Shape your remote connection to your GCE Instance

By : Mr. Didiet Agus P

DevOps Community in Indonesia

Bandung,29 November 2019

gits indonesia

Secure your remote connection to your GCE Instance

About Me

- DevOps Engineer PT. Gits Indonesia
- Member of openSUSE Project, openSUSE-Id, KLAS, Kubernetes-Id etc
- Cloud Enthusiast
- Contact me :
  - didiet@gits.id
  - pambudiono@opensuse.org

Background

- Web services are still under development and aren't ready to be exposed to external users because they're feature incomplete or haven't yet been configured with HTTPS.
- An instance might be providing services designed to be consumed only by other instances in the project.
- Instances should only be reached through dedicated interconnect options from company offices or data centers.

Two Kind of GCE Instance :

- With External IP addresses
  - With Public IP Address
  - Accessible from internet
- Without External IP addresses
  - No Public IP Address
  - Not accessible from internet

Connecting services on machine with external IP address

- Firewall
- Bastion host and SSH forwarding
- VPN
- HTTPS and SSL
- Multi Factor Authentication

Connecting services on machine without external IP address

- Bastion host and SSH forwarding
- VPN
- HTTPS and SSL proxy load balancers

Firewall

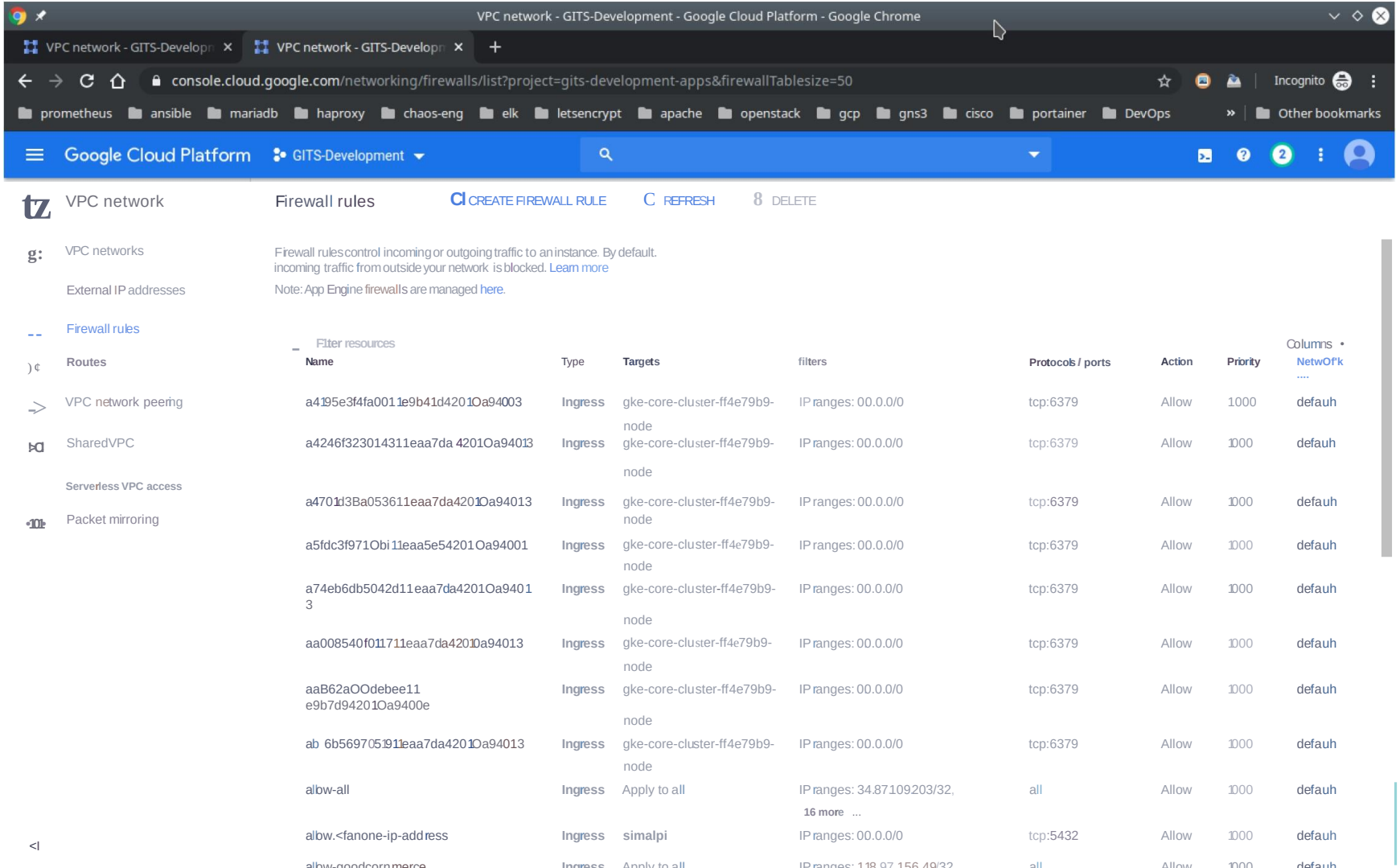
- First line of defense to restrict who can reach the instance.
- By creating firewall rules, we can restrict all traffic to a target machine
- Firewalls aren't a standalone solution. Restricting traffic to specific source IPs doesn't protect sensitive information, such as login credentials, commands that create or destroy resources or files, or logs.
- In addition, firewalls aren't always the appropriate solution. For example, firewalls aren't ideal for development environments that don't have static IP addresses, such as roaming laptops.

