Tugas Demo GCP 2

Identity Aware Proxy

Disusun Oleh : KELOMPOK 1

Christianus Yoga Wibisono	**(212410101005)**
Moch. Bima Pangestu	**(212410102042)**
Ciko Tegar Saputra	**(212410101041)**
Faith Reyhan	**(222410102082)**
Achmad Azriel Amaldany	**(222410102037)**

KOMPUTASI AWAN

UNIVERSITAS JEMBER

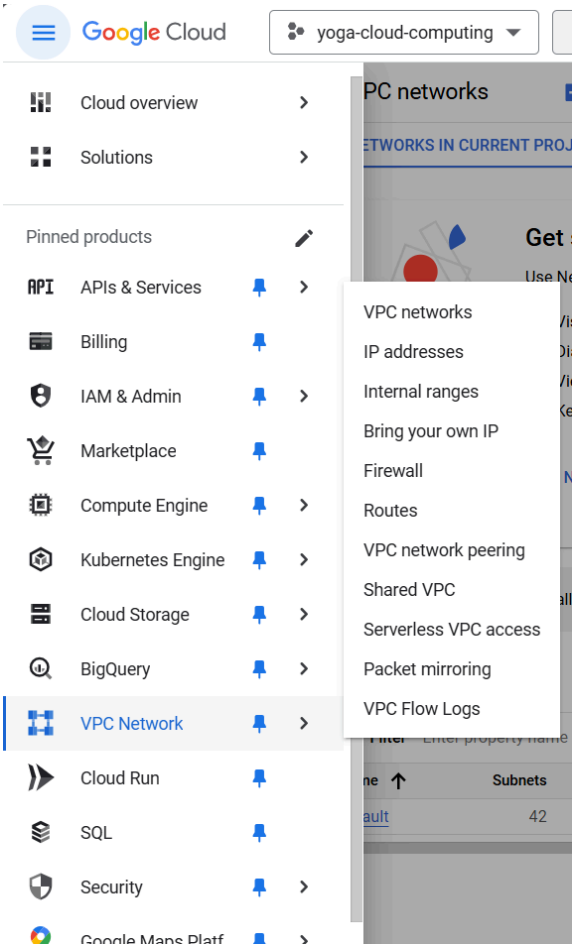
2024

A. **Buat Sebuah Virtual Private Cloud (VPC) pada Google Cloud platform dengan ketentuan sebagai berikut :**

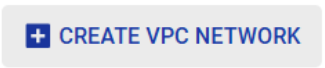
1. **Nama VPC : vpc-test-kelompok1**
2. **Pada bagian subnet Set nama dengan “subnet-test”**
3. **Region pilih southeast asia**
4. **Set Alamat IP random xxx.xxx.xxx.xxx/20**

Demo :

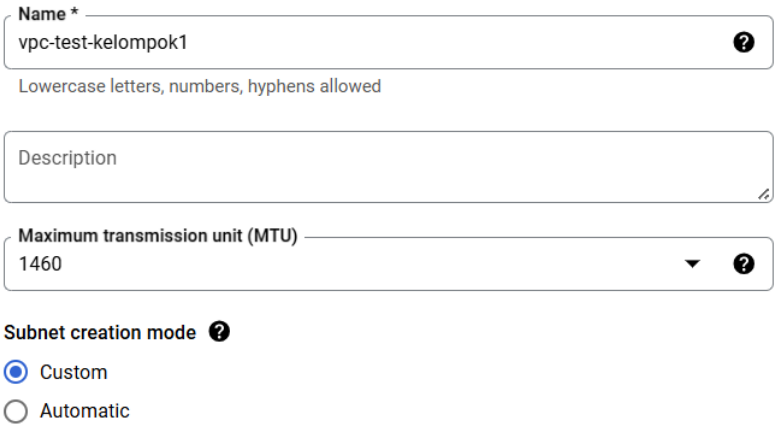
1. **Klik hamburger menu kamudian pilih PVC network**



