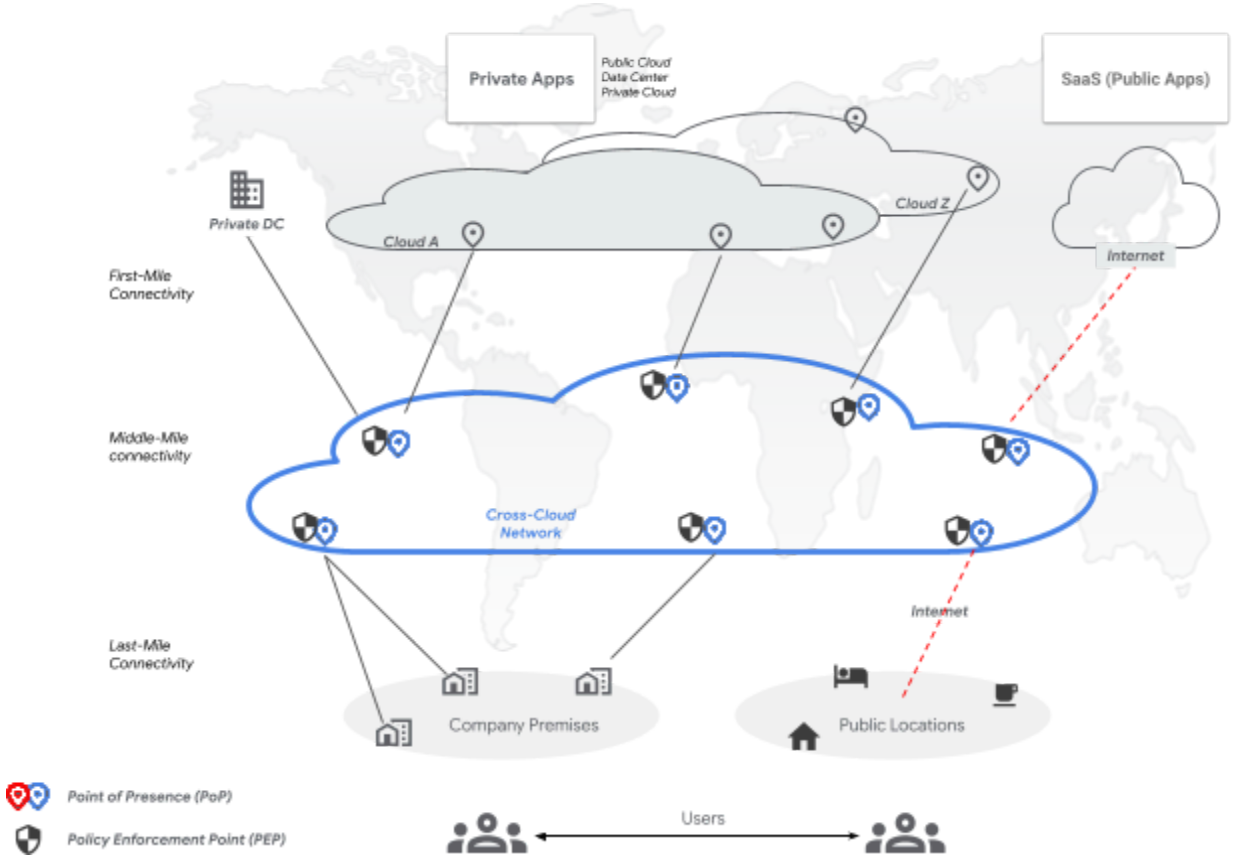
Consolidation of the access network

Wide area network (WAN) solutions rely on a middle-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 security 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 b ought to the PoPs as quickly and efficiently as possible. Thus, the middle-mile must have a pervasive footprint of PoPs that is as close to the users as possible.



A middle-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 middle-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). 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 middle-mile network, Cross-Cloud Network can be used to deliver the middle-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 202 PoPs and presence in over 200 countries and territories. By consolidating the middle-mile network into 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, 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 Cross-Cloud Network as the middle-mile for the enterprise WAN presents benefits to the security providers, access network providers and the end users of the security and access services. Security providers can simplify their middle-mile network, expand their geographic reach and evolve their managed services offerings. Network security consumers can leverage cloud-native security 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.