VPC (Virtual Private Cloud) Network

- A Virtual Private Cloud network is a virtual version of a physical network, like a data center network.
- It provides connectivity for Compute Engine virtual machine (VM) instances, Kubernetes Engine clusters, App Engine Flex instances, and other resources in the project.

VPC Specifications

- Traffic to and from instances can be controlled with network firewall rules.
- Resources within a VPC network can communicate with one another using internal (private) IPv4 addresses, subject to applicable network firewall rules.
- VPC networks can be connected to other VPC networks in different projects or organizations by using VPC Network Peering.
- VPC networks can be securely connected in hybrid environments using Cloud VPN or Cloud Interconnect.
- VPC networks only support IPv4 unicast traffic


VPC network - GITS-Development - Google Cloud Platform - Google Chrome
VPC network - GITS-Develop
VPC network - GITS-Develop
console.cloud.google.com/networking/firewalls/list?project=gits-development-apps&firewallTablesize=50
Incognito
prometheus
ansible
mariadb
haproxy
chaos-eng
elk
letsencrypt
apache
openstack
gcp
gns3
cisco
portainer
DevOps
Other bookmarks
Google Cloud Platform
GITS-Development
VPC network
Firewall rules
CREATE FIREWALL RULE
REFRESH
DELETE
VPC networks
External IP addresses
Firewall rules
Routes
VPC network peering
SharedVPC
Serverless VPC access
Packet mirroring
Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more
Note: App Engine firewalls are managed here.
Filter resources
Columns
Name
Type
Targets
filters
Protocols / ports
Action
Priority
Network
a4195e3f4fa0011e9b41d4201Oa94003
Ingress
gke-core-cluster-ff4e79b9-node
IP ranges: 00.0.0/0
tcp:6379
Allow
1000
defauh
a4246f323014311eaa7da 4201Oa94013
Ingress
gke-core-cluster-ff4e79b9-node
IP ranges: 00.0.0/0
tcp:6379
Allow
1000
defauh
a4701d3Ba053611eaa7da4201Oa94013
Ingress
gke-core-cluster-ff4e79b9-node
IP ranges: 00.0.0/0
tcp:6379
Allow
1000
defauh
a5fdc3f971Obi11eaa5e54201Oa94001
Ingress
gke-core-cluster-ff4e79b9-node
IP ranges: 00.0.0/0
tcp:6379
Allow
1000
defauh
a74eb6db5042d11eaa7da4201Oa9401 3
Ingress
gke-core-cluster-ff4e79b9-node
IP ranges: 00.0.0/0
tcp:6379
Allow
1000
defauh
aa008540f011711eaa7da42010a94013
Ingress
gke-core-cluster-ff4e79b9-node
IP ranges: 00.0.0/0
tcp:6379
Allow
1000
defauh
aaB62aOOdebee11 e9b7d94201Oa9400e
Ingress
gke-core-cluster-ff4e79b9-node
IP ranges: 00.0.0/0
tcp:6379
Allow
1000
defauh
ab 6b5697051911eaa7da4201Oa94013
Ingress
gke-core-cluster-ff4e79b9-node
IP ranges: 00.0.0/0
tcp:6379
Allow
1000
defauh
allow-all
Ingress
Apply to all
IP ranges: 34.87109203/32, 16 more ...
all
Allow
1000
defauh
allow.<fanone-ip-address
Ingress
simalpi
IP ranges: 00.0.0/0
tcp:5432
Allow
1000
defauh

DMZ or Demilitarized Zone

- a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.
- The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN):
- an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled.
- The DMZ functions as a small, isolated network positioned between the Internet and the private network.

