Réseau sur le cloud
Comprendre les bases

et quelques bonnes pratiques !

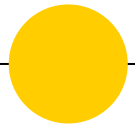
Julien Rollin – @TalanLabs – Ruche 28/01/2020

A propos de cette présentation ?

Déployons notre superbe application dans le Cloud !

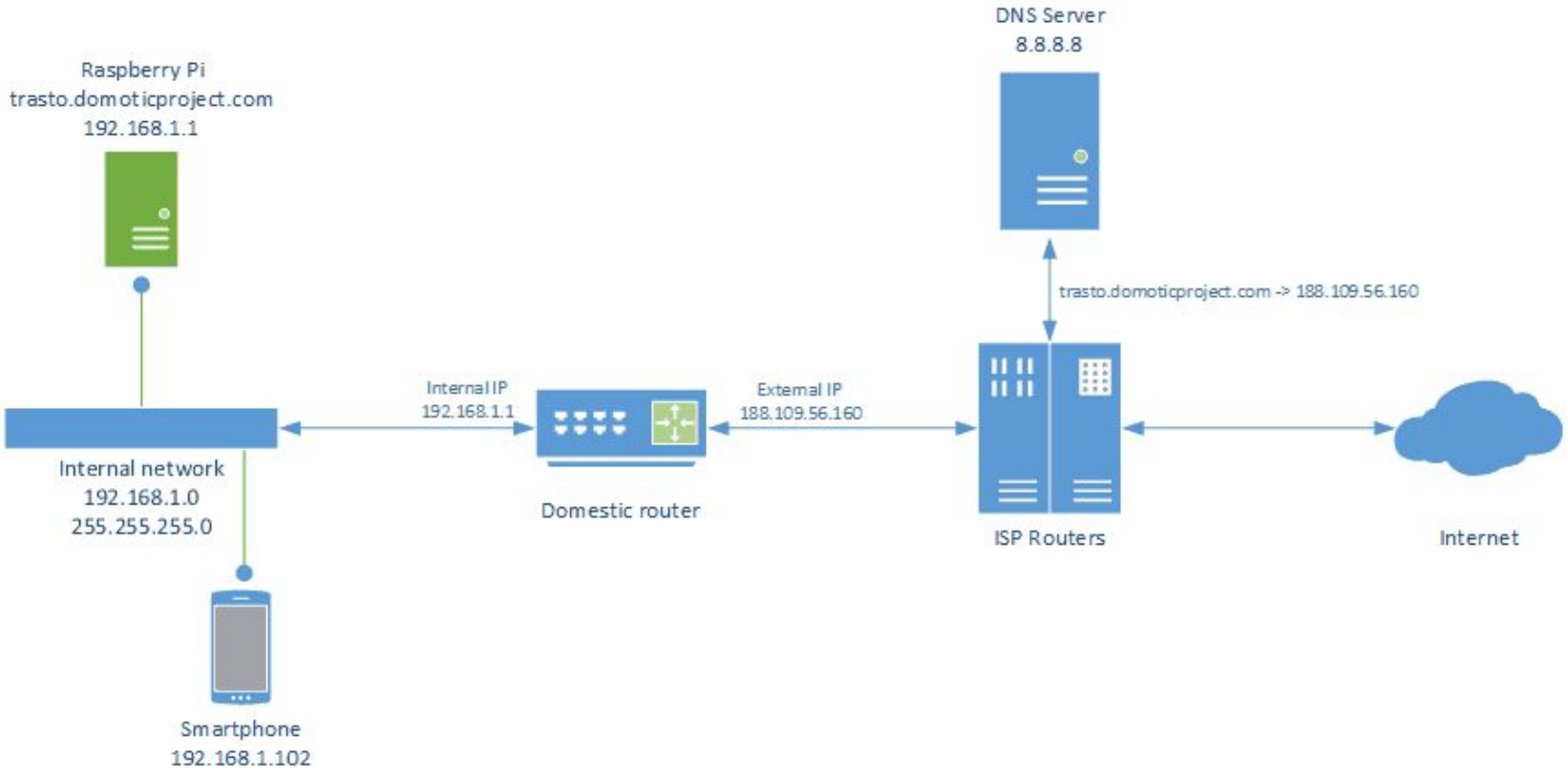
“

Quelques rappels



Que se passe-t'il quand je tape une adresse web dans mon navigateur ?

“



requête internet

Et du côté hébergeur Cloud, comment ça marche ?

“

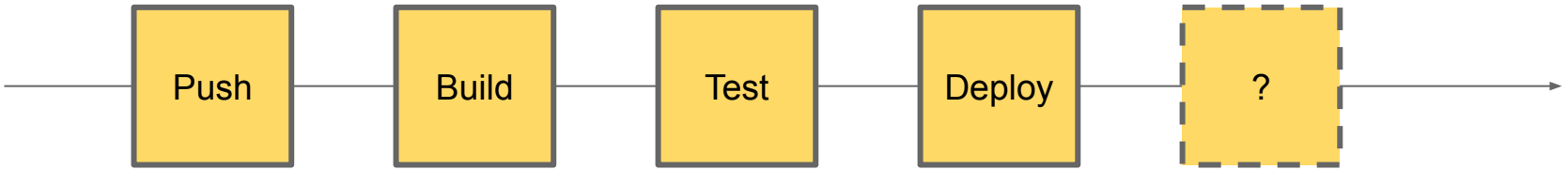
Prenons des exemples !