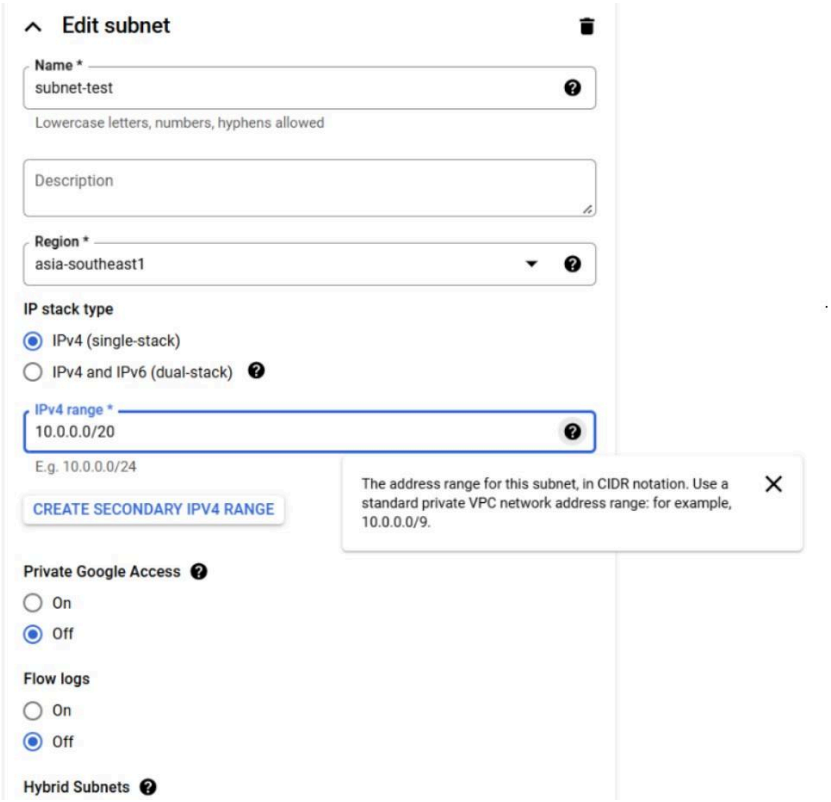
2. **Click “CREATE VPC NETWORK”**



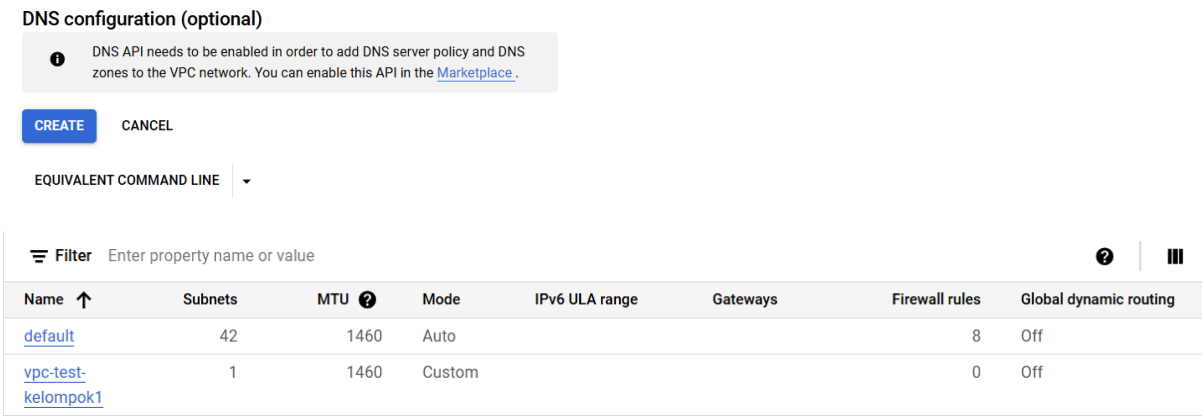
3. **Isi sesuai nama VPC network dengan “vpc-test-kelompok1” dan set Subnet ke Custom**



