

Deep Dive

Virtual Private Cloud (VPC)

Julien Simon

Principal Technical Evangelist, AWS

julsimon@amazon.fr

@julsimon

`aws vpc --expert-mode`



Agenda

172.16.0.0

172.16.1.0

172.16.2.0

Routage et
connexions
privées



Peering
de VPC



Enhanced
Networking



Points de
terminaison
pour Amazon S3

Configurations réseau

EC2-Classic

Simple à démarrer – toutes les instances ont une connectivité Internet, des adresses IP privées et publiques auto-attribuées

Groupes de sécurité entrants



VPC par défaut

Le meilleur des deux

Mise en route avec l'expérience EC2-Classic

Si et quand cela s'avère nécessaire, commencez à utiliser la fonctionnalité VPC dont vous avez besoin



VPC

Services de mise en réseau avancée : ENI et plusieurs IP, Tables de routage, Groupes de sécurité, ACL réseau, Connectivité privée, Mise en réseau améliorée, etc.

Configurations réseau

EC2-Classic

Simple à démarrer – toutes les instances ont une connectivité Internet, des adresses IP privées et publiques auto-

Tous les comptes créés après le 04/12/2013 prennent en charge VPC uniquement et ont un VPC par défaut dans chaque région

VPC par défaut

Le meilleur des deux

Mise en route avec l'expérience EC2-Classic

Si et quand cela s'avère nécessaire, commencez à utiliser la fonctionnalité VPC dont vous avez besoin

VPC



Services de mise en réseau avancée :
ENI et plusieurs IP
Tables de routage
Groupes de sécurité
ACL réseau
Connectivité privée

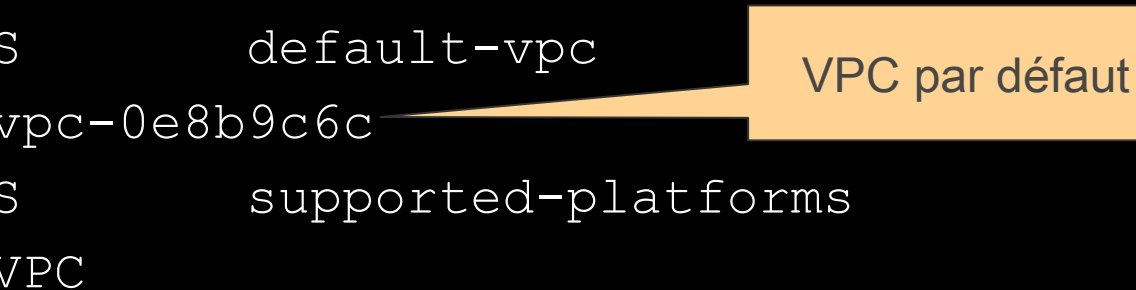
Mise en réseau améliorée

Etc.



Identifier le VPC par défaut

```
$ aws ec2 describe-account-attributes
  --attribute-names supported-platforms default-vpc
ACCOUNTATTRIBUTES      default-vpc
ATTRIBUTEVALUES vpc-0e8b9c6c
ACCOUNTATTRIBUTES      supported-platforms
ATTRIBUTEVALUES VPC
```



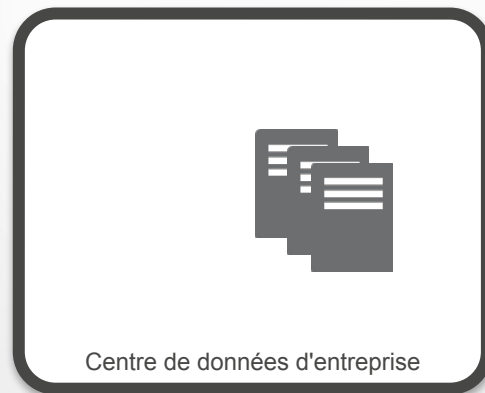
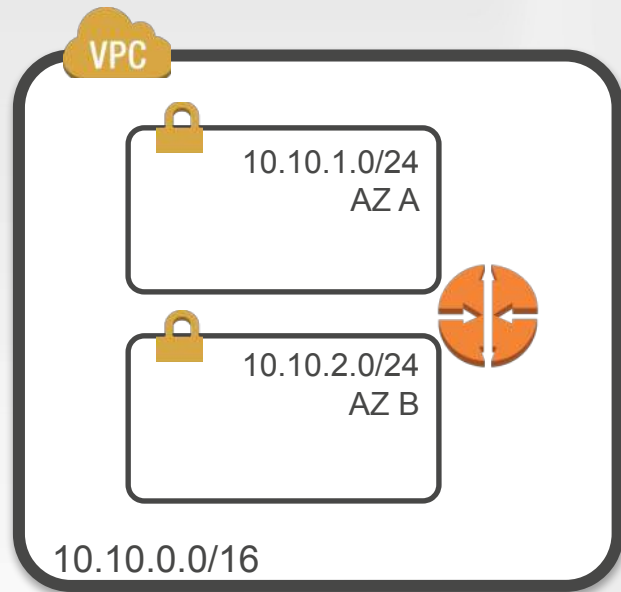
The diagram consists of two orange rectangular boxes with callout lines pointing to specific parts of the command output. The first box, labeled 'VPC par défaut', has a line pointing to the value 'vpc-0e8b9c6c' under the 'ATTRIBUTEVALUES' for the 'default-vpc' attribute. The second box, labeled 'Configuration VPC', has a line pointing to the value 'VPC' under the 'ATTRIBUTEVALUES' for the 'supported-platforms' attribute.

