Google Cloud

Infrastructure Google

Présentation de la conception de la sécurité

Livre blanc Google Cloud

Google Cloud

Table des matières

Google Cloud

Résumé au niveau du DSI

- Google dispose d'une infrastructure technique à l'échelle mondiale conçue pour assurer la sécurité tout au long du cycle de vie du traitement des informations chez Google. Cette infrastructure permet un déploiement sécurisé des services, un stockage sécurisé des données avec des garanties de confidentialité de l'utilisateur final, des communications sécurisées entre les services, une communication sécurisée et privée avec les clients sur Internet et un fonctionnement sécurisé par les administrateurs.

- Google utilise cette infrastructure pour créer ses services Internet, notamment des services grand public tels que Search, Gmail et Photos, ainsi que des services d'entreprise tels que G Suite et Google Cloud Platform.

- La sécurité de l'infrastructure est conçue en couches progressives, depuis la sécurité physique des centres de données, en passant par la sécurité du matériel et des logiciels qui sous-tendent l'infrastructure, et enfin, les contraintes techniques et les processus en place pour soutenir la sécurité opérationnelle.

- Google investit massivement dans la sécurisation de son infrastructure avec plusieurs centaines d'ingénieurs dédiés à la sécurité et à la confidentialité répartis dans l'ensemble de Google, dont beaucoup sont des autorités reconnues du secteur.

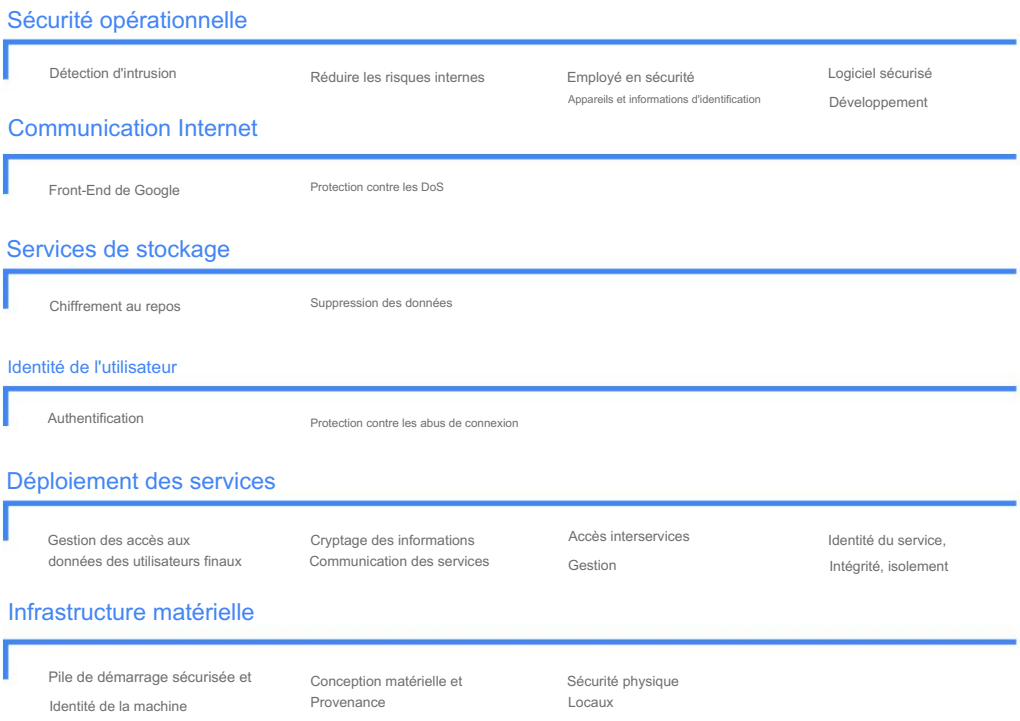
Introduction

Ce document donne un aperçu de la façon dont la sécurité est conçue dans l'infrastructure technique de Google. Cette infrastructure à l'échelle mondiale est conçue pour assurer la sécurité tout au long du cycle de vie du traitement des informations chez Google. Cette infrastructure permet un déploiement sécurisé des services, un stockage sécurisé des données avec des garanties de confidentialité de l'utilisateur final, des communications sécurisées entre les services, une communication sécurisée et privée avec les clients sur Internet et un fonctionnement sécurisé par les administrateurs.

Google utilise cette infrastructure pour créer ses services Internet, notamment des services grand public tels que Search, Gmail et Photos, ainsi que des services d'entreprise tels que G Suite et Google Cloud Platform.

Nous décrirons la sécurité de cette infrastructure par couches progressives, en commençant par la sécurité physique de nos centres de données, en passant par la manière dont le matériel et les logiciels qui sous-tendent l'infrastructure sont sécurisés, et enfin, en décrivant les contraintes techniques et les processus en place pour soutenir les opérations. sécurité.

Couches de sécurité de l'infrastructure Google



Graphique 1.
Couches de sécurité de l'infrastructure Google : Les différentes couches de sécurité, depuis l'infrastructure matérielle au niveau inférieur jusqu'à la sécurité opérationnelle au niveau supérieur. Le contenu de chaque couche est décrit en détail dans le document.