4. **Atur Subnet sesuai dengan ketentuan**



5. **Click Create dan VPC sudah berhasil dibuat**

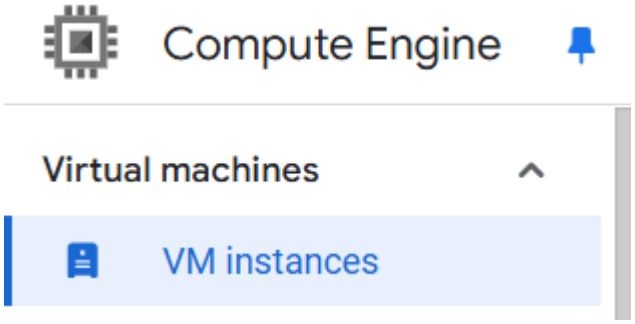


B. Buat sebuah VM dengan ketentuan sebagai berikut :

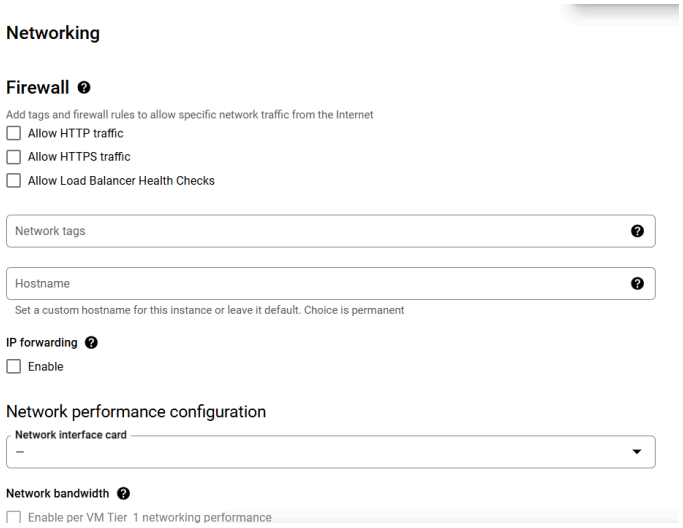
1. **Nama VM: iap-testing-kelompok**
2. **Unchecklist semua pada Bagian Firewall**
3. **Pada bagian advance option, set network interface ke “vpc-test”**
4. **Kosongkan IP eksternal**

Demo :

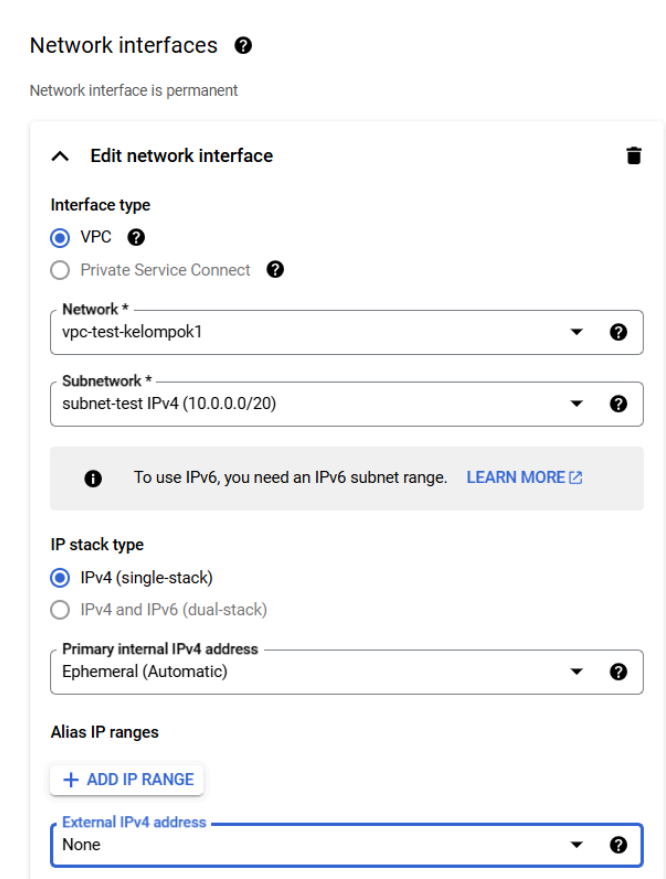
1. **Click VM instance**



2. **Unchecklist semua pada Bagian Firewall**



3. **Pada bagian advance option, set network interface ke “vpc-test” dan Kosongkan IP eksternal**