“

Application statique HTML

React, Angular, Vuejs, VanillaJS, etc

Livrer son application

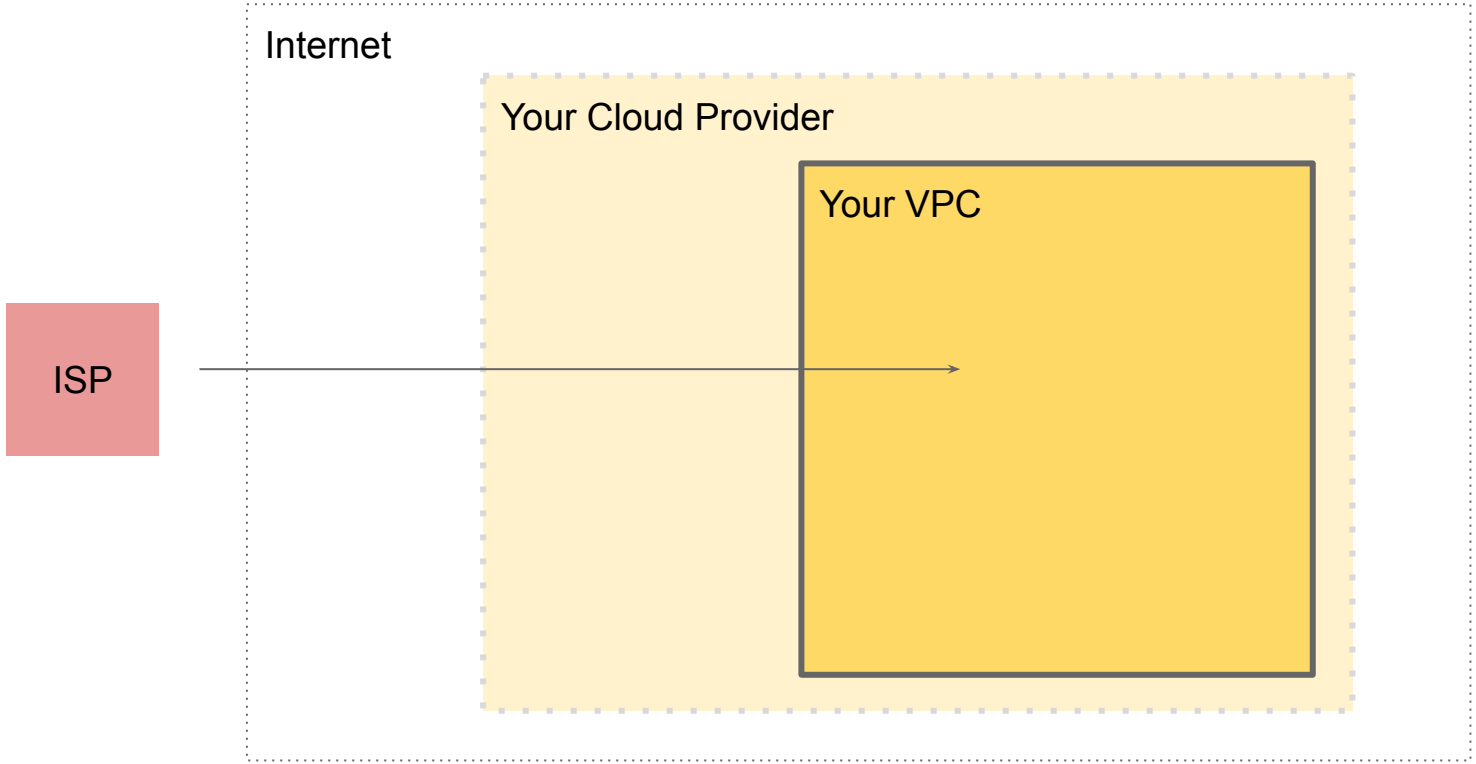


Intégration continue et livraison continue

Il faut un serveur HTTP pour y déposer et servir nos fichiers

Virtual Private Cloud

Votre réseau

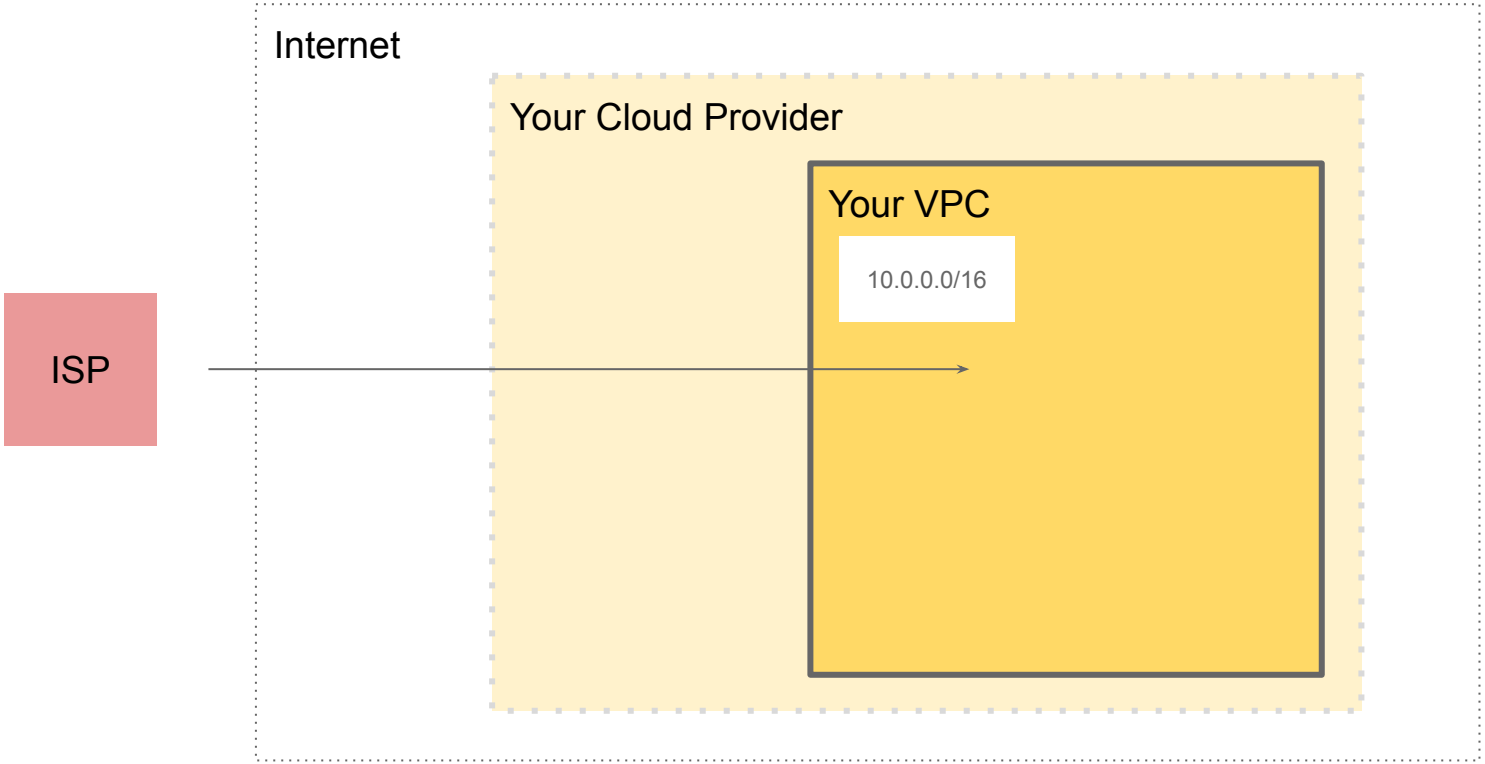


Virtual Private Cloud

Combien d'adresses IP devrais-je gérer ?

CIDR Block	Number of IP Addresses
/28	16
/27	32
/26	64
/25	128
/24	254
/23	510
/22	1022
/21	2046
/20	4094
/19	8190
/18	16,382
/17	32,766
/16	65,536

CIDR (Classless Inter-Domain Routing) - Plage d'adresses IP

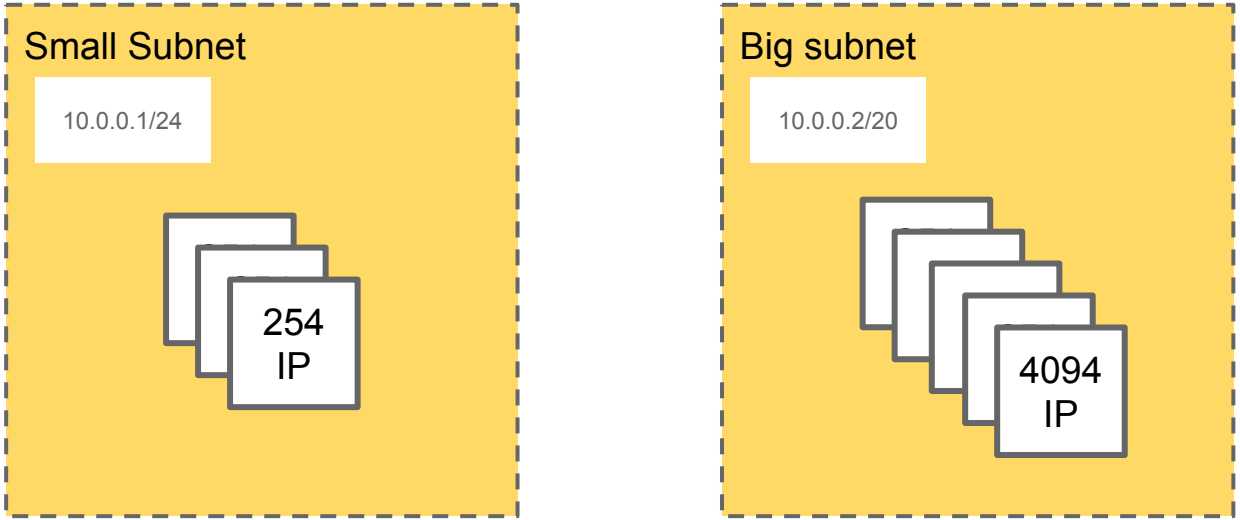


Virtual Private Cloud avec 65 536 IP possibles

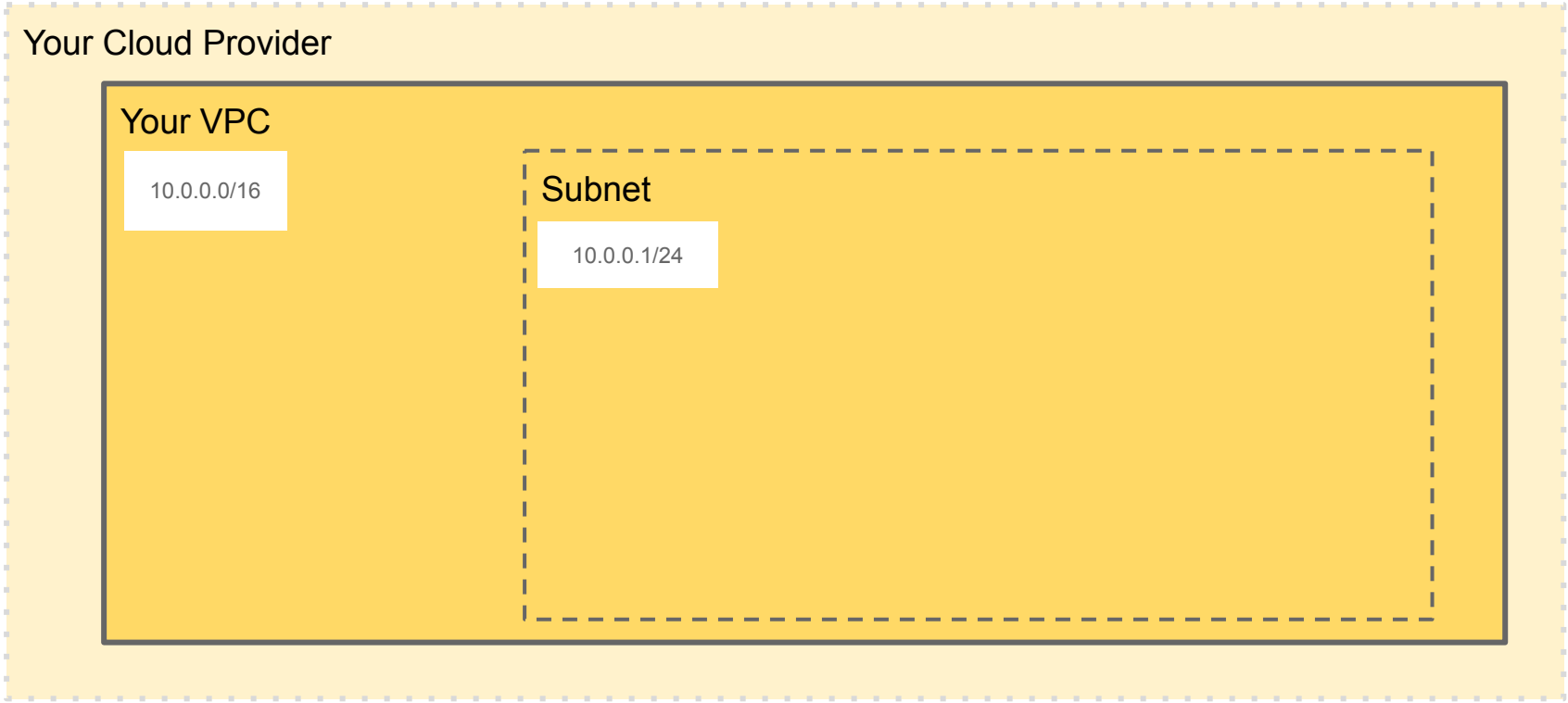
Définition d'un réseau pour notre application