Infrastructure de bas niveau sécurisée

Dans cette section, nous décrivons comment nous sécurisons les couches les plus basses de notre infrastructure, allant des locaux physiques au matériel spécialement conçu dans nos centres de données en passant par la pile logicielle de bas niveau exécutée sur chaque machine.

Sécurité des locaux physiques

Google conçoit et construit ses propres centres de données, qui intègrent plusieurs couches de protections de sécurité physique. L'accès à ces centres de données est limité à une très petite fraction seulement des employés de Google. Nous utilisons plusieurs couches de sécurité physique pour protéger les étages de nos centres de données et utilisons des technologies telles que l'identification biométrique, la détection de métaux, des caméras, des barrières pour véhicules et des systèmes de détection d'intrusion par laser. Google héberge également certains serveurs dans des centres de données tiers, où nous veillons à ce que des mesures de sécurité physique contrôlées par Google s'ajoutent aux couches de sécurité fournies par l'opérateur du centre de données. Par exemple, sur ces sites, nous pouvons utiliser des systèmes d'identification biométrique indépendants, des caméras et des détecteurs de métaux.

Conception et provenance du matériel

Un centre de données Google se compose de milliers de serveurs connectés à un réseau local. Les cartes serveur et l'équipement réseau sont conçus sur mesure par Google. Nous examinons les fournisseurs de composants avec lesquels nous travaillons et choisissons les composants avec soin, tout en travaillant avec les fournisseurs pour auditer et valider les propriétés de sécurité fournies par les composants. Nous concevons également des puces personnalisées, notamment une puce de sécurité matérielle actuellement déployée sur les serveurs et les périphériques. Ces puces nous permettent d'identifier et d'authentifier en toute sécurité les appareils Google légitimes au niveau matériel.

Pile de démarrage sécurisée et identité de la machine

Les serveurs Google utilisent diverses technologies pour garantir qu'ils démarrent la bonne pile logicielle. Nous utilisons des signatures cryptographiques sur des composants de bas niveau tels que le BIOS, le chargeur de démarrage, le noyau et l'image de base du système d'exploitation. Ces signatures peuvent être validées lors de chaque démarrage ou mise à jour.
Les composants sont tous contrôlés, construits et renforcés par Google. Avec chaque nouvelle génération de matériel, nous nous efforçons d'améliorer continuellement la sécurité : par exemple, en fonction de la génération de conception du serveur, nous enracinons la confiance de la chaîne de démarrage soit dans une puce de micrologiciel verrouillable, soit dans un microcontrôleur exécutant un code de sécurité écrit par Google, soit dans le puce de sécurité conçue par Google mentionnée ci-dessus.

Chaque machine serveur du centre de données possède sa propre identité spécifique qui peut être liée à la racine matérielle de confiance et au logiciel avec lequel la machine a démarré. Cette identité est utilisée pour authentifier les appels d'API vers et depuis les services de gestion de bas niveau sur la machine.

Google a créé des systèmes automatisés pour garantir que les serveurs exécutent des versions à jour de leurs piles logicielles (y compris les correctifs de sécurité), afin de détecter et

Un centre de données Google se compose de milliers de machines serveurs connecté à un local réseau. Les deux cartes de serveur et les les équipements réseau sont conçus sur mesure par Google.

Nous utilisons l'authentification cryptographique et autorisation au couche applicative pour interservices communication. Cela fournit un contrôle d'accès fort à un niveau d'abstraction et granularité que les administrateurs et les services peuvent naturellement comprendre.

diagnostiquer les problèmes matériels et logiciels et mettre les machines hors service si nécessaire.

Déploiement de services sécurisés

Nous allons maintenant décrire comment nous passons du matériel et des logiciels de base pour garantir qu'un service est déployé en toute sécurité sur notre infrastructure. Par « service », nous entendons un binaire d'application qu'un développeur a écrit et souhaite exécuter sur notre infrastructure, par exemple un serveur SMTP Gmail, un serveur de stockage BigTable, un transcodeur vidéo YouTube ou un bac à sable App Engine exécutant une application client. Il peut y avoir des milliers de machines exécutant des copies du même service pour gérer l'échelle requise de la charge de travail. Les services exécutés sur l'infrastructure sont contrôlés par un service d'orchestration de cluster appelé Borg.

Comme nous le verrons dans cette section, l'infrastructure n'assume aucune confiance entre les services exécutés sur l'infrastructure. En d'autres termes, l'infrastructure est fondamentalement conçue pour être multi-tenant.

Identité, intégrité et isolement du service

Nous utilisons l'authentification et l'autorisation cryptographiques au niveau de la couche application pour la communication interservices. Cela fournit un contrôle d'accès fort à un niveau d'abstraction et une granularité que les administrateurs et les services peuvent naturellement comprendre.

Nous ne nous appuyons pas sur la segmentation du réseau interne ou sur le pare-feu comme principaux mécanismes de sécurité, bien que nous utilisions le filtrage des entrées et des sorties à divers points de notre réseau pour empêcher l'usurpation d'adresse IP comme couche de sécurité supplémentaire. Cette approche nous aide également à maximiser les performances et la disponibilité de notre réseau.