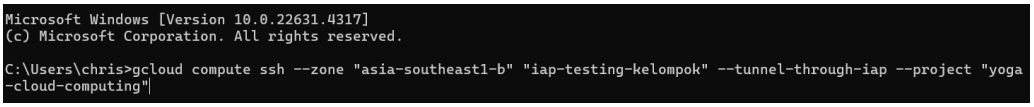
C. Slide 3

1. **Run VM yang sudah dibuat**

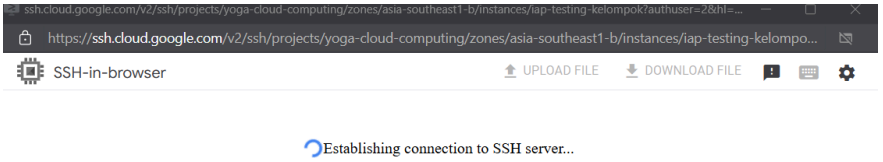
2. **Masuk kedalam VM dengan SSH atau dengan command gcloud compute ssh --zone "server_zone" "iap-testing" --project "project_name" pada CLI, Apa yang akan terjadi dan berikan penjelasan mengapa hal tersebut bisa terjadi ?**

   Demo :

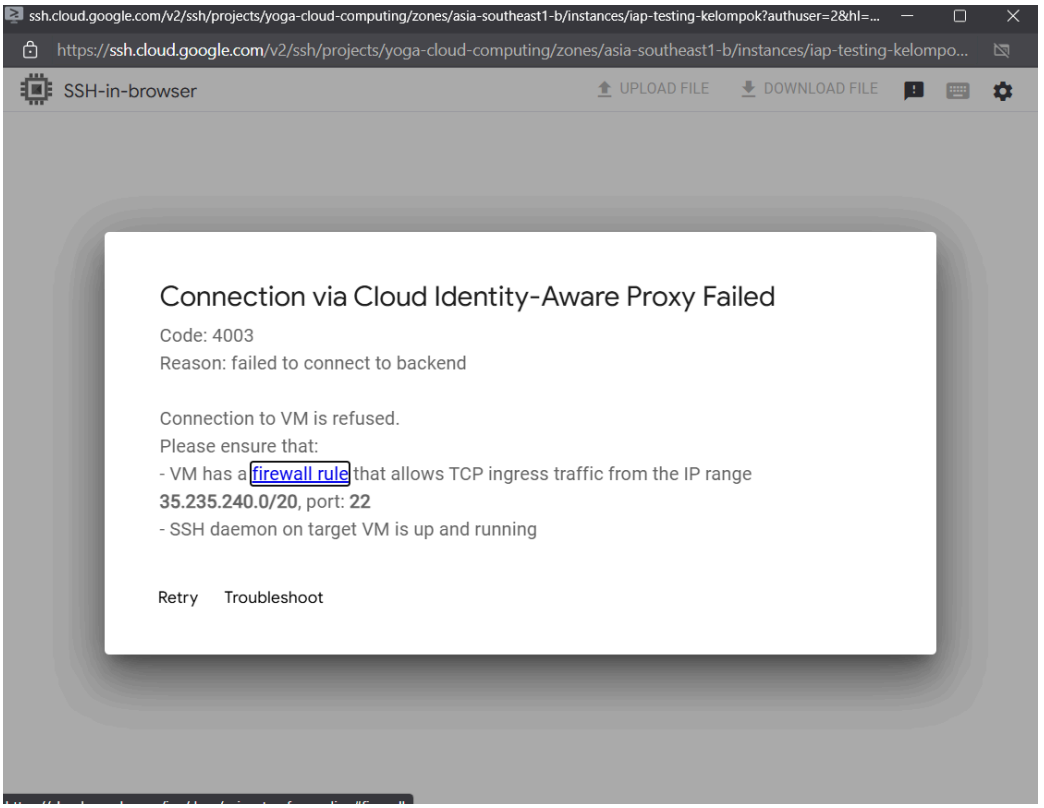
   1. **Masuk CLI dan masukkan command**



2. **Tunggu**



3. **Muncul alert Failed**



4. **Penjelasan**

Hal ini disebabkan oleh:

Firewall default dari GCP yang secara otomatis memblokir koneksi SSH masuk jika aturan firewall tidak diatur. Tidak adanya IP eksternal berarti VM

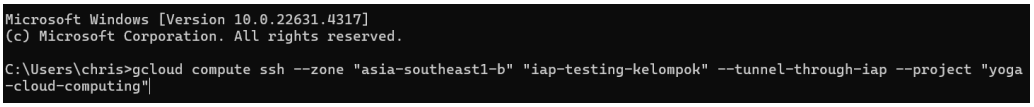
hanya dapat diakses dari dalam jaringan VPC itu sendiri, atau melalui metode seperti Identity-Aware Proxy (IAP) jika diaktifkan.

