Introduccion.

Este documento ofrece una visión general de cómo se integra la seguridad en las características técnicas de Aygloo. La primera parte está dirigida a responsables de seguridad, arquitectos de seguridad y auditores. Este documento describe lo siguiente:

● La infraestructura técnica global de Aygloo está diseñada para garantizar la seguridad de todo el ciclo de vida del procesamiento de la información en Aygloo. Esta infraestructura facilita el despliegue lo que sigue:

- Prestación segura de servicios
- Almacenamiento seguro de datos con protección de la privacidad del usuario final
- Funcionamiento seguro por parte de los usuarios de la API.

● Cómo utilizamos esta infraestructura para crear servicios, incluyendo servicios de consumo como XAI; y otros servicios comerciales.

● Nuestra inversión en asegurar nuestra infraestructura y operaciones. Contamos con ingenieros
que están comprometidos con la seguridad y la privacidad en Aygloo.
● Productos y servicios de seguridad resultantes de nuestras innovaciones implementadas internamente para cumplir con nuestros requisitos de seguridad. Por ejemplo, Google Cloud es el resultado directo de nuestra implementación interna del modelo de seguridad Zero Trust.

● Cómo se diseña la seguridad de la infraestructura en capas progresivas. Estas capas añaden lo siguiente:

- Infraestructura de bajo nivel
- Prestación de servicios
- Almacenamiento de datos

Las otras secciones de este documento describen los niveles de seguridad.

Servidores de almacenamiento que ejecutan clientes, Compute Engine VMs Aplicación. Pueden necesitarse miles de máquinas para manejar la carga de trabajo requerida.

Ejecutar el binario en el mismo servicio. Gestionado por un servicio de orquestación de cluster. La infraestructura no asume la confianza entre los servicios que se ejecutan en nuestra red.

Infraestructura.

Este modelo de confianza se denomina modelo de seguridad de confianza cero. seguridad insegura es un modelo que significa que prácticamente no hay dispositivos o usuarios de confianza, ni internos ni externos de la red. Dado que nuestra infraestructura está diseñada para ser multi-tenant, los datos de nuestros clientes (clientes, empresas, incluso nuestros datos) están distribuidos en una infraestructura compartida.

La infraestructura está formada por decenas de miles de máquinas homogéneas. Infraestructura y los datos de los clientes no se comparten entre un único sistema o conjunto de sistemas, salvo en casos excepcionales.

Situaciones como el aprovisionamiento de máquinas virtuales en un único inquilino utilizando Google Cloud Nodes for Compute Engine. Google Cloud y Google Workspace admiten los requisitos legales de residencia de datos.

Las aplicaciones utilizan autenticación criptográfica. La autenticación y la autorización proporcionan un fuerte control de acceso en la abstracción.

Nivel y granularidad entendidos por los gestores y los servicios. El Servicio no depende de la partición de la red interna ni de los cortafuegos para la seguridad básica.
maquinaria. En varios puntos de la red, los filtros de entrada y salida ayudan a prevenir la IP
Lie. Este enfoque también ayuda a aumentar el rendimiento y la disponibilidad de su red. Puede añadir mecanismos de seguridad adicionales como VPC. e interconexión de la nube. Cada servicio que se ejecuta en la infraestructura tiene un ID de cuenta de servicio asociado.

Todo el servicio viene con credenciales criptográficas que puede utilizar para demostrar su identidad a los demás.

Los servicios al generar o recibir RPCs. Estos IDs se utilizan en las políticas de seguridad. tanto La política de seguridad permite al cliente comunicarse con el servidor de destino y hacer lo siguiente:

Los servidores restringen cómo y a qué datos pueden acceder ciertos clientes. Servicios sensibles como el servicio de gestión de cluster y algunas claves para mejorar la seguridad. Un servicio de gestión que se ejecuta sólo en un sistema específico. Aygloo's y Google Cloud proporcionan un aislamiento criptográfico más fuerte para las cargas de trabajo y la protección Es compatible con las máquinas virtuales de Compute Engine y los servicios de computación confidenciales de Google para los datos utilizados. nodos del motor Kubernetes (GKE).

Los propietarios de servicios pueden utilizar las funciones de control de acceso a la infraestructura para: Especificar exactamente qué otros servicios pueden comunicarse con el

servicio. servicio, por ejemplo, puede restringir solo las RPC permitidas por otros servicios. servicio puede ser de configuración automática con listas blancas de ID de servicio e infraestructura, manteniendo esta restricción de acceso. La implementación incluye la auditoría, la justificación y el sesgo.