Using the Google network as the middle-mile backbone gives the enterprise access to planet-scale networking reach and capacity that can be consumed elastically. The Google network has an extensive footprint with over 202 PoPs thoughtfully distributed worldwide. A rich menu of connectivity options allows enterprises to connect their sites privately with dedicated capacity using Dedicated Interconnect or sub-rate services delivered via Partner Interconnect. Direct back-to-back connectivity with other CSPs is also available with Cross-Cloud Interconnect. Google has a pervasive footprint of internet

peerings, and the Verified Peering Partner (VPP) program guarantees a high standard of reliability for internet connectivity when using an internet partner that participates in the VPP program. Premium tier networking allows enterprises to ensure that traffic enters the Google network as soon as possible to minimize any last--mile delays, and also guarantees that traffic remains on the Google network as long as possible so that it can benefit from the performance and reliability characteristics of the Google network.

The large number of PoPs and regions in the Google network are interconnected with high path diversity inclusive of subsea cable paths that are exclusive to Google. This high path diversity serves as the foundation to achieve a level of reliability that would be very expensive to match in a private network. The Google network delivers a 99.99% SLO through the unique combination of broad path diversity, routing protocol optimization and Protective ReRoute to maximize traffic paths, convergence efficiency and route around network protocol failures. By consolidating connectivity onto the Google network, enterprises inherit the ubiquity, scale, throughput, latency and reliability benefits that the Google network offers to Google's own global applications. These network benefits can all be consumed as a service with Cloud WAN.

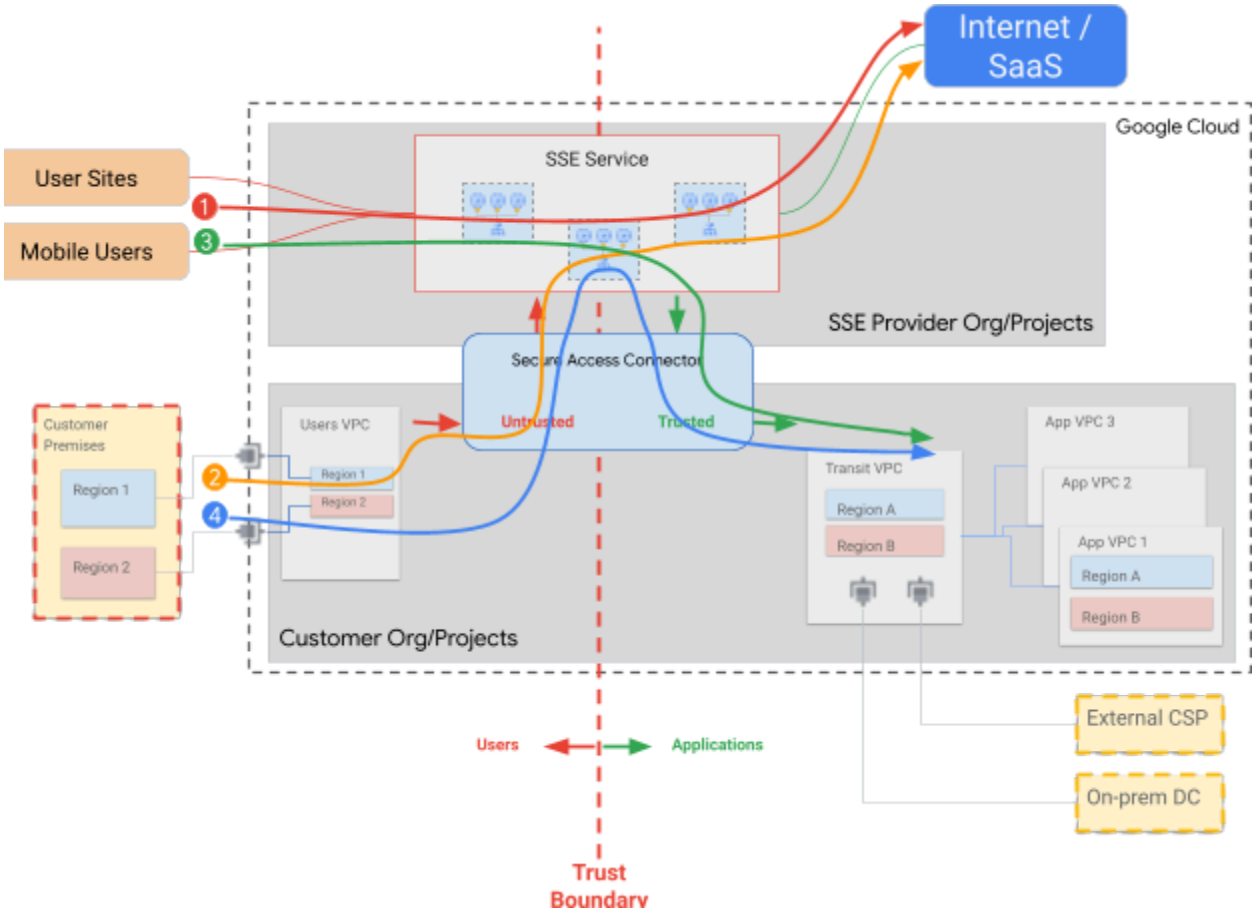
The high performance, reliable connectivity offered by the Google network can be combined with an SD-WAN overlay to automate and scale the enterprise access network and aggregate site traffic onto the Cross-Cloud Network. Cloud WAN optimizes the deployment of SD-WAN head-ends and high performance connections to external data centers and orchestrates the connectivity amongst these multiple external networks using the Network Connectivity Center (NCC) as the orchestration hub. Connecting multiple external networks on a global footprint is as simple as bringing the cloud resources through which the external networks connect under the management of a common NCC orchestration hub.