D. Slide 4

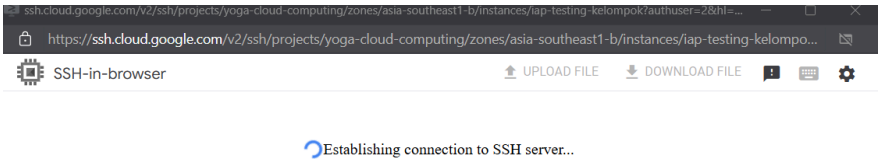
1. **Masuk kedalam VM dengan SSH atau dengan command gcloud compute ssh --zone "server_zone" "iap-testing" --project "project_name" pada CLI, Apa yang akan terjadi dan berikan penjelasan mengapa hal tersebut bisa terjadi ?**

   Demo :

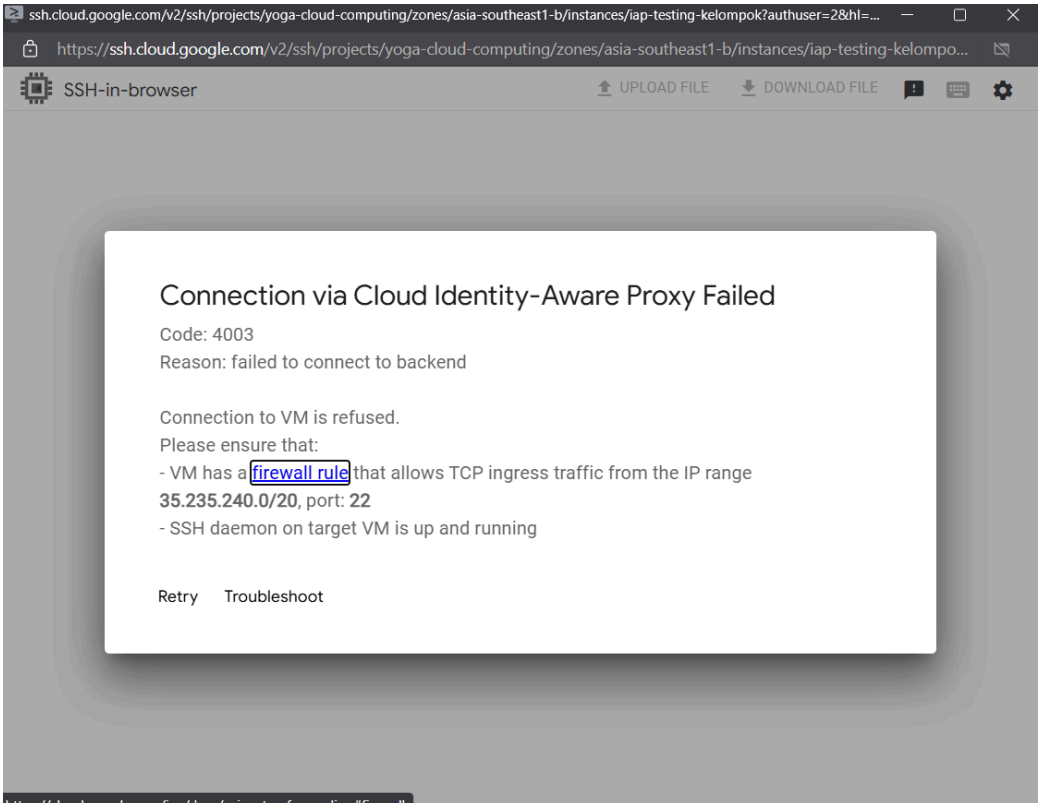
   1. **Masuk CLI dan masukkan command**