Bastion Host

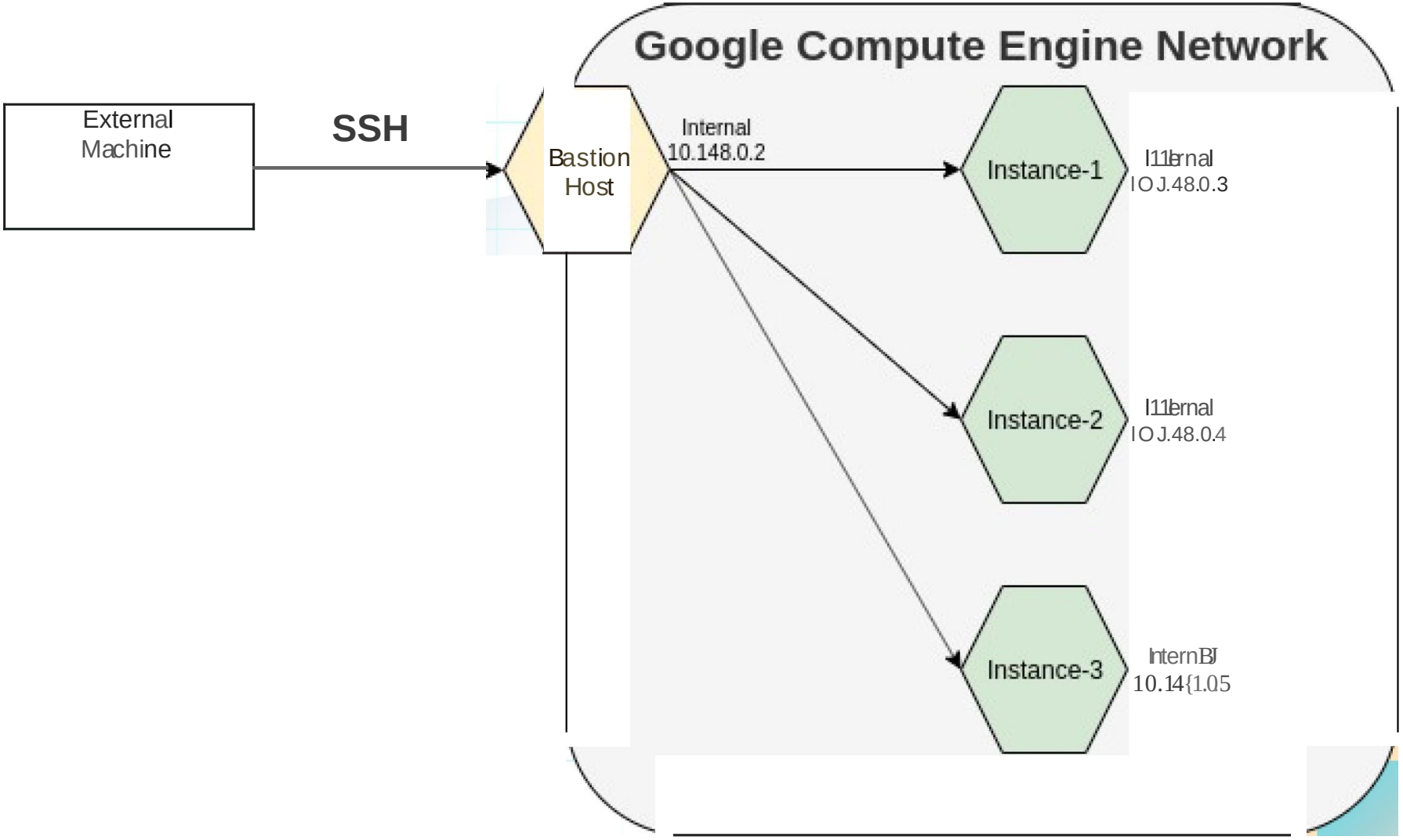
- a system identified by the firewall administrator as a critical strong point in the network security.
- Generally, bastion hosts will have some degree of extra attention paid to their security, may undergo regular audits, and may have modified software.