Subnet

Réseau dans le réseau



Subnet - réseaux dans le réseau


Your Cloud Provider
Your VPC
10.0.0.0/16
Subnet
10.0.0.1/24

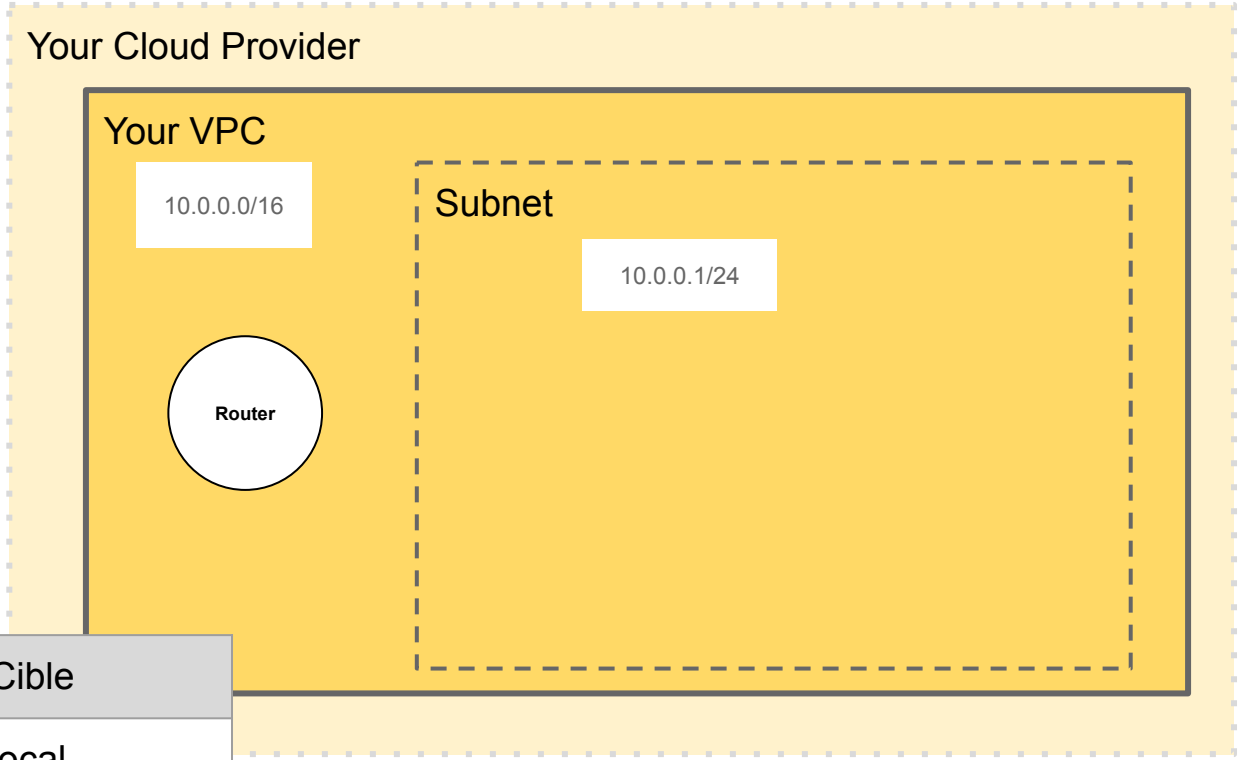
Comment rediriger le trafic vers le bon réseau ?