Routage et connexions privées

Implémentation d'une architecture hybride

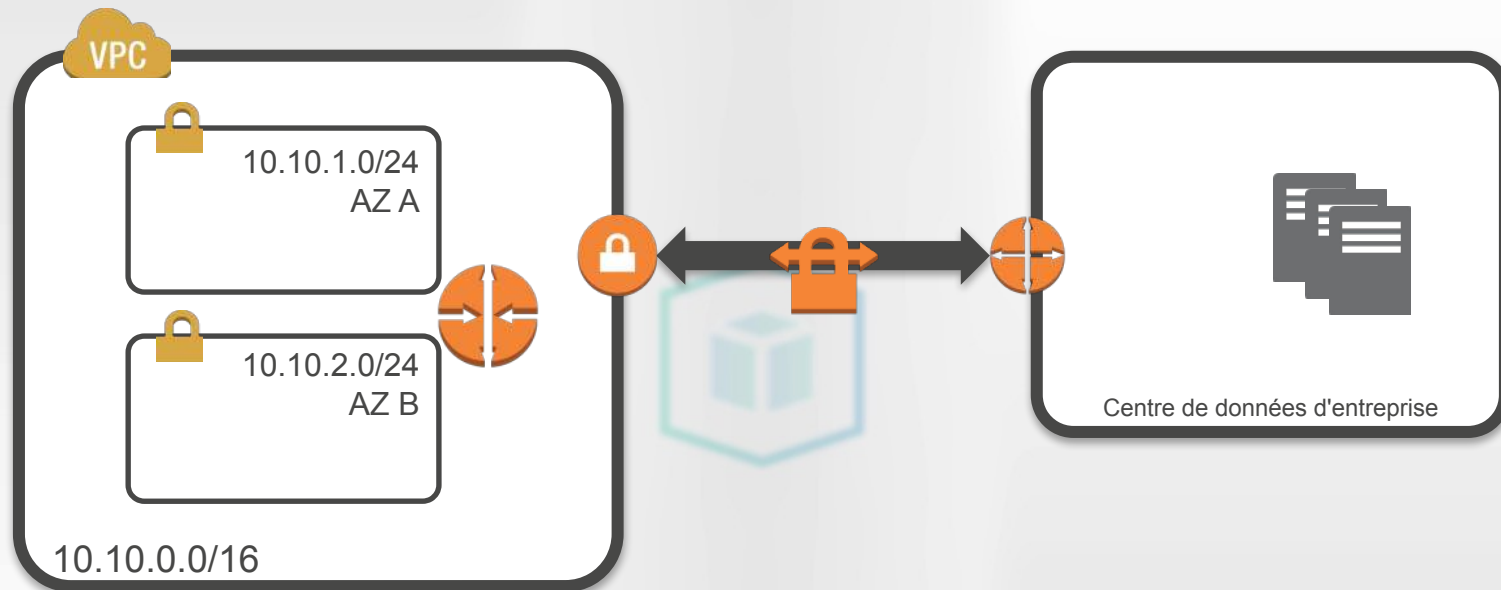


Créer un VPC



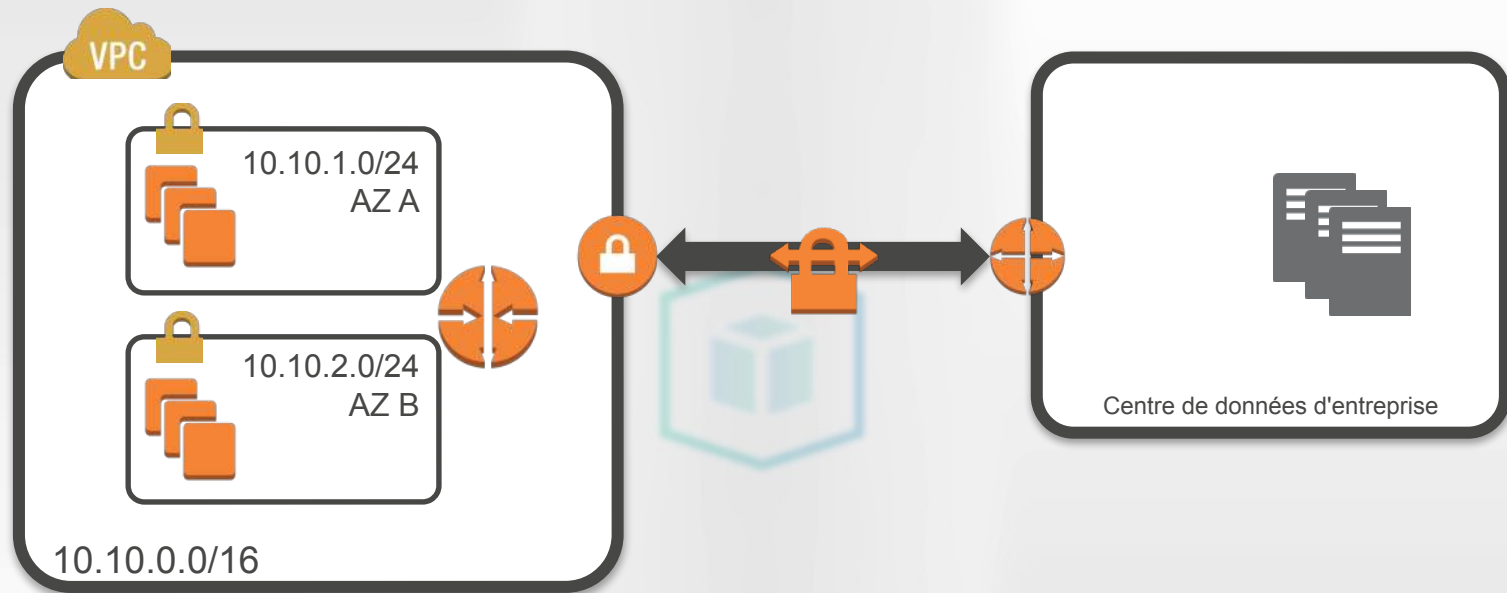
```
aws ec2 create-vpc --cidr 10.10.0.0/16
aws ec2 create-subnet --vpc vpc-c15180a4 --cidr 10.10.1.0/24 --a us-west-2a
aws ec2 create-subnet --vpc vpc-c15180a4 --cidr 10.10.2.0/24 --a us-west-2b
```