Chaque service qui s'exécute sur l'infrastructure est associé à un compte de service identité. Un service reçoit des informations d'identification cryptographiques qu'il peut utiliser pour prouver son identité lors de l'émission ou de la réception d'appels de procédure à distance (RPC) vers d'autres services. Ces identités sont utilisées par les clients pour garantir qu'ils parlent au bon serveur prévu, et par les serveurs pour limiter l'accès aux méthodes et aux données à des clients particuliers.

Le code source de Google est stocké dans un référentiel central où les versions actuelles et passées du service sont vérifiables. L'infrastructure peut en outre être configurée pour exiger que les binaires d'un service soient construits à partir d'un code source spécifique examiné, archivé et testé. De telles révisions de code nécessitent l'inspection et l'approbation d'au moins un ingénieur autre que l'auteur, et le système impose que les modifications de code apportées à tout système doivent être approuvées par les propriétaires de ce système. Ces exigences limitent la capacité d'un interne ou d'un adversaire à apporter des modifications malveillantes au code source et fournissent également une trace médico-légale depuis un service jusqu'à sa source.

Nous disposons de diverses techniques d'isolation et de sandboxing pour protéger un service des autres services exécutés sur la même machine. Ces techniques incluent la séparation normale des utilisateurs Linux, les bacs à sable basés sur le langage et le noyau, ainsi que la virtualisation matérielle. En général, nous utilisons davantage de couches d'isolation pour les charges de travail plus risquées ; par exemple, lors de l'exécution de convertisseurs de formats de fichiers complexes sur des données fournies par l'utilisateur ou lors de l'exécution de code fourni par l'utilisateur pour des produits tels que Google App Engine ou Google Compute Engine. Comme limite de sécurité supplémentaire, nous permettons aux services très sensibles, tels que le service d'orchestration de cluster et certains services de gestion de clés, de s'exécuter exclusivement sur des machines dédiées.

Gestion des accès interservices

Le propriétaire d'un service peut utiliser les fonctionnalités de gestion des accès fournies par l'infrastructure pour spécifier exactement quels autres services peuvent communiquer avec lui. Par exemple, un service peut vouloir proposer certaines API uniquement à une liste blanche spécifique d'autres services. Ce service peut être configuré avec la liste blanche des identités de compte de service autorisées et cette restriction d'accès est ensuite automatiquement appliquée par l'infrastructure.

Le propriétaire d'un service peut utiliser les fonctionnalités de gestion des accès fournies par l'infrastructure pour préciser exactement quels autres services peuvent communiquer avec lui.

Les ingénieurs Google qui accèdent aux services reçoivent également des identités individuelles, de sorte que les services peuvent être configurés de la même manière pour autoriser ou refuser leurs accès. Tous ces types d'identités (machine, service et employé) se trouvent dans un espace de noms global géré par l'infrastructure. Comme cela sera expliqué plus loin dans ce document, les identités des utilisateurs finaux sont traitées séparément.

L'infrastructure fournit un riche système de flux de travail de gestion des identités pour ces identités internes, y compris les chaînes d'approbation, la journalisation et les notifications. Par exemple, ces identités peuvent être attribuées à des groupes de contrôle d'accès via un système qui permet un contrôle à deux parties où un ingénieur peut proposer une modification à un groupe qu'un autre ingénieur (qui est également un administrateur du groupe) doit approuver. Ce système permet aux processus de gestion des accès sécurisés de s'adapter aux milliers de services exécutés sur l'infrastructure.

En plus du mécanisme de contrôle d'accès automatique au niveau de l'API, l'infrastructure offre également aux services la possibilité de lire à partir des bases de données centrales d'ACL et de groupe afin qu'ils puissent mettre en œuvre leur propre contrôle d'accès personnalisé et précis si nécessaire.

Cryptage des communications interservices

Au-delà des capacités d'authentification et d'autorisation RPC évoquées dans les sections précédentes, l'infrastructure assure également la confidentialité et l'intégrité cryptographiques des données RPC sur le réseau. Pour offrir ces avantages en matière de sécurité à d'autres protocoles de couche application tels que HTTP, nous les encapsulons dans les mécanismes RPC de notre infrastructure. Essentiellement, cela permet d'isoler la couche application et supprime toute dépendance à l'égard de la sécurité du chemin réseau. Les communications interservices cryptées peuvent rester sécurisées même si le réseau est exploité ou si un périphérique réseau est compromis.

Les services peuvent configurer le niveau de protection cryptographique qu'ils souhaitent pour chaque RPC d'infrastructure (par exemple, configurer uniquement la protection de niveau d'intégrité pour les données de faible valeur à l'intérieur des centres de données). Pour vous protéger contre des adversaires sophistiqués qui pourraient tenter d'exploiter nos liaisons WAN privées, l'infrastructure chiffre automatiquement tout le trafic RPC de l'infrastructure qui transite sur le WAN entre les centres de données, sans nécessiter aucune configuration explicite de la part du service. Nous avons commencé à déployer des accélérateurs cryptographiques matériels qui nous permettront d'étendre ce chiffrement par défaut à tout le trafic RPC de l'infrastructure au sein de nos centres de données.