Router

rediriger les paquets dans le bon réseau

Destination	Cible
10.0.0.0/16	local

Router - table de chemins



Destination	Cible
10.0.0.0/16	local

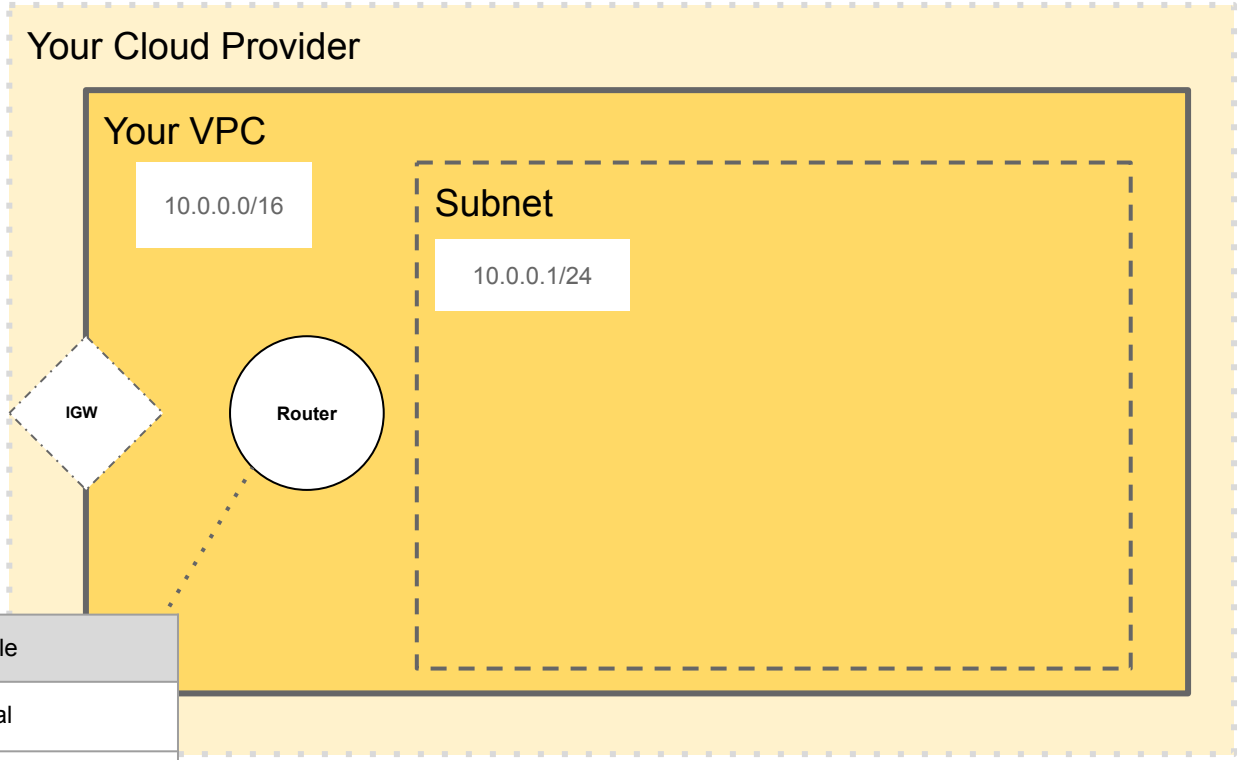
Router assigné au VPC

Notre VPC a besoin de se connecter à internet

“

Internet Gateway

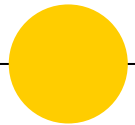
communiquer avec internet

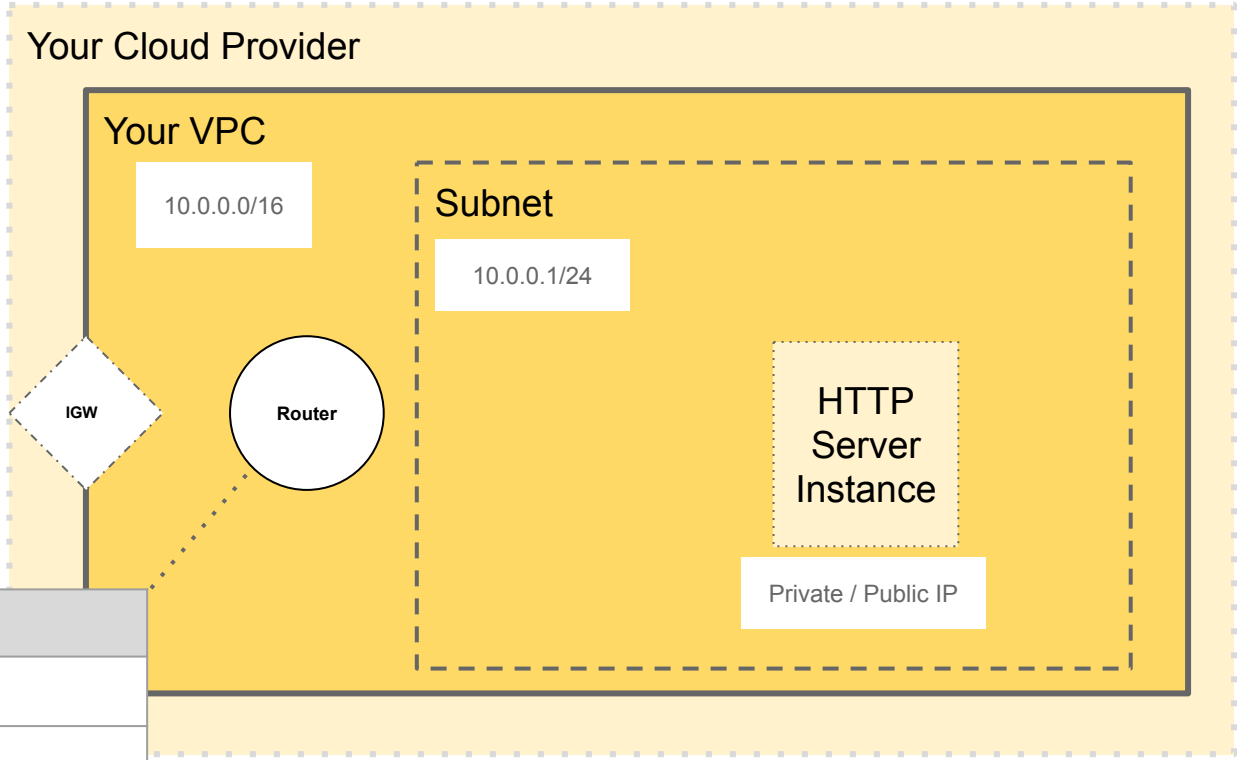


Destination	Cible
10.0.0.0/16	local
0.0.0.0/0	igw

Route vers la gateway ajoutée

Ajouter son serveur au réseau



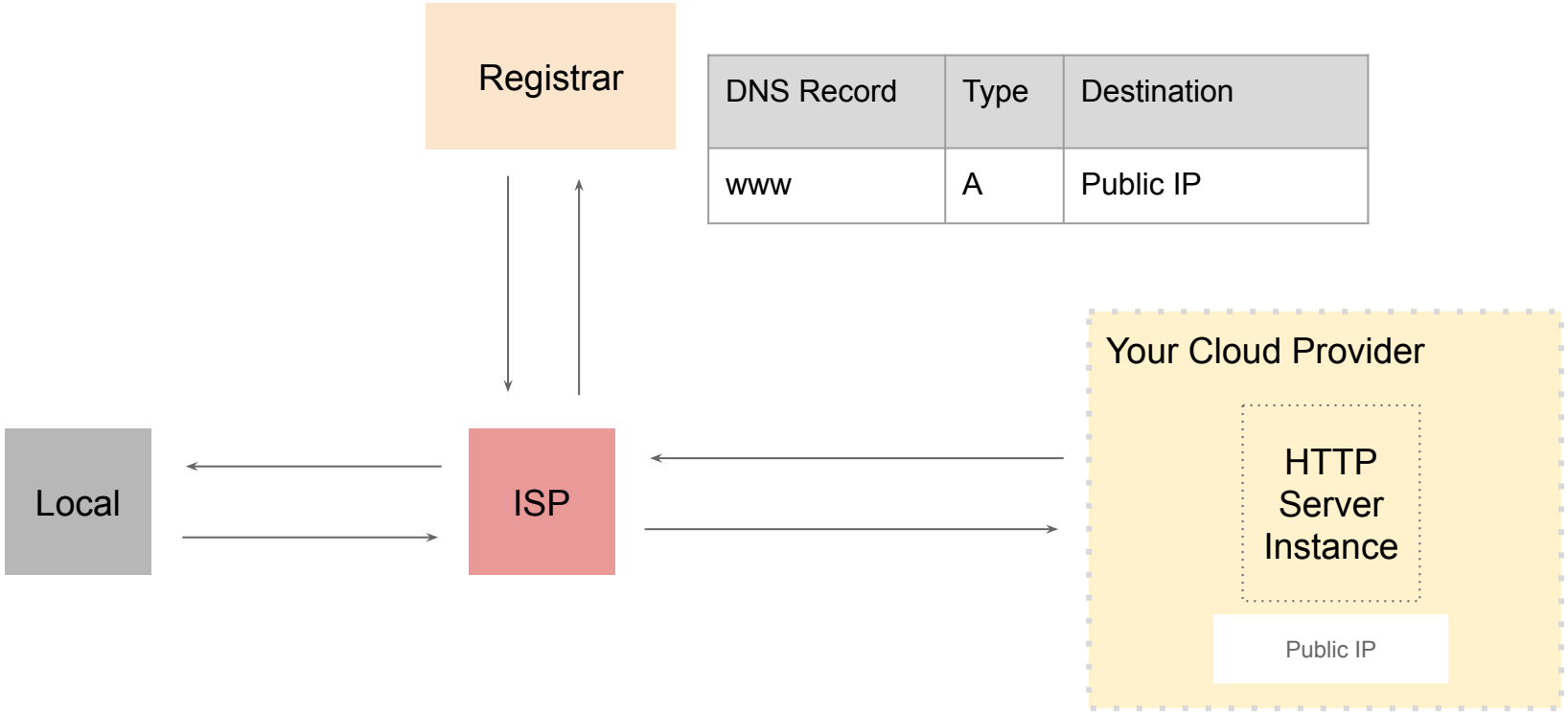


Destination	Cible
10.0.0.0/16	local
0.0.0.0/0	igw

Ajout d'une "instance" de serveur HTTP

Remarques sur l’assignation IP

- Private IP
- Public IP
- Elastic IP parfois



Version simplifiée

Et hop !
y a plus qu'à déployer non ?

“

Heu...
Et la sécurité ??!

“

Les groupes de sécurité

définir des règles d'accès

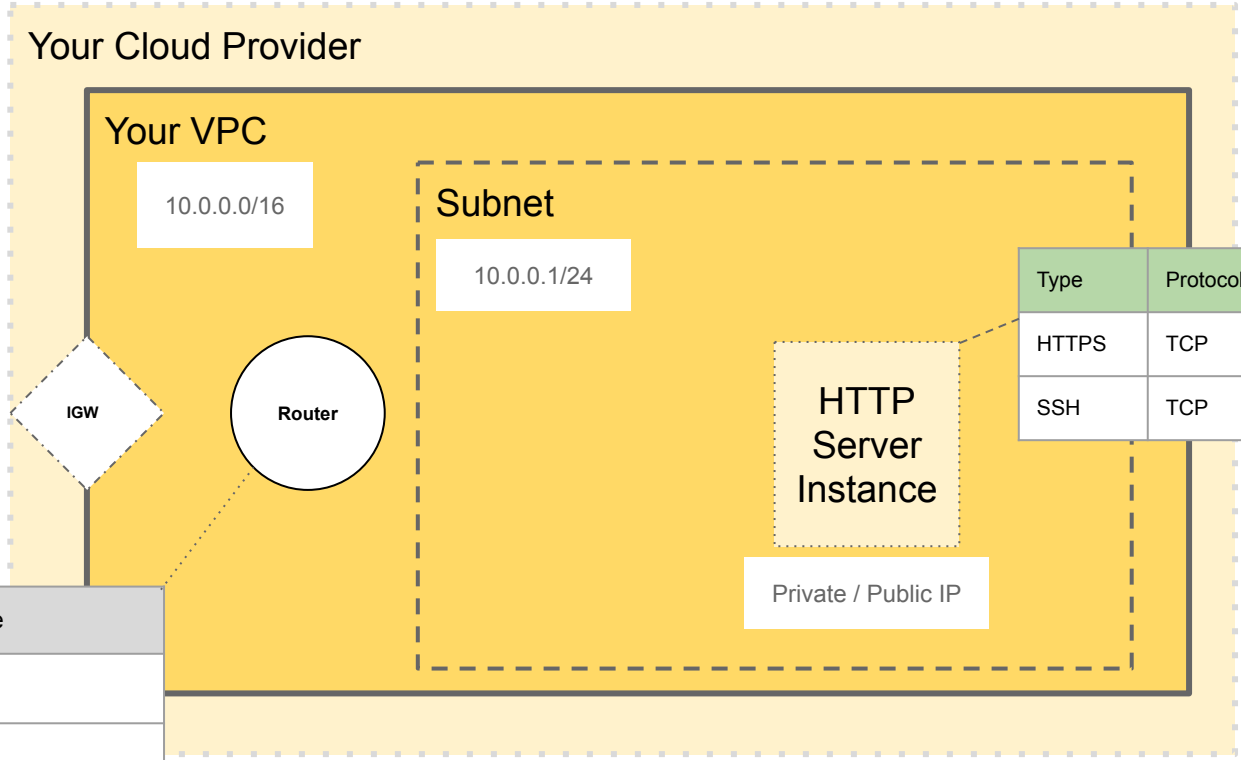
Network Access Control List (subnet)