Créer une connexion VPN



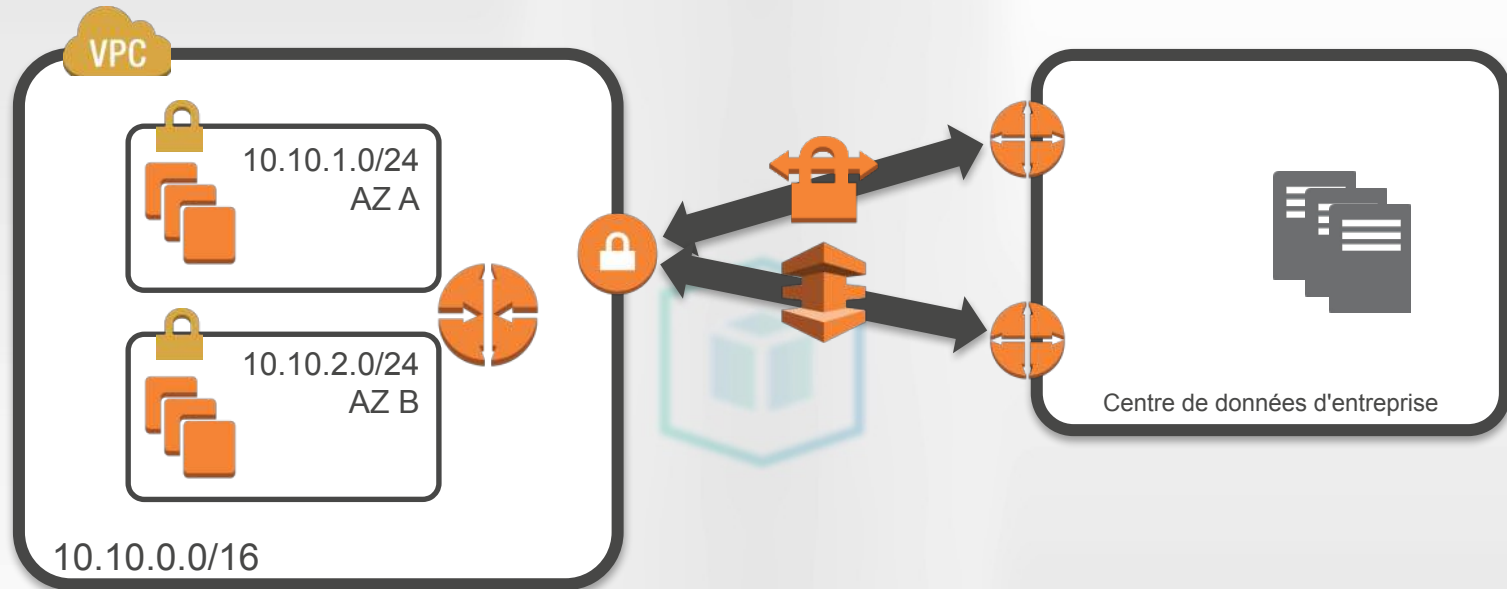
```
aws ec2 create-vpn-gateway --type ipsec.1
aws ec2 attach-vpn-gateway --vpn vgw-f9da06e7 --vpc vpc-c15180a4
aws ec2 create-customer-gateway --type ipsec.1 --public 54.64.1.2 --bgp 6500