Gestion des accès aux données des utilisateurs finaux

Un service Google typique est écrit pour faire quelque chose pour un utilisateur final. Par exemple, un utilisateur final peut stocker son courrier électronique sur Gmail. L'interaction de l'utilisateur final avec une application telle que Gmail s'étend à d'autres services au sein de l'infrastructure. Ainsi, par exemple, le service Gmail peut appeler une API fournie par le service Contacts pour accéder au carnet d'adresses de l'utilisateur final.

Nous avons vu dans la section précédente que le service Contacts peut être configuré de telle sorte que les seules requêtes RPC autorisées proviennent du service Gmail (ou de tout autre service particulier souhaité par le service Contacts). permettre).

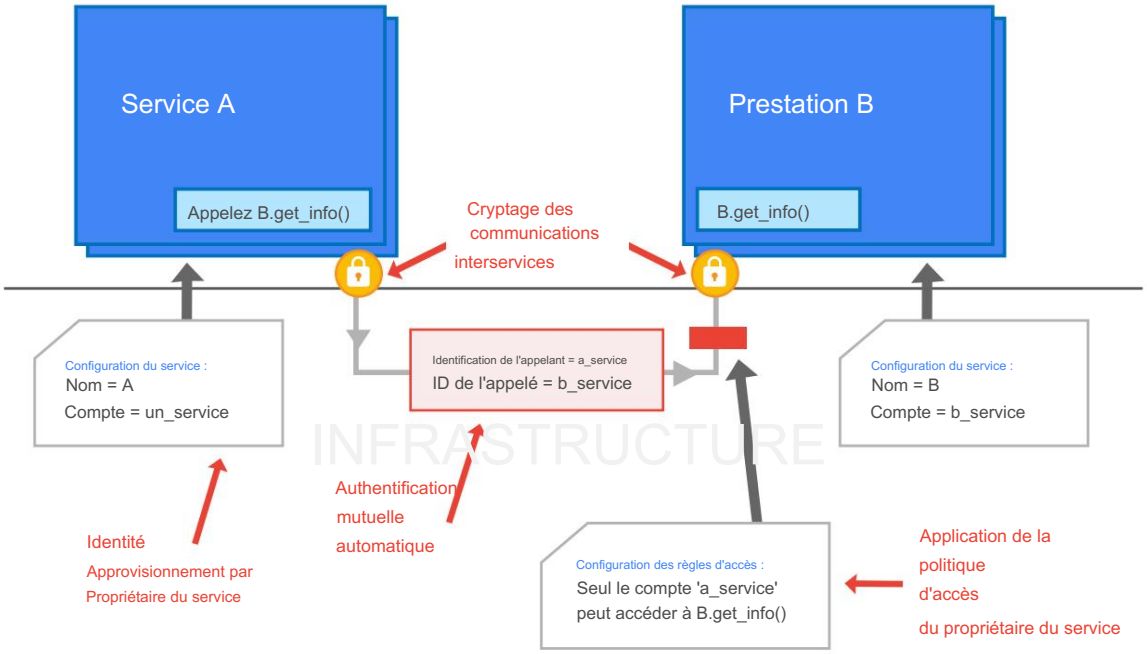
Il s'agit toutefois d'un ensemble très large d'autorisations. Dans le cadre de cette autorisation, le service Gmail serait en mesure de demander les contacts de n'importe quel utilisateur à tout moment.

Étant donné que le service Gmail envoie une requête RPC au service Contacts au nom d'un utilisateur final particulier, l'infrastructure offre au service Gmail la possibilité de présenter un « ticket d'autorisation de l'utilisateur final » dans le cadre du RPC. Ce ticket prouve que le service Gmail traite actuellement une demande au nom de cet utilisateur final particulier. Cela permet au service Contacts de mettre en œuvre une protection selon laquelle il renvoie uniquement les données de l'utilisateur final nommé dans le ticket.

L'infrastructure fournit un service central d'identité des utilisateurs qui émet ces « tickets d'autorisation de l'utilisateur final ». La connexion d'un utilisateur final est vérifiée par le service d'identité central qui délivre ensuite un identifiant d'utilisateur, tel qu'un cookie ou un jeton OAuth, au périphérique client de l'utilisateur. Chaque demande ultérieure de l'appareil client vers Google doit présenter ces informations d'identification utilisateur.

Lorsqu'un service reçoit un identifiant d'utilisateur final, il transmet l'identifiant au service d'identité central pour vérification. Si les informations d'identification de l'utilisateur final sont correctement vérifiées, le service d'identité central renvoie un « ticket d'autorisation de l'utilisateur final » de courte durée qui peut être utilisé pour les RPC liés à la demande. Dans notre exemple, le service qui obtient le « ticket d'autorisation de l'utilisateur final » serait le service Gmail, qui le transmettrait au service Contacts. À partir de ce moment, pour tout appel en cascade, le « ticket d'autorisation de l'utilisateur final » peut être transmis par le service appelant à l'appelé dans le cadre de l'appel RPC.

Pour vous protéger contre des adversaires sophistiqués qui pourraient tenter d'exploiter nos liaisons WAN privées, l'infrastructure chiffre automatiquement tous les RPC de l'infrastructure trafic qui transite sur le WAN entre centres de données.