Règle	Type	Protocol	Port	Source	Allow/Deny
100	SSH	TCP	22	0.0.0.0/0	DENY
200	ALL	ALL	ALL	0.0.0.0/0	ALLOW

Security Group (instance)

Type	Protocol	Port	Source
HTTPS	TCP	443	0.0.0.0/0
SSH	TCP	22	YOUR IP

Exemples de règles au niveau réseau et/ou au niveau instance (in/out)



Type	Protocol	Port	Source
HTTPS	TCP	443	0.0.0.0/0
SSH	TCP	22	YOUR IP

Destination	Cible
10.0.0.0/16	local
0.0.0.0/0	igw

Ajout d'une "instance" de serveur HTTP

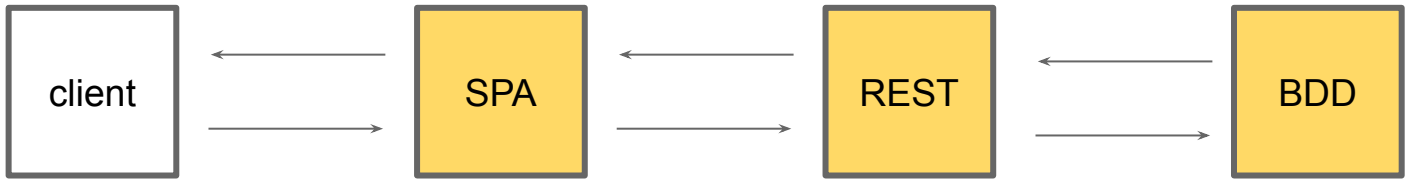
Ce qu'on a vu

- VPC
- Subnet
- Internet Gateway
- Routeur
- Instances
- Règles d'accès entrantes et sortantes

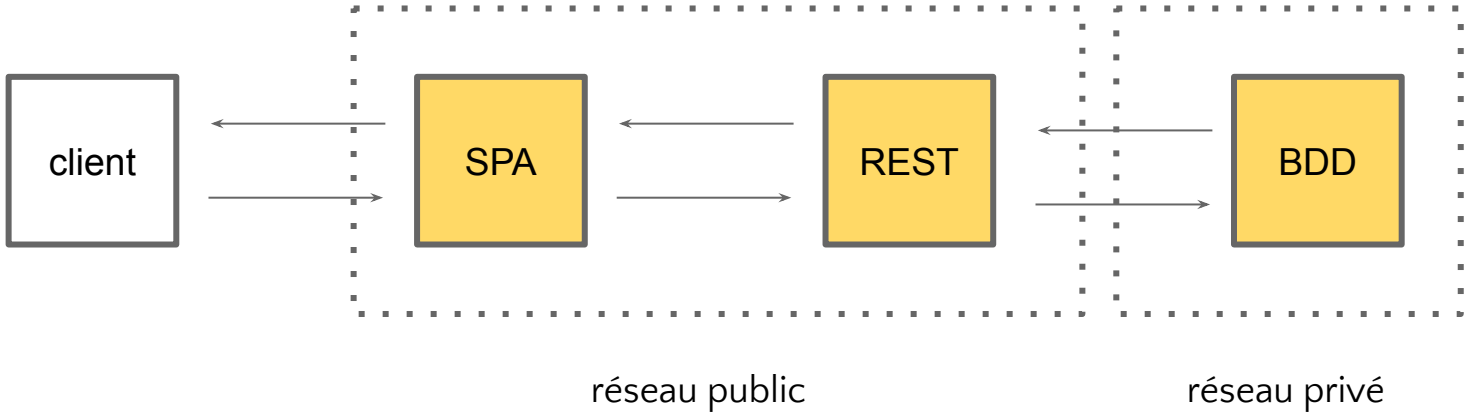
Application SPA avec REST API

Front React et API REST avec springboot

Composants de notre stack



Réseau privé vs public

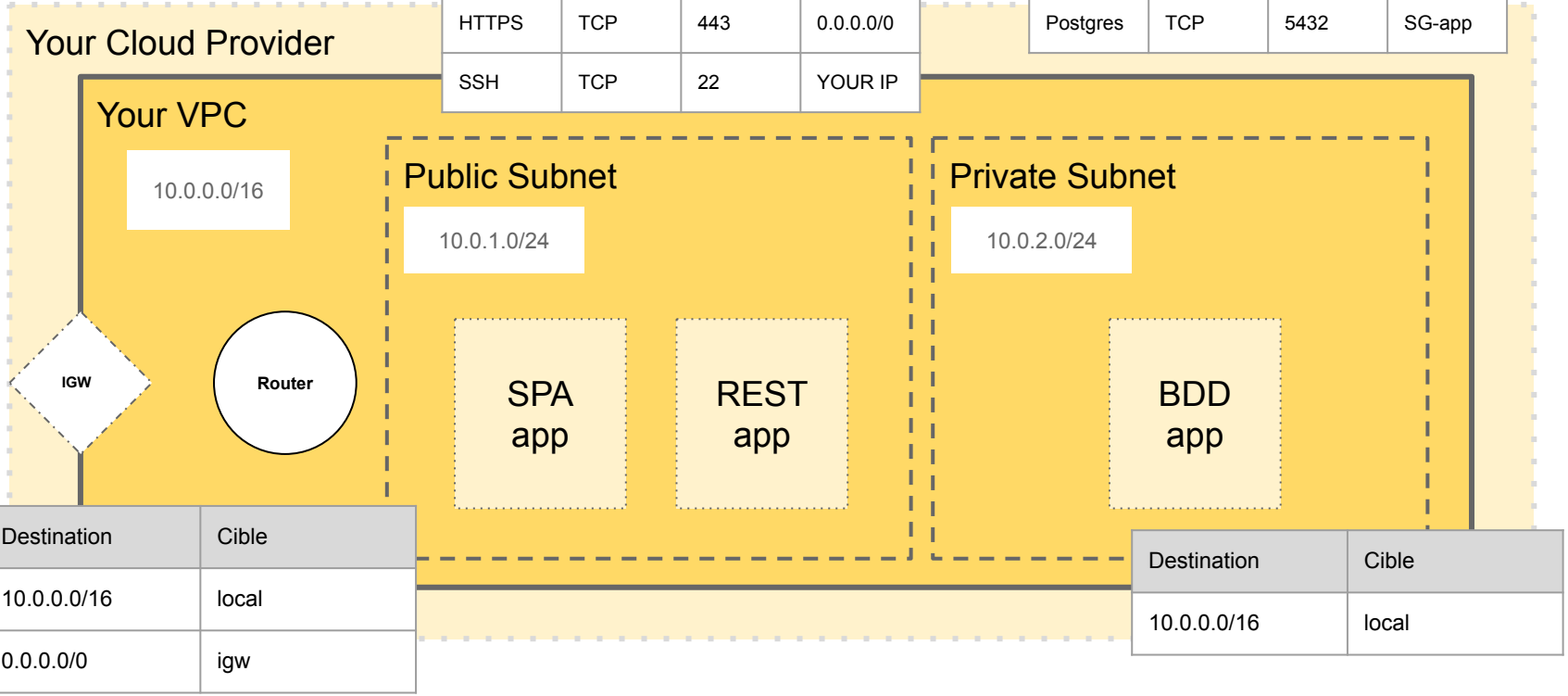


app-sg

Type	Protocol	Port	Source
HTTPS	TCP	443	0.0.0.0/0
SSH	TCP	22	YOUR IP

bdd-sg

Type	Protocol	Port	Source
Postgres	TCP	5432	SG-app



Destination	Cible
10.0.0.0/16	local
0.0.0.0/0	igw

Destination	Cible
10.0.0.0/16	local

Réseau privé sans accès internet et règles de sécurité spécifiques

Je ne peux plus patcher ma BDD...
Comment faire ?