aws ec2 create-vpn-connection --vpn vgw-f9da06e7 --cust cgw-f4d905ea --t ipsec.1
```

Lancer des instances



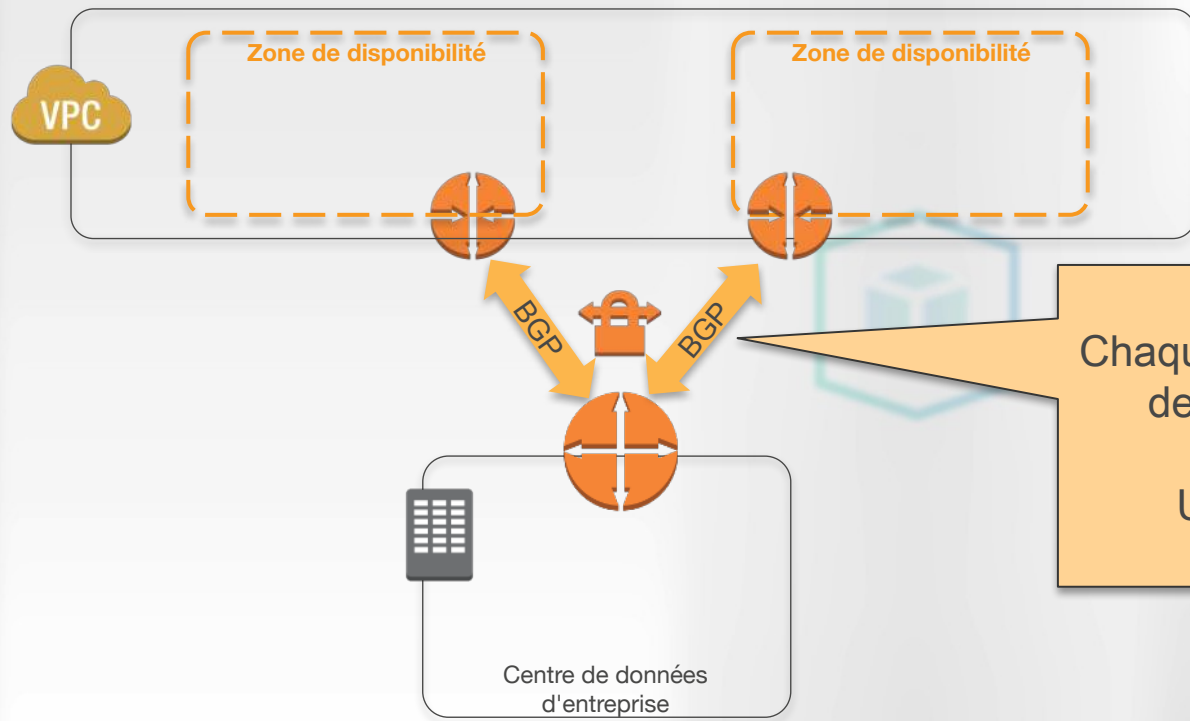
```
aws ec2 run-instances --image ami-d636bde6 --sub subnet-d83d91bd --count 3
aws ec2 run-instances --image ami-d636bde6 --sub subnet-b734f6c0 --count 3
```