Graphique 2.
Gestion des identités et des accès aux services :
L'infrastructure fournit l'identité du service, l'authentification mutuelle automatique, la communication interservices cryptée et l'application des politiques d'accès définies par le propriétaire du service.

Stockage sécurisé des données

Jusqu'à présent dans la discussion, nous avons décrit comment nous déployons les services en toute sécurité. Nous passons maintenant à la manière dont nous mettons en œuvre un stockage sécurisé des données sur l'infrastructure.

Chiffrement au repos

L'infrastructure de Google fournit une variété de services de stockage, tels que BigTable et Spanner, ainsi qu'un service central de gestion des clés. La plupart des applications de Google accèdent indirectement au stockage physique via ces services de stockage. Les services de stockage peuvent être configurés pour utiliser les clés du service central de gestion des clés pour chiffrer les données avant qu'elles ne soient écrites sur le stockage physique. Ce service de gestion de clés prend en charge la rotation automatique des clés, fournit des journaux d'audit complets et s'intègre aux tickets d'autorisation des utilisateurs finaux mentionnés précédemment pour lier les clés à des utilisateurs finaux particuliers.

Le chiffrement au niveau de la couche application permet à l'infrastructure de s'isoler des menaces potentielles aux niveaux inférieurs du stockage, telles que les micrologiciels de disque malveillants. Cela dit, l'infrastructure met également en œuvre des couches de protection supplémentaires. Nous permettons la prise en charge du chiffrement matériel sur nos disques durs et SSD et suivons méticuleusement chaque disque tout au long de son cycle de vie. Avant qu'un périphérique de stockage crypté mis hors service puisse physiquement quitter notre garde, il est nettoyé à l'aide d'un processus en plusieurs étapes qui comprend deux vérifications indépendantes. Les appareils qui ne réussissent pas cette procédure d'effacement sont physiquement détruits (par exemple déchiquetés) sur site.

Suppression des données

La suppression des données chez Google commence le plus souvent par le marquage de données spécifiques comme « planifiées pour suppression » plutôt que par la suppression totale des données. Cela nous permet de récupérer des suppressions involontaires, qu'elles soient initiées par le client ou dues à un bug ou à une erreur de processus en interne. Après avoir été marquées comme « suppression planifiée », les données sont supprimées conformément aux politiques spécifiques au service.

Lorsqu'un utilisateur final supprime l'intégralité de son compte, l'infrastructure informe les services gérant les données de l'utilisateur final que le compte a été supprimé. Les services peuvent ensuite planifier les données associées au compte d'utilisateur final supprimé pour suppression.

Le Google Front End garantit que tous les TLS les connexions sont terminé à l'aide de certificats corrects et suivre les meilleures pratiques telles que la prise en charge d'une confidentialité parfaite.

Communication Internet sécurisée

Jusqu'à présent dans ce document, nous avons décrit comment nous sécurisons les services sur notre infrastructure. Dans cette section, nous décrivons comment nous sécurisons la communication entre Internet et ces services.

Comme indiqué précédemment, l'infrastructure se compose d'un vaste ensemble de machines physiques interconnectées via le LAN et le WAN et la sécurité de la communication interservices ne dépend pas de la sécurité du réseau.
Cependant, nous isolons notre infrastructure d'Internet dans un espace IP privé afin de pouvoir plus facilement mettre en œuvre des protections supplémentaires telles que des défenses contre les attaques par déni de service (DoS) en exposant uniquement un sous-ensemble de machines directement au trafic Internet externe.

Service frontal Google

Lorsqu'un service souhaite se rendre disponible sur Internet, il peut s'enregistrer auprès d'un service d'infrastructure appelé Google Front End (GFE). Le GFE garantit que toutes les connexions TLS sont terminées à l'aide de certificats corrects et en suivant les meilleures pratiques telles que la prise en charge d'une parfaite confidentialité de transmission. Le GFE applique en outre des protections contre les attaques par déni de service (dont nous parlerons plus en détail plus tard). Le GFE transmet ensuite les demandes de service en utilisant le protocole de sécurité RPC évoqué précédemment.

En effet, tout service interne qui choisit de se publier en externe utilise le GFE comme interface intelligente de proxy inverse. Ce frontal fournit un hébergement IP public de son nom DNS public, une protection contre le déni de service (DoS) et une terminaison TLS.
Notez que les GFE s'exécutent sur l'infrastructure comme n'importe quel autre service et ont donc la capacité de s'adapter aux volumes de requêtes entrantes.

Protection contre le déni de service (DoS)

L'ampleur de notre infrastructure permet à Google d'absorber simplement de nombreuses attaques DoS. Cela dit, nous disposons de protections DoS multiniveaux et multicouches qui réduisent encore davantage le risque de tout impact DoS sur un service exécuté derrière un GFE.

Une fois que notre backbone fournit une connexion externe à l'un de nos centres de données, celle-ci passe par plusieurs couches d'équilibrage de charge matérielle et logicielle. Ces équilibreurs de charge transmettent des informations sur le trafic entrant à un service DoS central exécuté sur l'infrastructure. Lorsque le service DoS central détecte qu'une attaque DoS a lieu, il peut configurer les équilibreurs de charge pour abandonner ou limiter le trafic associé à l'attaque.