   2. **Tunggu**



3. **Muncul alert Failed**



4. **Penjelasan**

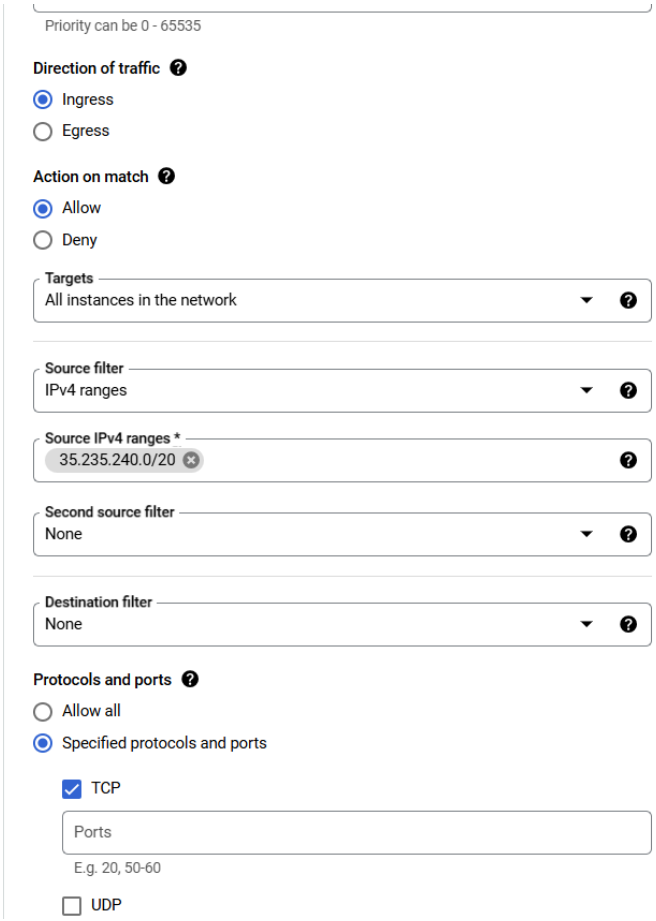
   Hal ini disebabkan oleh:

   Firewall default dari GCP yang secara otomatis memblokir koneksi SSH masuk jika aturan firewall tidak diatur. Tidak adanya IP eksternal berarti VM hanya dapat diakses dari dalam jaringan VPC itu sendiri, atau melalui metode seperti Identity-Aware Proxy (IAP) jika diaktifkan.

2. **Masuk pada VPC yang sudah dibuat diawal “vpc-test”**
3. **Tambahkan rule pada firewall**
4. **Masukkan range IPv4 35.235.240.0/20**
5. **set protocol ke TCP only**

   Demo :

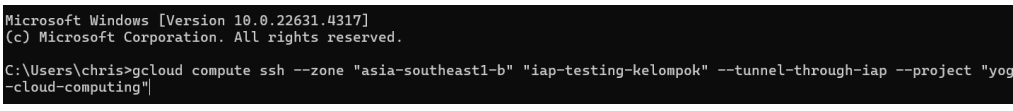
a. **Lakukan sesuai perintah diatas**



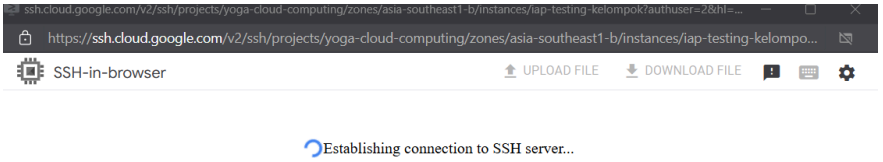
6. **Coba masuk ke dalam VM Kembali, Jelaskan tentang kondisi apa yang terjadi.**

   Demo :