Cloud-native security stacks

In 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. SSE 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 SSEproviders and SSE end-users alike. Similarly, enterprises may consume NGFW security stacks as a cloud-native service enabled by packet interception using firewall policies. The scaling and lifecycle management of the firewalls is handled by Google Cloud or a 3rd party security provider, the insertion of the firewalls is expressed as packet interception policy and does not require complex routing exceptions.

An elastic deployment model allows enterprises using Cloud WAN to optimize the location of the WAN aggregation nodes, NGFWs, and SSE stacks. Traffic no longer needs to be concentrated in predetermined regions or PoPs to be steered through a particular security service, but can leverage the global footprint of the Google network. Furthermore, the capacity of any particular security stack can scale-out horizontally, making the cloud-native security solutions truly scalable for the needs of the end-user. User traffic is seamlessly steered to the SSE or NGFW 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 a NGFW or an SSE stack, the privacy and integrity of the processed traffic must be preserved as it travels from the security stack to the application. SSE providers that offer security as a service use the internet to transport the "scrubbed" traffic and guarantee the privacy and integrity of the data by encrypting the traffic from the SSE/NGFW stack to the destination applications. This encryption has an impact on performance, scale and operations. These issues can be avoided by natively deploying the

SSE stacks in the cloud and maintaining the traffic inside a private network such as Cross-Cloud Network in which privacy, integrity, and service levels can be guaranteed without the need for encryption. 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 network. These managed services are hosted in the SSE provider projects and must use the internet to connect to any customer projects. 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. SAC is a resource present in the customer project which can steer traffic to or from the SSE service nodes. 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 Cross-Cloud Network with privacy and high performance, without going out to the internet (flow 3 in the diagram). The on-ramp function of SAC allows sites that require very high capacity connectivity to Google Cloud to access the internet via the SSE service (flow 2 in the diagram). 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 Cross-Cloud Network securely through the SSE stack (flow 4 in the diagram).