Au niveau de la couche suivante, les instances GFE rapportent également des informations sur les demandes qu'elles reçoivent au service DoS central, y compris des informations sur la couche application dont les équilibreurs de charge ne disposent pas. Le service DoS central peut alors configurez également les instances GFE pour abandonner ou limiter le trafic d'attaque.

Authentification utilisateur

Après la protection DoS, la couche de défense suivante vient de notre service d'identité central. Ce service se manifeste généralement aux utilisateurs finaux sous la forme de la page de connexion Google. En plus de demander un simple nom d'utilisateur et un mot de passe, le service demande également intelligemment aux utilisateurs des informations supplémentaires en fonction de facteurs de risque, tels que s'ils se sont connectés à partir du même appareil ou d'un emplacement similaire dans le passé. Après avoir authentifié l'utilisateur, le service d'identité émet des informations d'identification telles que des cookies et des jetons OAuth qui peuvent être utilisés pour les appels ultérieurs.

Les utilisateurs ont également la possibilité d'utiliser des seconds facteurs tels que des OTP ou des clés de sécurité résistantes au phishing lors de la connexion. Pour garantir que les avantages vont au-delà de Google, nous avons travaillé au sein de l'alliance FIDO avec plusieurs fournisseurs d'appareils pour développer le 2ème facteur universel (U2F).) norme ouverte. Ces appareils sont désormais disponibles sur le marché et d'autres services Web majeurs nous ont également suivi dans la mise en œuvre du support U2F.

L'ampleur de notre infrastructure permet Google va simplement absorber de nombreuses attaques DoS. Cela dit, nous disposons de protections DoS multiniveaux et multicouches qui réduisent encore davantage le risque de tout impact DoS sur un service exécuté derrière un GFE.

Sécurité opérationnelle

Jusqu'à présent, nous avons décrit comment la sécurité est conçue dans notre infrastructure et avons également décrit certains des mécanismes permettant un fonctionnement sécurisé, tels que les contrôles d'accès sur les RPC.

Nous passons maintenant à la description de la manière dont nous exploitons réellement l'infrastructure en toute sécurité : nous créons des logiciels d'infrastructure en toute sécurité, nous protégeons les machines et les informations d'identification de nos employés, et nous nous défendons contre les menaces pesant sur l'infrastructure, provenant à la fois d'acteurs internes et externes.

Développement de logiciels sécurisé Au-delà des fonctionnalités de contrôle de source central et de révision bipartite décrites précédemment, nous fournissons également des bibliothèques qui empêchent les développeurs d'introduire certaines classes de bogues de sécurité. Par exemple, nous disposons de bibliothèques et de frameworks qui éliminent les vulnérabilités XSS dans les applications Web. Nous disposons également d'outils automatisés pour détecter automatiquement les bogues de sécurité, notamment des fuzzers, des outils d'analyse statique et des scanners de sécurité Web.

En guise de contrôle final, nous utilisons des examens de sécurité manuels qui vont du tri rapide pour les fonctionnalités les moins risquées à des examens approfondis de la conception et de la mise en œuvre pour les fonctionnalités les plus risquées. Ces examens sont effectués par une équipe composée d'experts en sécurité Web, en cryptographie et en sécurité des systèmes d'exploitation. Les révisions peuvent également aboutir à de nouvelles fonctionnalités de bibliothèque de sécurité et à de nouveaux fuzzers qui pourront ensuite être appliqués à d'autres produits futurs.

De plus, nous gérons un programme de récompenses de vulnérabilité dans le cadre duquel nous rémunérons toute personne capable de découvrir et de nous informer de bugs dans notre infrastructure ou nos applications. Nous avons payé plusieurs millions de dollars en récompenses dans ce programme.

Google investit également beaucoup d'efforts dans la recherche d'exploits 0-day et d'autres problèmes de sécurité dans tous les logiciels open source que nous utilisons et dans la remontée de ces problèmes. Par exemple, le bug OpenSSL Heartbleed a été trouvé chez Google et nous sommes le plus grand contributeur de CVE et de corrections de bugs de sécurité pour l'hyperviseur Linux KVM.

Nous gérons une vulnérabilité Programme de récompenses où nous rémunérons toute personne capable de d

et informez-nous des bugs de notre infrastructure ou des candidatures.

Assurer la sécurité des appareils et des identifiants des employés

Nous investissons massivement dans la protection des appareils et des informations d'identification de nos employés contre toute compromission, ainsi que dans la surveillance des activités afin de découvrir d'éventuelles compromissions ou des activités internes illicites. Il s'agit d'un élément essentiel de notre investissement pour garantir que notre infrastructure est exploitée en toute sécurité.

Le phishing sophistiqué est un moyen persistant de cibler nos employés. Pour nous prémunir contre cette menace, nous avons remplacé les seconds facteurs OTP phishables par l'utilisation obligatoire de clés de sécurité compatibles U2F pour les comptes de nos employés.