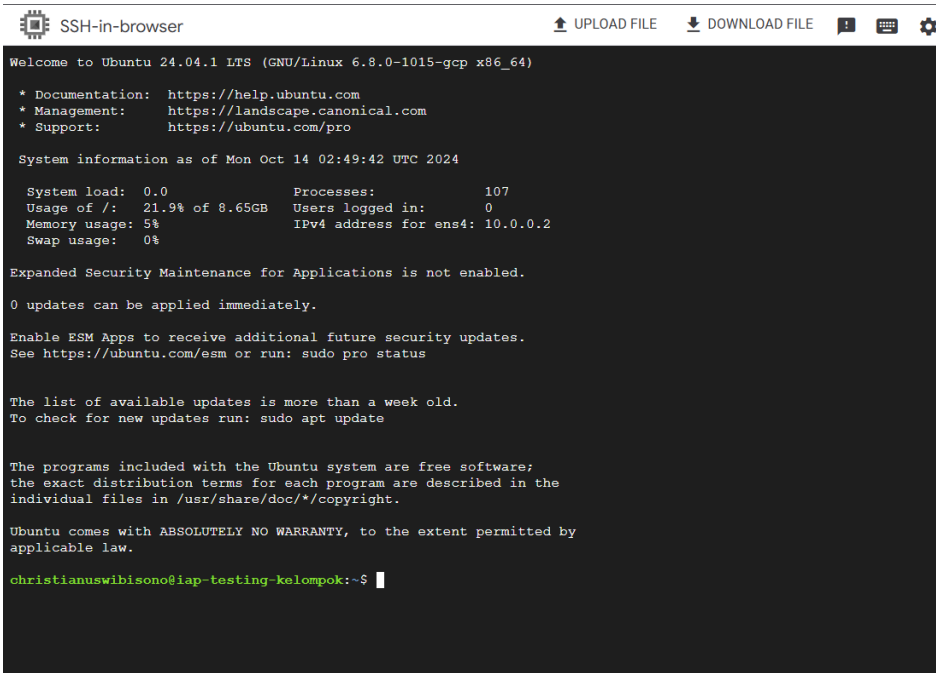
   a. **Masuk CLI dan masukkan command**



b. Tunggu



c. Selesai



d. Penjelasan

Setelah masuk ke VPC vpc-test-kelompok1 dan menambahkan aturan firewall baru dengan:

- Range IPv4: 35.235.240.0/20 (IP range untuk akses IAP).
- Protocol: TCP (untuk protokol SSH).

Kondisi yang terjadi setelah penambahan firewall rule:

- Setelah aturan firewall ini ditambahkan, kita bisa mengakses VM melalui SSH menggunakan perintah di atas. Ini karena:
- IAP (Identity-Aware Proxy) di GCP memungkinkan kita mengakses VM meskipun tidak memiliki IP eksternal, dengan memanfaatkan IP internal dan mengatur akses melalui firewall khusus. IP range 35.235.240.0/20 digunakan oleh IAP, sehingga setelah menambahkan aturan ini, koneksi SSH melalui IAP berhasil.

Penjelasan Mengapa Hal Ini Terjadi:

- Tanpa IP Eksternal: VM tidak bisa diakses secara langsung dari internet karena tidak ada IP eksternal, yang artinya hanya bisa diakses dari dalam VPC atau melalui metode seperti IAP.

Firewall Default: GCP secara default memblokir koneksi masuk kecuali diatur melalui aturan firewall. Karena itu, tanpa menambahkan aturan untuk mengizinkan koneksi SSH, akses ke VM akan terblokir.

Dengan IAP: Menambahkan aturan firewall untuk range IP IAP (35.235.240.0/20) memungkinkan koneksi SSH ke VM meskipun tanpa IP eksternal, karena IAP menyediakan cara aman untuk mengakses VM dari internet melalui jaringan internal.

E. Analisis Slide 3

- Percobaan Masuk VM melalui SSH (tanpa Firewall Rule):
  Saat mencoba mengakses VM melalui SSH menggunakan perintah:
  bash
  Copy code
  gcloud compute ssh --zone "server_zone" "iap-testing" --project "project_name"
  Kondisi yang terjadi: Kita tidak dapat mengakses VM. Hal ini disebabkan oleh:
  Firewall default dari GCP yang secara otomatis memblokir koneksi SSH masuk jika aturan firewall tidak diatur.

  Tidak adanya IP eksternal berarti VM hanya dapat diakses dari dalam jaringan VPC itu sendiri, atau melalui metode seperti Identity-Aware Proxy (IAP) jika diaktifkan.

F. Analisis Slide 4

- **Setelah masuk ke VPC vpc-test-kelompok1 dan menambahkan aturan firewall baru dengan:**
    - Range IPv4: 35.235.240.0/20 (IP range untuk akses IAP).
    - Protocol: TCP (untuk protokol SSH).