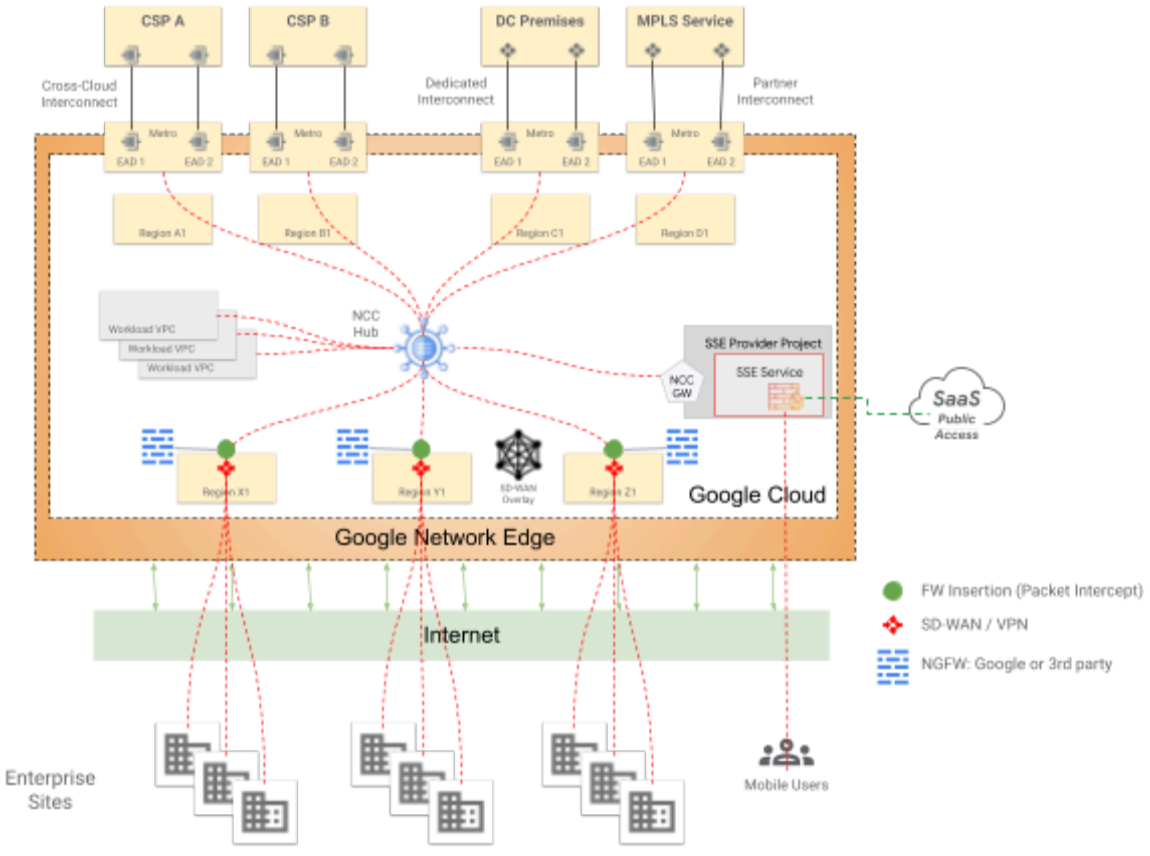
By using SAC in the VPC network, customers can streamline security for all user-to-application flows through the SSE service of their choice. The insertion of the SSE stack is based on policy and the stack instances are available elastically in Google Cloud throughout the globe. Optimal placement of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

In many cases, using an NGFW may be preferable to an SSE service. Cross-Cloud Network offers NGFWs as-a-service. Customers have a choice of Google Cloud provided NGFWs or 3rd party firewalls as follows:

- Cloud NGFW using firewall endpoints.
- 3rd party NGFWs using in-band Network Security Integration (NSI)