Nous investissons beaucoup dans la surveillance des appareils clients que nos employés utilisent pour faire fonctionner notre infrastructure. Nous veillons à ce que les images du système d'exploitation de ces appareils clients soient à jour avec les correctifs de sécurité et nous contrôlons les applications qui peuvent être installées. Nous disposons également de systèmes pour analyser les applications installées par les utilisateurs, les téléchargements, les extensions de navigateur et le contenu consulté sur le Web pour vérifier leur adéquation aux clients d'entreprise.

Être sur le réseau local de l'entreprise n'est pas notre principal mécanisme pour accorder des privilèges d'accès. Nous utilisons plutôt des contrôles de gestion des accès au niveau des applications qui nous permettent d'exposer les applications internes à des utilisateurs spécifiques uniquement lorsqu'elles proviennent d'un appareil correctement géré et des réseaux et emplacements géographiques attendus. (Pour plus de détails, consultez notre lecture supplémentaire sur « BeyondCorp ».)

Réduire les risques internes

Nous limitons de manière agressive et surveillons activement les activités des employés qui ont obtenu un accès administratif à l'infrastructure et travaillons continuellement à éliminer le besoin d'accès privilégié pour des tâches particulières en fournissant une automatisation capable d'accomplir les mêmes tâches de manière sûre et contrôlée.

Cela inclut l'exigence d'approbations bipartites pour certaines actions et l'introduction d'API limitées qui permettent le débogage sans exposer d'informations sensibles.

L'accès des employés de Google aux informations sur les utilisateurs finaux peut être enregistré via des hooks d'infrastructure de bas niveau. L'équipe de sécurité de Google surveille activement les modèles d'accès et enquête sur les événements inhabituels.

Détection d'intrusion

Google dispose de pipelines de traitement de données sophistiqués qui intègrent des signaux basés sur l'hôte sur des appareils individuels, des signaux basés sur le réseau provenant de divers points de surveillance de l'infrastructure et des signaux provenant des services d'infrastructure. Les règles et l'intelligence artificielle construites au-dessus de ces pipelines avertissent les ingénieurs de sécurité opérationnelle d'incidents possibles. Nos équipes d'enquête et de réponse aux incidents trient, enquêtent et répondent à ces incidents potentiels 24 heures sur 24, 365 jours par an. Nous menons des exercices Red Team pour mesurer et améliorer l'efficacité de nos mécanismes de détection et de réponse.

Règles et machine les renseignements construits au-dessus des pipelines de surveillance des signaux avertissent les ingénieurs de sécurité opérationnels d'incidents possibles.

Sécuriser le cloud Google Plateforme (GCP)

Dans cette section, nous soulignons comment notre infrastructure de cloud public, GCP, bénéficie de la sécurité de l'infrastructure sous-jacente. Dans cette section, nous prendrons Google Compute Engine (GCE) comme exemple de service et décrirons en détail les améliorations de sécurité spécifiques au service que nous construisons au-dessus de l'infrastructure.

GCE permet aux clients d'exécuter leurs propres machines virtuelles sur l'infrastructure de Google. L'implémentation GCE se compose de plusieurs composants logiques, notamment le plan de contrôle de gestion et les machines virtuelles elles-mêmes.

Le plan de contrôle de gestion expose la surface de l'API externe et orchestre des tâches telles que la création et la migration de machines virtuelles. Il fonctionne comme une variété de services sur l'infrastructure, ce qui lui permet d'obtenir automatiquement des fonctionnalités d'intégrité fondamentales telles qu'une chaîne de démarrage sécurisée. Les services individuels s'exécutent sous des comptes de service internes distincts afin que chaque service puisse se voir accorder uniquement les autorisations dont il a besoin lors des appels de procédure à distance (RPC) vers le reste du plan de contrôle. Comme indiqué précédemment, le code de tous ces services est stocké dans le référentiel central du code source de Google, et il existe une piste d'audit entre ce code et les binaires qui sont finalement déployés.

Le plan de contrôle GCE expose son API via le GFE et profite ainsi des fonctionnalités de sécurité de l'infrastructure telles que la protection contre le déni de service (DoS) et la prise en charge SSL/TLS gérée de manière centralisée. Les clients peuvent bénéficier de protections similaires pour les applications exécutées sur leurs VM GCE en choisissant d'utiliser l'outil Google en option.

Service Cloud Load Balancer qui repose sur GFE et peut atténuer de nombreux types d'attaques DoS.

L'authentification de l'utilisateur final auprès de l'API du plan de contrôle GCE s'effectue via le service d'identité centralisé de Google qui fournit des fonctionnalités de sécurité telles que la détection de piratage. L'autorisation est effectuée à l'aide du service Cloud IAM central.

Le trafic réseau pour le plan de contrôle, à la fois depuis les GFE vers le premier service derrière lui et entre les autres services du plan de contrôle, est automatiquement authentifié par l'infrastructure et chiffré chaque fois qu'il passe d'un centre de données à un autre. De plus, l'infrastructure a été configurée pour chiffrer également une partie du trafic du plan de contrôle au sein du centre de données.