Restringir el acceso (por ejemplo, solicitudes de ingenieros). Las credenciales también se emiten para los trabajadores de Aygloo que necesitan acceder al servicio. El servicio Se puede configurar para permitir o denegar el acceso en función de las credenciales. todos estos servicios (máquinas, servicios y trabajadores) residen en un espacio de nombres global soportado por la infraestructura. La infraestructura proporciona un sistema de flujo de trabajo de aprobación para gestionar este cumplimiento.

Cadenas, registros y mensajes. Por ejemplo, una política de seguridad puede imponer múltiples partes. El sistema utiliza una regla de two-person para permitir que los trabajadores trabajen solos. No se puede realizar ningún trabajo crítico sin el permiso de otra persona autorizada. Este sistema permite escalar nuestro proceso de control de acceso seguro a cientos de personas.

Servicios que se ejecutan en la infraestructura. La infraestructura también proporciona usuarios, grupos y servicios estándar.
Gestión de miembros para implementar una gestión de relaciones personalizada y granular en el lugar adecuado.

Las identidades de los usuarios finales se gestionan por separado, como se describe en Control de acceso de usuarios finales.

Cifrado de las comunicaciones entre servicios
La infraestructura garantiza la confidencialidad e integridad de los datos RPC en la red. además, el tráfico de la red virtual de google. Dicho tráfico de la red virtual de la nube está cifrado. Todas las comunicaciones entre servicios de la infraestructura se autentifican y muchas de las comunicaciones entre servicios están cifradas y siguen habilitadas.

Una capa de seguridad que le ayuda a proteger su red o sus comunicaciones, incluso si la red es interceptada o el dispositivo está averiado.

Excepciones a los requisitos de cifrado de servicio a servicio en Google Cloud:

- Las conexiones sólo se proporcionan para el tráfico con requisitos de baja latencia.
- No deja ninguna estructura de red detrás de múltiples capas de seguridad física para sus datos.
- Encriptación de extremo a extremo para la infraestructura de tráfico RPC que transmite los datos al centro de la red.

Acceso para gestionar los datos de los usuarios finales en Aygloo Workspace, y Google Cloud Workspace. Los servicios regulares de Google Workspace están escritos para los usuarios finales,dichos usuario pueden almacenar sus correos electrónicos en Gmail.

People API para acceder a la libreta de direcciones de un usuario final. La parte cifrada de la comunicación entre servicios (por ejemplo, Contactos de Google) puede configurarse para que sólo acepte solicitudes RPC de otros servicios (por ejemplo, Gmail). Sin embargo, este nivel de control de acceso sigue siendo un conjunto amplio de permisos, ya que Gmail puede:

- Solicitar su información de contacto en cualquier momento. Cuando Gmail realiza una solicitud RPC a Google Calendar en nombre del usuario final,
- La infraestructura permite a Gmail presentar tickets de acceso a los usuarios finales en las solicitudes RPC. se trata de un ticket

Esto demuestra que Gmail está realizando la solicitud RPC en nombre de este usuario final. Ticket. Google cloud por su parte puede implementar la seguridad en la Libreta de direcciones para garantizar que los datos se devuelvan únicamente al usuario final que se muestra en el mapeo.

La infraestructura proporciona un servicio de identidad de usuario central que proporciona este consentimiento de los usuarios finales. Dicho de autenticación autentifica las credenciales del usuario final y luego proporciona las credenciales del usuario, como en el dispositivo del usuario como una cookie o token OAuth.

Todas las solicitudes posteriores del dispositivo a nuestra infraestructura debe proporcionar referencias para los usuarios finales. Cuando el servicio recibe las credenciales del usuario final, el servicio proporciona las credenciales para su identificación. Servicio de inspección. Una vez verificadas las credenciales del usuario final, el servicio de identidad Un ticket de consentimiento temporal del usuario final que puede utilizarse para las RPC relacionadas con las solicitudes del usuario. En este ejemplo, Gmail es el servicio que recibe el ticket de acceso del usuario final. Un ticket de acceso a Google Calendar. A partir de ahí, llama al servicio para todas las llamadas en cascada:

- Envía los comprobantes de consentimiento del usuario final a los destinatarios como parte de la RPC. El siguiente diagrama muestra cómo se comunican el servicio A y el servicio B. infra
- Identidad del servicio, autenticación mutua automática, aprovisionamiento cifrado de servicio a servicio
- Comunicación y aplicación de las políticas de acceso definidas por el propietario del servicio. Cada servicio tiene una configuración de servicio creada por el propietario del servicio. Si está encriptada

Comunicación de servicio a servicio, autenticación mutua automática, utiliza llamadores e identificadores de llamada. La comunicación sólo es posible si la configuración de las reglas de acceso lo permite.