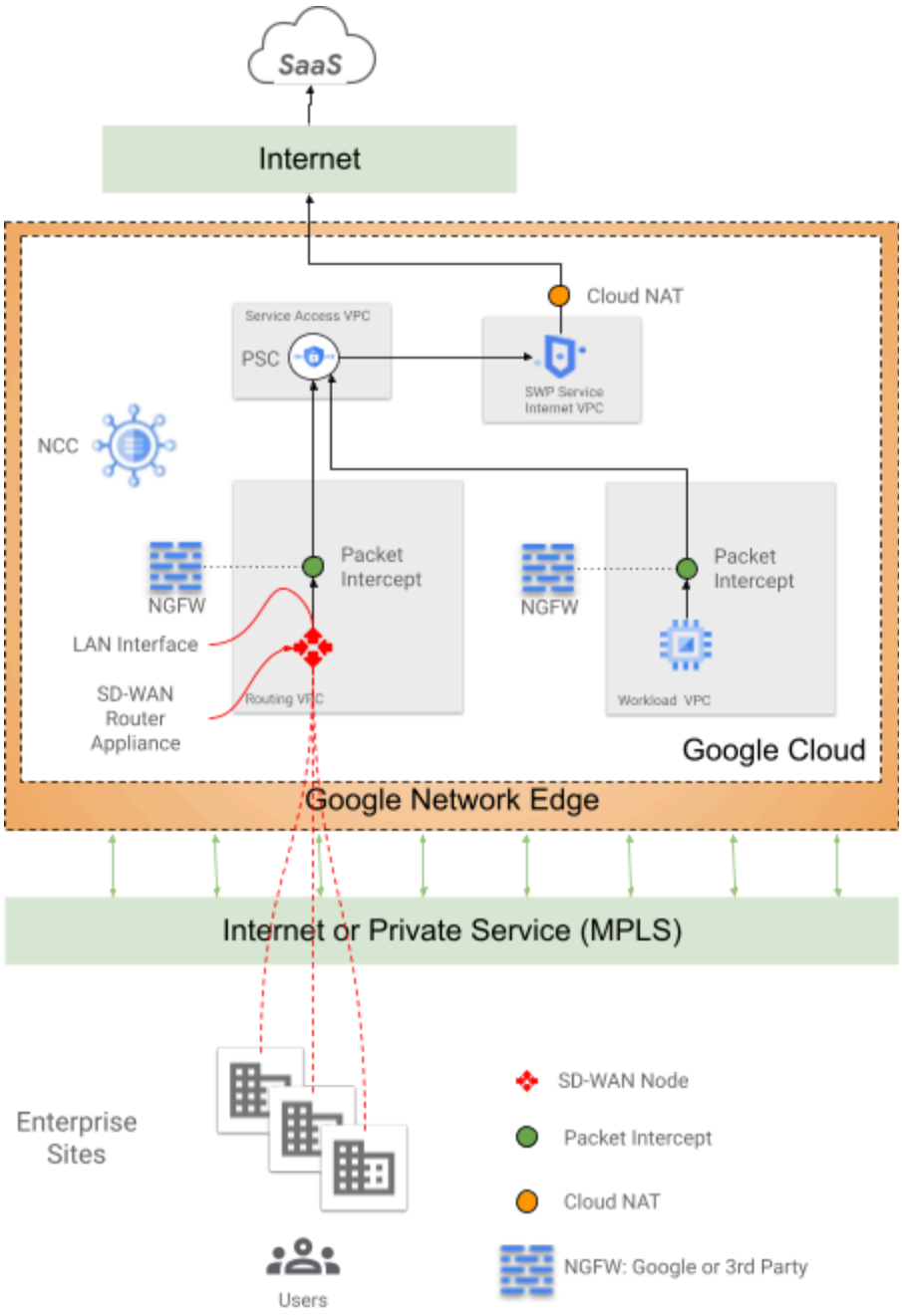
Cloud NGFW is fully managed by Google and offers an integrated policy language that is optimized to integrate with the Google Cloud networking and resource model. 3rd party NGFWs enable enterprises to use policy engines and tooling that may be consistent with other areas of their deployment.

Insertion of either of these firewalls in-band is enabled by packet interception using firewall policies. Traffic entering or leaving a workload can be intercepted (when there is a policy match) and steered to a firewall resource (and back) for enforcement of security policies. Traffic being aggregated using SD-WAN router appliances offer an ideal point for packet interception and security policy enforcement for all user traffic coming via SD-WAN as depicted in the figure below. The firewall resource can be fully managed by Google Cloud in the case of the firewall endpoints for the Cloud NGFW, or it may be managed by the user when opting for 3rd party NGFWs using in-band Network Security Integration (NSI).



The packet interception model is also instrumental in enabling efficient internet egress security with network address translation (NAT) and proxy services for URL filtering using Secure Web Proxy (SWP). SWP can be deployed as a service leveraging the Private Service Connect (PSC) producer-consumer

model in combination with NGFW and NAT functionality as illustrated in the following diagram. As depicted, the same pattern can be used to secure internet egress connectivity for any workload hosted in Google Cloud.



Security Partner Ecosystem

Cross-Cloud Network offers a broad choice of SSE solutions from leading SSE partners. This growing ecosystem includes Broadcom, Check Point, Cisco, Fortinet, and Palo Alto Networks.

Summary

In Cross-Cloud Network, NGFW and 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 security stacks. Furthermore, security enforcement is offered as a service and deployed in-line, without complex routing exceptions to steer traffic in suboptimal ways. As Cross-Cloud Network leverages the Google network to create a private, high performance network across 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. Cross-Cloud Network makes the experience and performance of deploying network security truly cloud-native by leveraging the performance and reliability of the Google network while making the consumption of the security resources demand-based and policy-driven.