Chaque machine virtuelle (VM) s'exécute avec une instance de service de gestionnaire de machine virtuelle (VMM) associée. L'infrastructure offre à ces services deux identités. Une identité est utilisée par l'instance de service VMM pour ses propres appels et une autre identité est utilisée pour les appels que le VMM effectue au nom de la machine virtuelle du client. Cela nous permet de segmenter davantage la confiance accordée aux appels provenant du VMM.

Les disques persistants GCE sont chiffrés au repos à l'aide de clés protégées par le système de gestion des clés de l'infrastructure centrale. Cela permet une rotation automatisée et un audit centralisé de l'accès à ces clés.

Le calcul Google Le plan de contrôle Engine (GCE) expose son API via Google Front-end (GFE), et profite donc de l'infrastructure des fonctionnalités de sécurité telles que la protection contre le déni de service (DoS) et la prise en charge SSL/TLS gérée de manière centralisée.

Les clients ont aujourd'hui le choix d'envoyer en clair le trafic de leurs machines virtuelles vers d'autres machines virtuelles ou vers Internet, ou de mettre en œuvre le chiffrement de leur choix pour ce trafic. Nous avons commencé à déployer le chiffrement automatique pour le saut de traversée WAN du trafic VM à VM client. Comme décrit précédemment, tout le trafic WAN du plan de contrôle au sein de l'infrastructure est déjà chiffré. À l'avenir, nous prévoyons de tirer parti du chiffrement réseau accéléré par le matériel évoqué précédemment pour chiffrer également le trafic LAN inter-VM au sein du centre de données.

L'isolation fournie aux machines virtuelles est basée sur la virtualisation matérielle utilisant la pile KVM open source. Nous avons encore renforcé notre implémentation particulière de KVM en déplaçant une partie de la pile de contrôle et d'émulation matérielle vers un processus non privilégié en dehors du noyau. Nous avons également testé de manière approfondie le cœur de KVM à l'aide de techniques telles que le fuzzing, l'analyse statique et la révision manuelle du code. Comme mentionné précédemment, la majorité des vulnérabilités récemment révélées publiquement et intégrées en amont dans KVM provenaient de Google.

Enfin, nos contrôles de sécurité opérationnels sont un élément clé pour garantir que les accès aux données respectent nos politiques. Dans le cadre de Google Cloud Platform, l'utilisation des données client par GCE suit la politique d'utilisation des données client de GCP, à savoir que Google n'accédera pas aux données client ni ne les utilisera, sauf si cela est nécessaire pour fournir des services aux clients.

Conclusion

Nous avons décrit comment l'infrastructure de Google est conçue pour créer, déployer et exploiter des services en toute sécurité à l'échelle d'Internet. Cela inclut à la fois les services grand public tels que Gmail et nos services d'entreprise. De plus, nos offres Google Cloud s'appuient sur cette même infrastructure.

Nous investissons massivement dans la sécurisation de nos infrastructures. Nous disposons de plusieurs centaines d'ingénieurs dédiés à la sécurité et à la confidentialité, répartis dans l'ensemble de Google, dont beaucoup sont des autorités reconnues du secteur.

Nous investissons massivement dans la sécurisation de nos infrastructures. Nous avons plusieurs centaines d'ingénieurs dédiés à la sécurité et à la confidentialité répartis dans tous de Google, dont beaucoup sont des autorités reconnues du secteur.

Comme nous l'avons vu, la sécurité de l'infrastructure est conçue en couches allant des composants physiques et du centre de données à la provenance du matériel, puis au démarrage sécurisé, à la communication interservices sécurisée, aux données sécurisées au repos, à l'accès protégé aux services depuis Internet et enfin, les technologies et les processus humains que nous déployons pour la sécurité opérationnelle.

Lecture supplémentaire

Veuillez consulter les documents suivants pour plus de détails sur des domaines spécifiques :

1. Sécurité physique de nos centres de données
   https://goo.gl/WYIKGG
2. Conception de notre gestion et orchestration de cluster
   http://research.google.com/pubs/pub43438.html
3. Chiffrement du stockage et fonctionnalités de chiffrement GCP destinées aux clients
   https://cloud.google.com/security/encryption-at-rest/
4. Service de stockage BigTable
   http://research.google.com/archive/bigtable.html
5. Service de stockage de clés
   http://research.google.com/archive/spanner.html
6. Architecture de notre équilibrage de charge réseau
   http://research.google.com/pubs/pub44824.html
7. Approche BeyondCorp en matière de sécurité d'entreprise
   http://research.google.com/pubs/pub43231.html

8. Combattre le phishing avec la clé de sécurité et le deuxième facteur universel (U2F) http://research.google.com/pubs/pub45409.html

9. En savoir plus sur le programme Google Vulnerability Rewards https://bughunter.withgoogle.com/

10. En savoir plus sur les HTTP et autres offres d'équilibrage de charge sur GCP https://cloud.google.com/compute/docs/load-balancing/

11. En savoir plus sur les bonnes pratiques en matière de protection DoS sur GCP https://cloud.google.com/files/GCPDDoSprotection-04122016.pdf

12. Politique d'utilisation des données client de Google Cloud Platform https://cloud.google.com/terms/

13. En savoir plus sur la sécurité et la conformité des applications dans G Suite (Gmail, Drive, etc.) https://goo.gl/3J20R2