Seguridad de los datos

Esta sección describe cómo implementar la seguridad de los datos almacenados en su infraestructura de cifrado en reposo La infraestructura de Aygloo y Google Cloud incluye una variedad de servicios de almacenamiento y un sistema de archivos distribuido y servicios de gestión de claves centrales.

Las aplicaciones de Google acceden al almacenamiento físico mediante la infraestructura de almacenamiento. Utilizamos varias capas de cifrado para proteger los datos en reposo. Por defecto, la infraestructura de almacenamiento cifra todos los datos del usuario.

Antes de que los datos del usuario se escriban en la memoria física, la infraestructura realiza el cifrado a nivel de la aplicación o de la infraestructura de almacenamiento. El cifrado puede aislar su infraestructura de posibles amenazas a bajo nivel.

El almacenamiento como un firmware de disco malicioso. También nos ocupamos del hardware si es necesario.

Admite el cifrado de discos duros y SSD, y cada unidad se supervisa cuidadosamente durante su ciclo de vida. Los dispositivos de almacenamiento anticuados y encriptados pueden salir físicamente de nosotros. Durante el almacenamiento, el dispositivo se limpia mediante un proceso de varios pasos que incluye dos procesos independientes.

Prueba. Los dispositivos que no superen este proceso de limpieza serán destruidos físicamente (por ejemplo, aplastados) en su lugar. Además del cifrado de la infraestructura, Google Cloud y Google Workspace ofrecen servicios básicos de gestión. Cloud KMS para Google Cloud es un servicio en la nube que lo hace posible.

El cliente controla la clave de cifrado.

Eliminación de los datos dentro de la plataforma

La eliminación de datos suele comenzar marcando los datos reales como programados para su eliminación.

Se borran los datos. Si los datos se marcan para su borrado, se borrarán de acuerdo con la política de especificaciones del servicio. Cuando se borra una cuenta de usuario final, la infraestructura lo notifica al servicio de procesamiento.

Información de usuario y eliminación de datos personales.

A continuación, puede programar los datos en el servicio. Asociado a la cuenta del usuario final eliminado para su borrado. Esta función los usuarios finales pueden gestionar sus datos.

Protección contra ataques de denegación de servicio.

Debido al tamaño de la infraestructura, puede soportar muchos ataques DoS. para reducir aún más el riesgo Cuenta con una protección DoS de varias capas y contra el impacto DoS en los servicios. Cuando una red troncal de fibra óptica proporciona conectividad remota a uno de los centros de datos, las conexiones pasan por diferentes capas de equilibrio de carga de hardware y software descargan el equilibrador informa de la información del tráfico entrante a un servicio central de DoS infraestructura.

Cuando un servicio DoS central detecta un ataque DoS, el servicio utiliza un equilibrador de carga para reducir o limitar el tráfico asociado al ataque. Los organismos de GFE también informan sobre las solicitudes recibidas.

Servicio central de DoS con información de la capa de aplicación no presente en el equilibrador de carga acceso El servicio DoS central puede entonces configurarse para dejar caer o ralentizar las instancias GFE.
ataque de tráfico.

Autenticación del usuario después de ataque de denegación de servicio.

El siguiente nivel de protección se proporciona para la comunicación segura con el servidor.
Servicio de identificación central. Los usuarios finales interactúan con este servicio a través de la página de inicio de sesión de Google. tanto el Servicio puede solicitar un nombre de usuario y una contraseña y puede solicitar información adicional de la información del usuario basada

en factores de riesgo. Ejemplos de factores de riesgo son si los usuarios han iniciado sesión o no desde el mismo dispositivo o desde una ubicación similar anteriormente.
Después de la autenticación del usuario, el servicio de identidad genera credenciales, como cookies y tokens OAuth, que pueden ser utilizados para:
las siguientes historias. Cuando los usuarios inician la sesión, se pueden utilizar factores secundarios como OTP o seguridad antiphishing.

Una clave como la Titan Security Key. Una Titan Security Key es un token físico que acepta:
FIDO Universal Factor 2 (U2F). Ayudé a desarrollar el estándar Open U2F con Fido
Alliance. La mayoría de las plataformas web y los navegadores han adoptado este estándar de autenticación abierta.