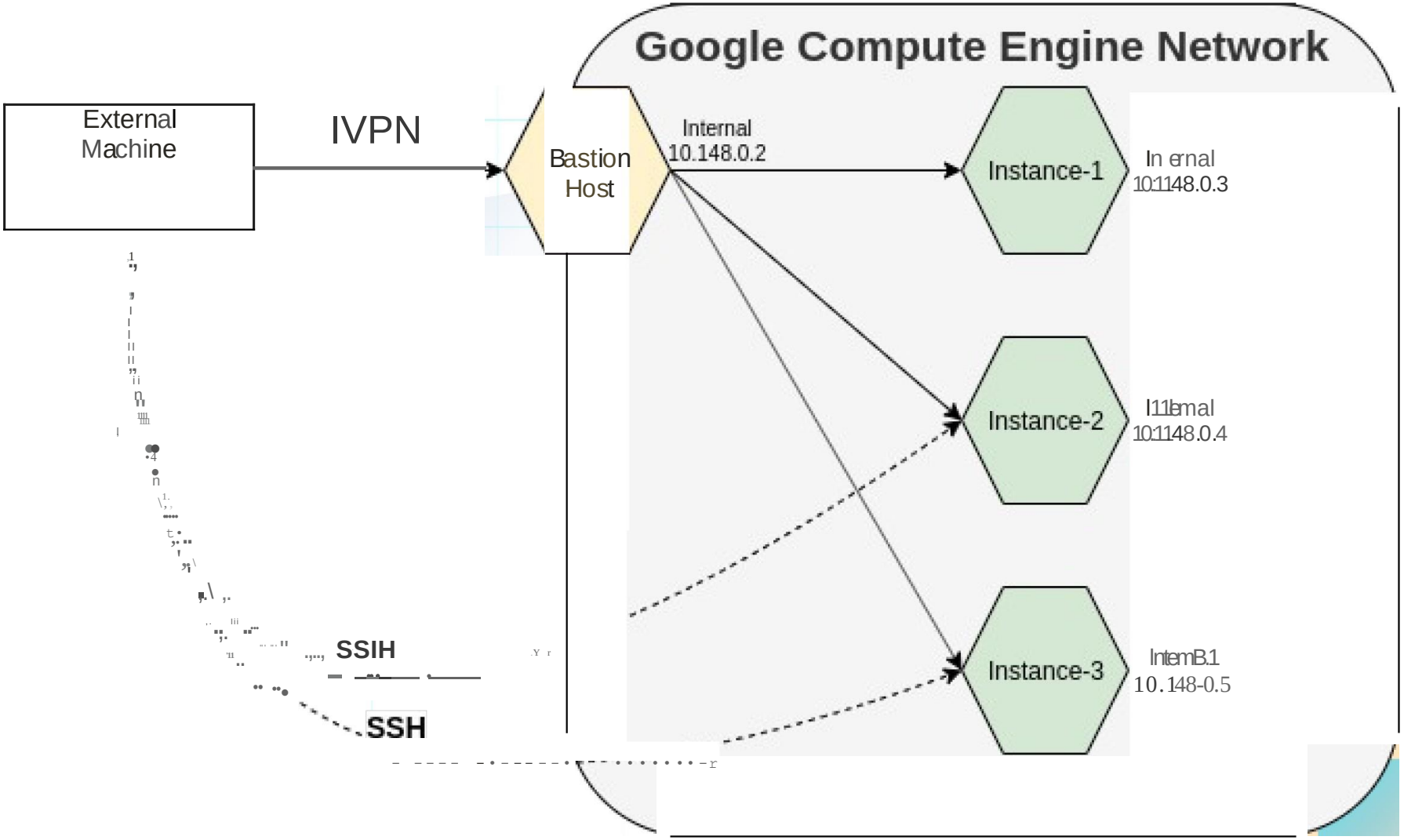
Bastion Host Placement

- requires two firewalls, with bastion hosts sitting between the first "outside world" firewall, and an inside firewall.
- in a DMZ, often smaller networks do not have multiple firewalls, so if only one firewall exists in a network, bastion hosts are commonly placed outside the firewall.

Bastion Host Placement

- requires two firewalls, with bastion hosts sitting between the first "outside world" firewall, and an inside firewall.
- in a DMZ, often smaller networks do not have multiple firewalls, so if only one firewall exists in a network, bastion hosts are commonly placed outside the firewall.