“

Network Address Translation Gateway

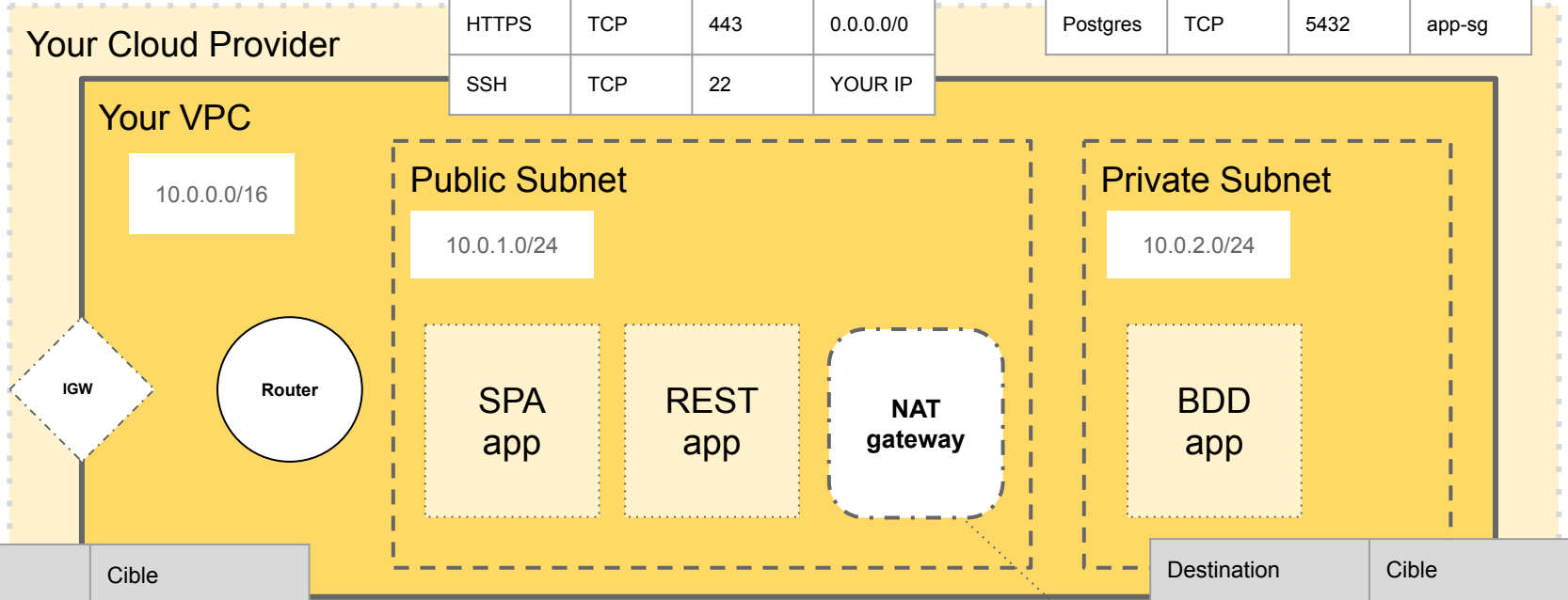
Accéder à internet depuis un réseau privé

app-sg

Type	Protocol	Port	Source
HTTPS	TCP	443	0.0.0.0/0
SSH	TCP	22	YOUR IP

bdd-sg

Type	Protocol	Port	Source
Postgres	TCP	5432	app-sg



Destination	Cible
10.0.0.0/16	local
0.0.0.0/0	igw

Destination	Cible
10.0.0.0/16	local
0.0.0.0/0	**nat-gw**

Réseau privé avec NAT Gateway

Notre application explose sur les réseaux sociaux !

“

Equilibreur de charge

répartir le trafic vers des cibles

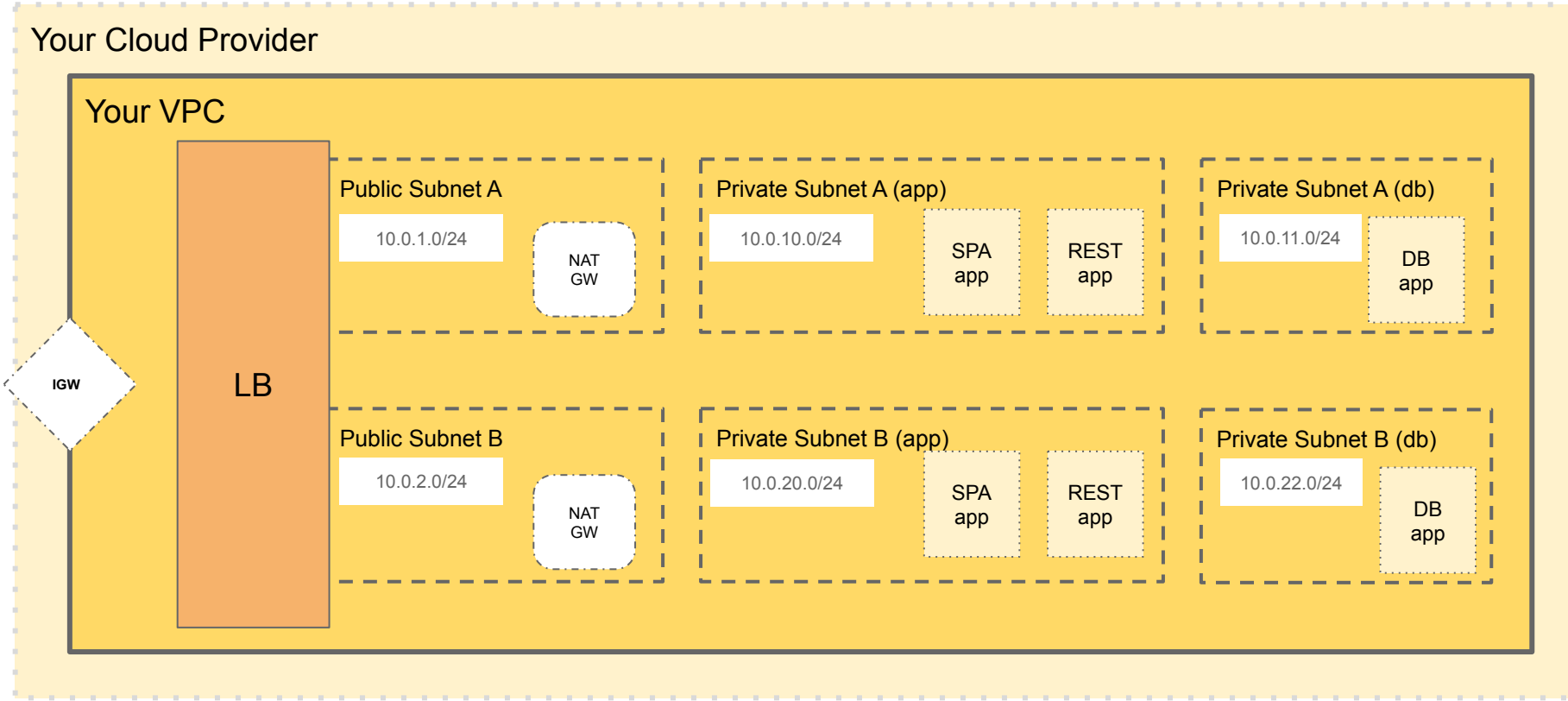


Schéma simplifié (pas pas de routeurs, règles sécurités, règles LB, master/slave DB, etc)