  Kondisi yang terjadi setelah penambahan firewall rule:
    - Setelah aturan firewall ini ditambahkan, kita bisa mengakses VM melalui SSH menggunakan perintah di atas. Ini karena:
    - IAP (Identity-Aware Proxy) di GCP memungkinkan kita mengakses VM meskipun tidak memiliki IP eksternal, dengan memanfaatkan IP internal dan mengatur akses melalui firewall khusus. IP range 35.235.240.0/20 digunakan oleh IAP, sehingga setelah menambahkan aturan ini, koneksi SSH melalui IAP berhasil.
-

G. Perbandingan Slide 3 dan Slide 4

- **Pada Slide 3,** akses SSH gagal karena tidak adanya aturan firewall yang memperbolehkan koneksi dari luar, serta tidak adanya IP eksternal.
- **Pada Slide 4,** akses SSH berhasil setelah aturan firewall baru ditambahkan untuk mengizinkan koneksi melalui Identity-Aware Proxy (IAP), meskipun VM tidak memiliki IP eksternal.

Perubahan utama yang dilakukan adalah pengaturan firewall yang memungkinkan IAP untuk memfasilitasi koneksi SSH, yang menjadi solusi utama untuk mengatasi masalah akses yang terjadi pada Slide 3.

H. Perandingan penerapan Identity aware proxy dengan penerapan regular VM pada tugas pertama

perbandingan antara hasil penerapan Identity-Aware Proxy (IAP) dengan Regular VM yang menggunakan IP eksternal dan tanpa VPC khusus:

A. Hasil 3 (IAP dengan Firewall Rule pada VPC):

Keamanan:

- Tanpa IP eksternal: VM dilindungi dari akses langsung dari internet. Koneksi ke VM hanya mungkin melalui jaringan internal (VPC) atau melalui IAP.
- Identity-Aware Proxy (IAP): IAP memberikan akses ke VM secara aman tanpa perlu IP publik. IAP mengharuskan pengguna terotentikasi

menggunakan akun Google yang memiliki izin yang sesuai, yang menambahkan lapisan keamanan tambahan.

- Firewall: Harus ada aturan firewall yang spesifik (seperti IP range 35.235.240.0/20 untuk IAP) agar IAP dapat mengakses VM. Akses langsung melalui IP internal dijamin aman.

Aksesibilitas:

- Akses ke VM hanya melalui IAP atau dari jaringan internal VPC, sehingga lebih aman untuk kasus di mana akses terbatas diperlukan.
- Pengguna harus terhubung dengan Google Cloud CLI atau konsol web untuk menggunakan IAP untuk SSH.

Skalabilitas dan Pengelolaan:

- Penggunaan IAP lebih cocok untuk lingkungan enterprise yang membutuhkan kontrol akses ketat dan log audit yang baik, karena IAP mencatat semua aktivitas pengguna.
- Mudah diintegrasikan dengan kebijakan akses berbasis identitas dan izin yang spesifik untuk setiap pengguna.

B. Hasil 4 (Regular VM tanpa VPC, dengan IP eksternal):

Keamanan:

- IP Eksternal Terbuka: VM yang dibuat secara default dengan IP eksternal akan memiliki akses langsung dari internet, yang membuatnya rentan terhadap serangan jika konfigurasi firewall atau otentikasi tidak diatur dengan baik.
- Firewall: Aturan firewall default akan menentukan apakah koneksi SSH diizinkan, namun ini tetap terbuka ke internet jika ada IP eksternal.

Aksesibilitas:

- VM dapat langsung diakses melalui internet menggunakan SSH dengan IP eksternal tanpa perlu menggunakan IAP.
- Pengguna tidak perlu konfigurasi tambahan seperti pada IAP, akses lebih cepat, dan lebih sederhana, namun dengan risiko keamanan yang lebih tinggi.

Skalabilitas dan Pengelolaan:

- Pengelolaan IP eksternal secara besar-besaran memerlukan lebih banyak perhatian dari segi keamanan. Misalnya, dengan banyak VM menggunakan IP publik, risiko serangan atau kesalahan konfigurasi dapat meningkat.
- Kurang cocok untuk lingkungan enterprise yang memerlukan kontrol akses ketat, karena otentikasi hanya bergantung pada SSH key atau password.