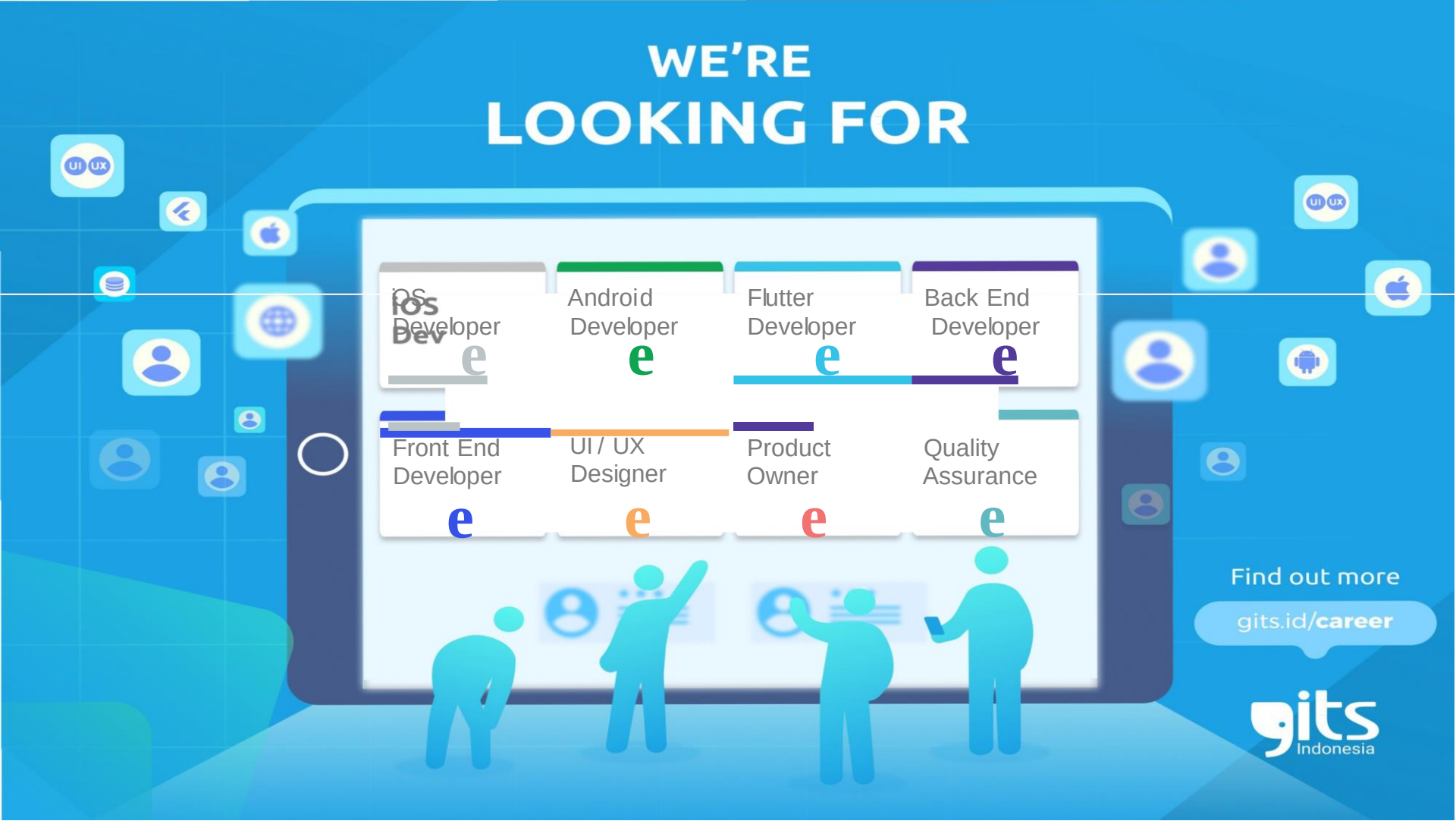

Google Compute Engine Network
External Machine
SSH
Bastion Host
Internal 10.148.0.2
Instance-1
Instance-2
Instance-3


Google Compute Engine Network
External Machine
IVPN
Bastion Host
Internal 10.148.0.2
Instance-1
In ernal 10.1148.0.3
Instance-2
I.11emal 10.1148.0.4
Instance-3
IntemB.1 10.148-0.5
SSIH
SSH

Thank You!

www.gits.id

@gitscreative


WE'RE
LOOKING FOR
iOS Developer
Android Developer
Flutter Developer
Back End Developer
Front End Developer
UI / UX Designer
Product Owner
Quality Assurance
Find out more
gits.id/career
gits Indonesia

Alone We are smart, together We are brilliant

DEVOPS INDONESIA

THANK YOU !

Quote by Steve Anderson

Stay Connected

@IDDevOps

http://www.devopsindonesia.com

@devopsindonesia

@DevOpsIndonesia

@IDDevOps

SCAN ME!

https://t.me/IDDevOpsBDG

https://t.me/IDDevOps