Autoscaling
Mise à l'échelle

Définir des stratégies d'action

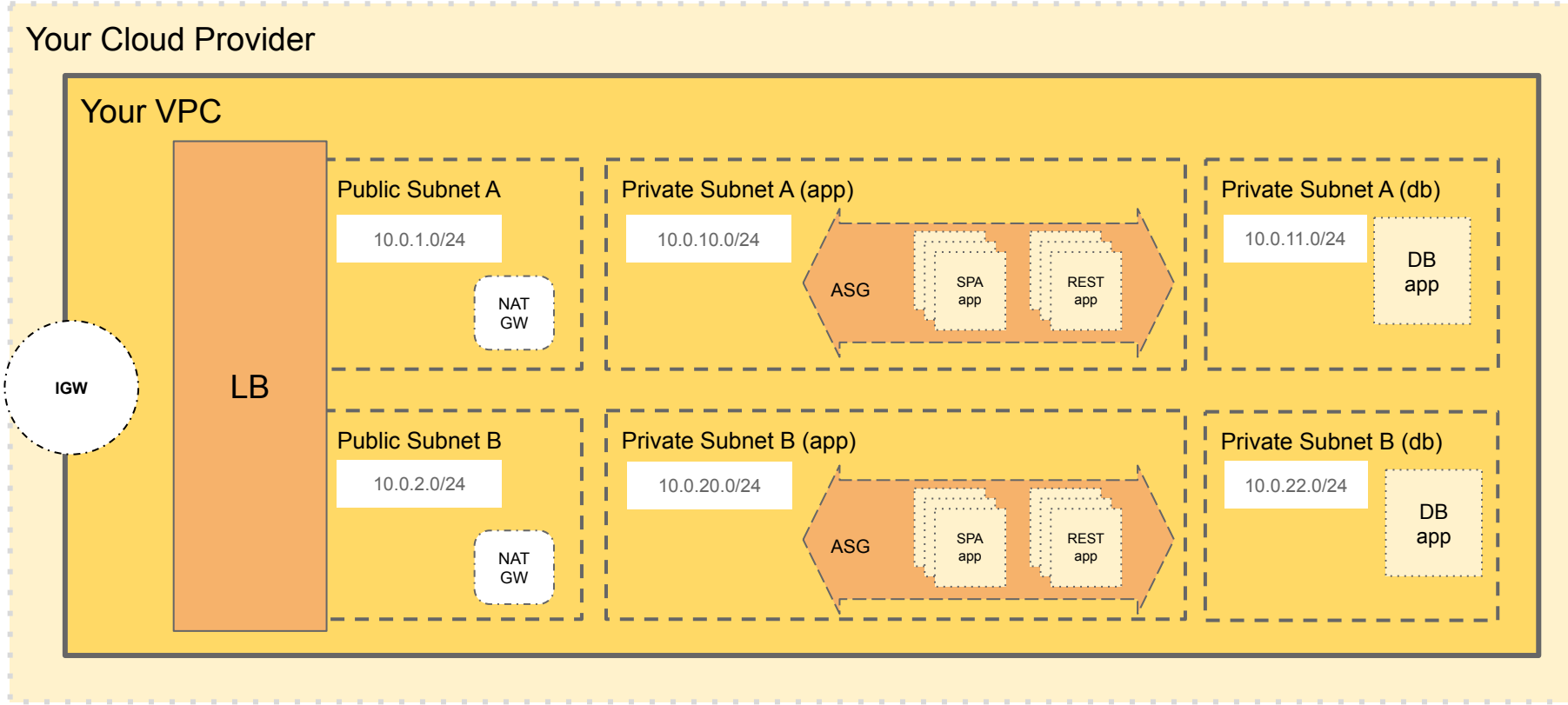


Schéma simplifié (pas pas de routeurs, règles sécurités, règles LB, master/slave DB, etc)

Ce qu'on a vu

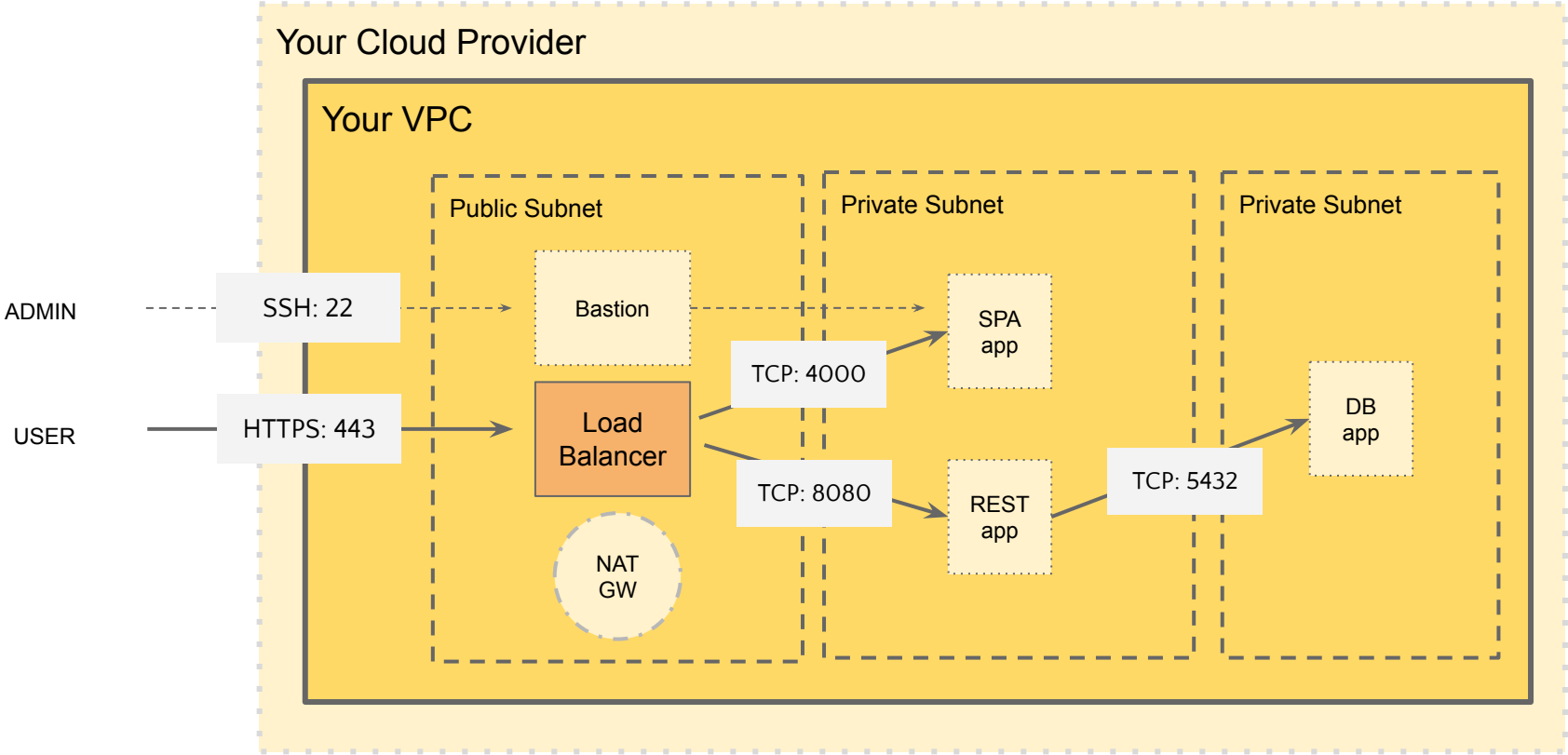
- VPC
- Subnet privé / public
- Internet Gateway
- NAT Gateway
- Routeur
- Instances
- Règles d'accès entrantes et sortantes
- Equilibreur de charge
- Auto Scaling groupe

Comment rajouter encore un peu plus de sécurité ?

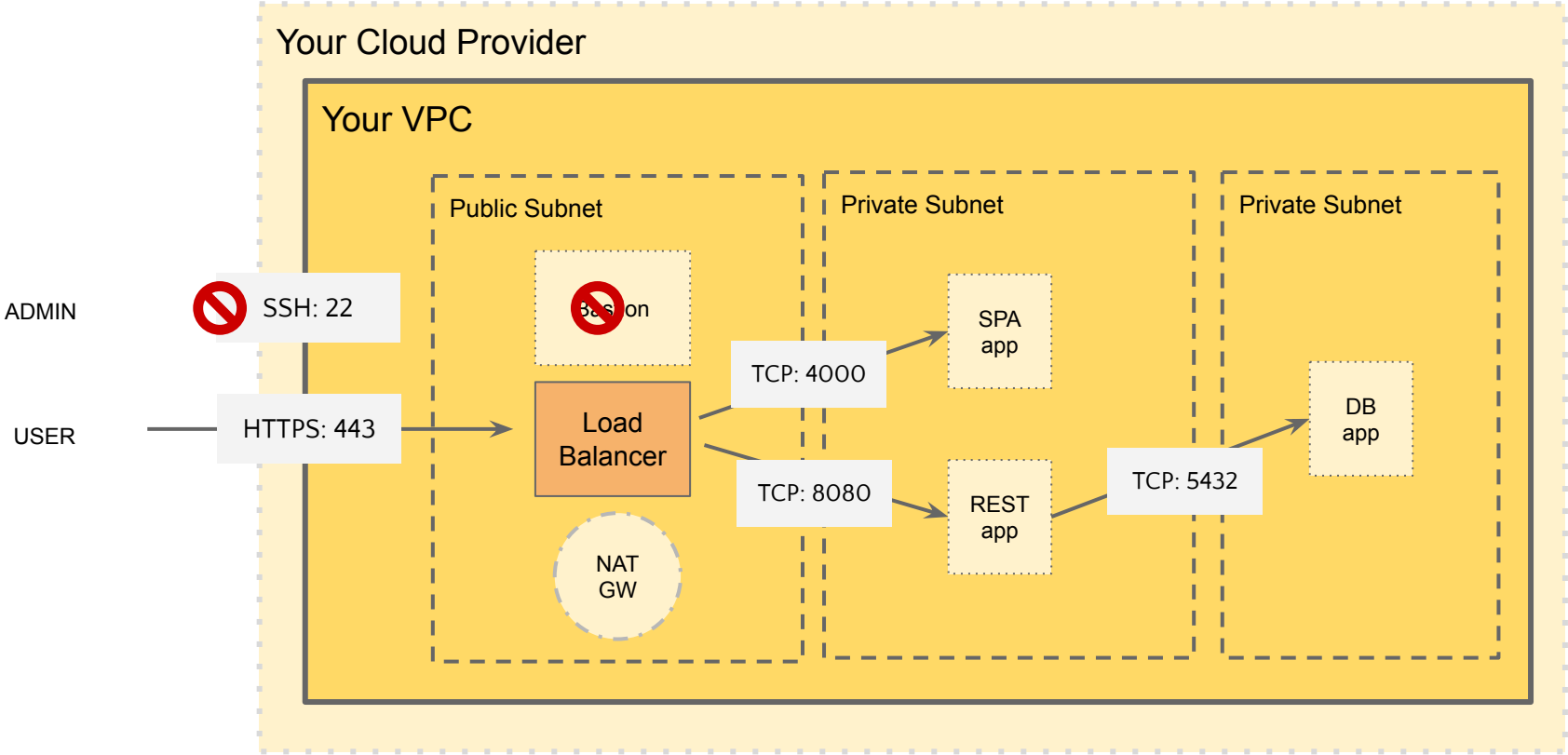
“

Un Bastion pour accéder aux réseaux

Vous ne passerez pas



Un bastion comme “relai” SSH vers les réseaux privés



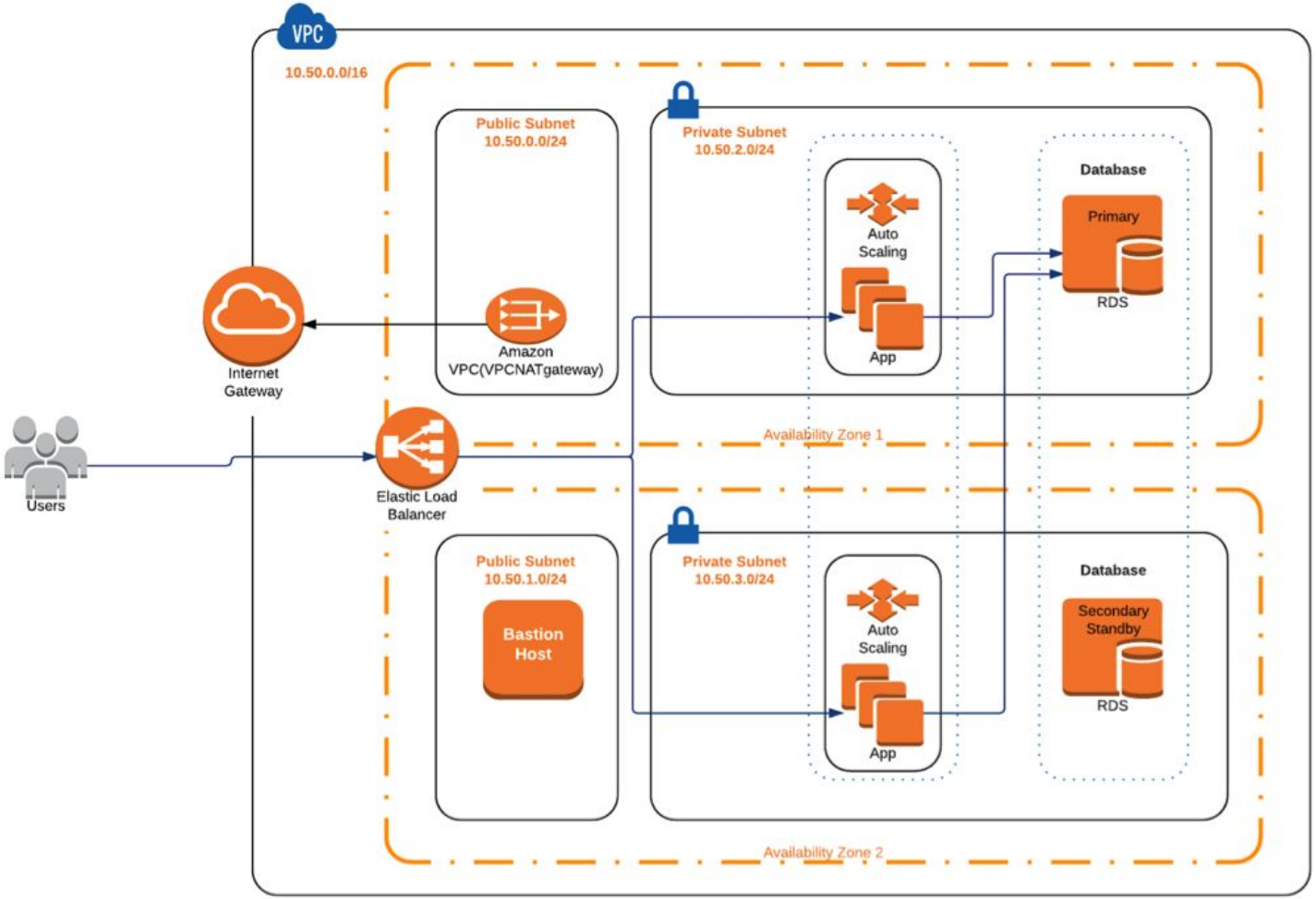
Détruire l'instance si plus besoin de se connecter

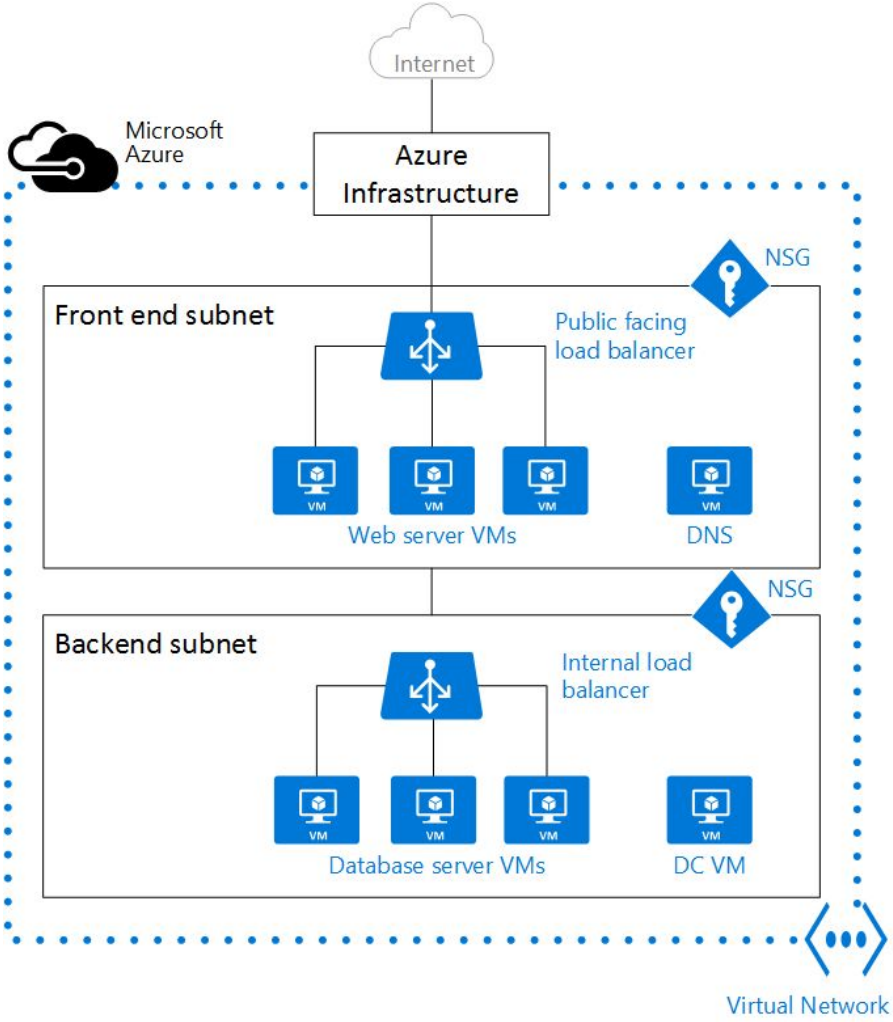
Points importants

- n’ouvrir que ce qui est nécessaire (in/out)
- utiliser des bastions avec des clés SSH
- ne pas assigner des IP inutilement

Et maintenant, les fameux schémas !

“


VPC
10.50.0.0/16
Public Subnet
10.50.0.0/24
Private Subnet
10.50.2.0/24
Database
Auto
Scaling
Primary
RDS
App
Amazon
VPC(VPCNATgateway)
Internet
Gateway
Users
Elastic Load
Balancer
Availability Zone 1
Public Subnet
10.50.1.0/24
Bastion
Host
Private Subnet
10.50.3.0/24
Database
Auto
Scaling
Secondary
Standby
RDS
App
Availability Zone 2


Internet
Microsoft Azure
Azure Infrastructure
NSG
Front end subnet
Public facing load balancer
VM
VM
VM
VM
Web server VMs
DNS
NSG
Backend subnet
Internal load balancer
VM
VM
VM
VM
Database server VMs
DC VM
Virtual Network

A vous de jouer !

“

Ce qui n’a pas été couvert

- Régions
- Zones de disponibilité
- CDN pour les médias
- Rôles et permissions IAM
- VPN / Peering
- etc

Merci !

“

Crédits

- Minions : oeuvre de Sergio Pablos
- Les Minions (Minions) est un film d'animation américain réalisé par Kyle Balda et Pierre Coffin, sorti en 2015.
- Schémas from AWS, Azure