Utilisation d'AWS Direct Connect



```
aws directconnect create-connection --loc EqSE2 --b 1Gbps --conn My_First
aws directconnect create-private-virtual-interface --conn dxcon-fgp13h2s --new
virtualInterfaceName=Foo, vlan=10, asn=60, authKey=testing,
amazonAddress=192.168.0.1/24, customerAddress=192.168.0.2/24,
virtualGatewayId=vgw-f9da06e7
```

Bonnes pratiques pour la connexion à distance



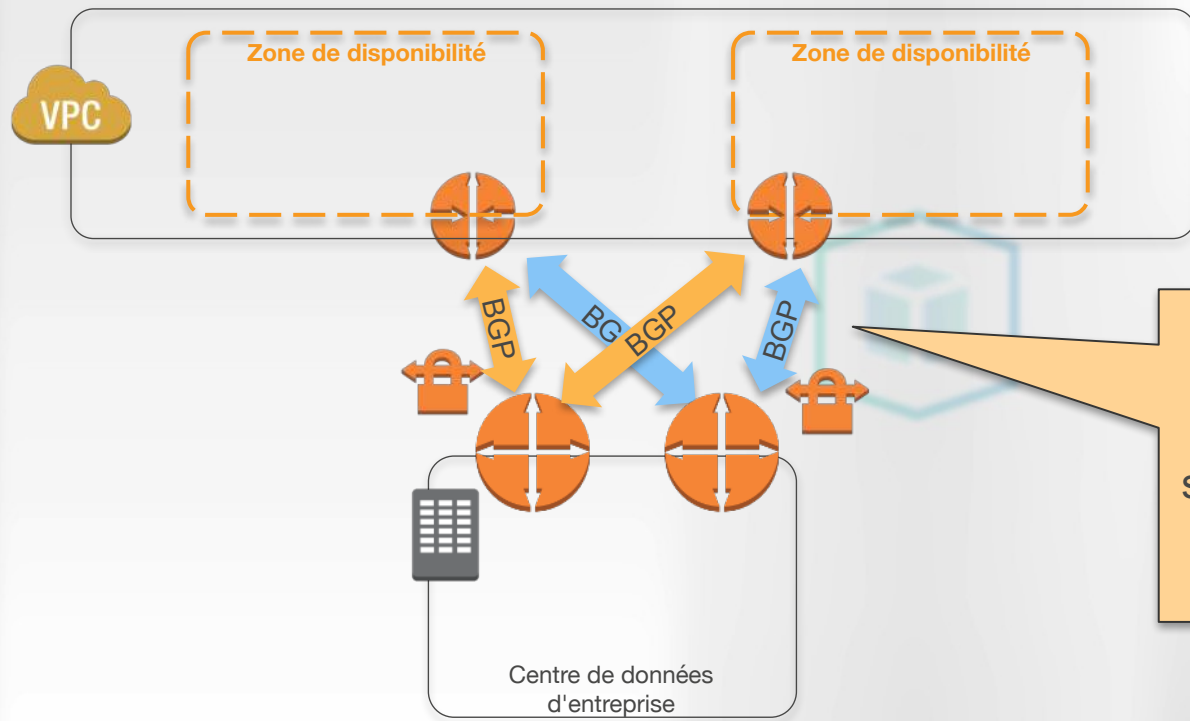
Chaque connexion VPN est composée de 2 tunnels IPsec redondants.

Utilisez BGP pour le routage.

Disponibilité :

Bonne 

Bonnes pratiques pour la connexion à distance

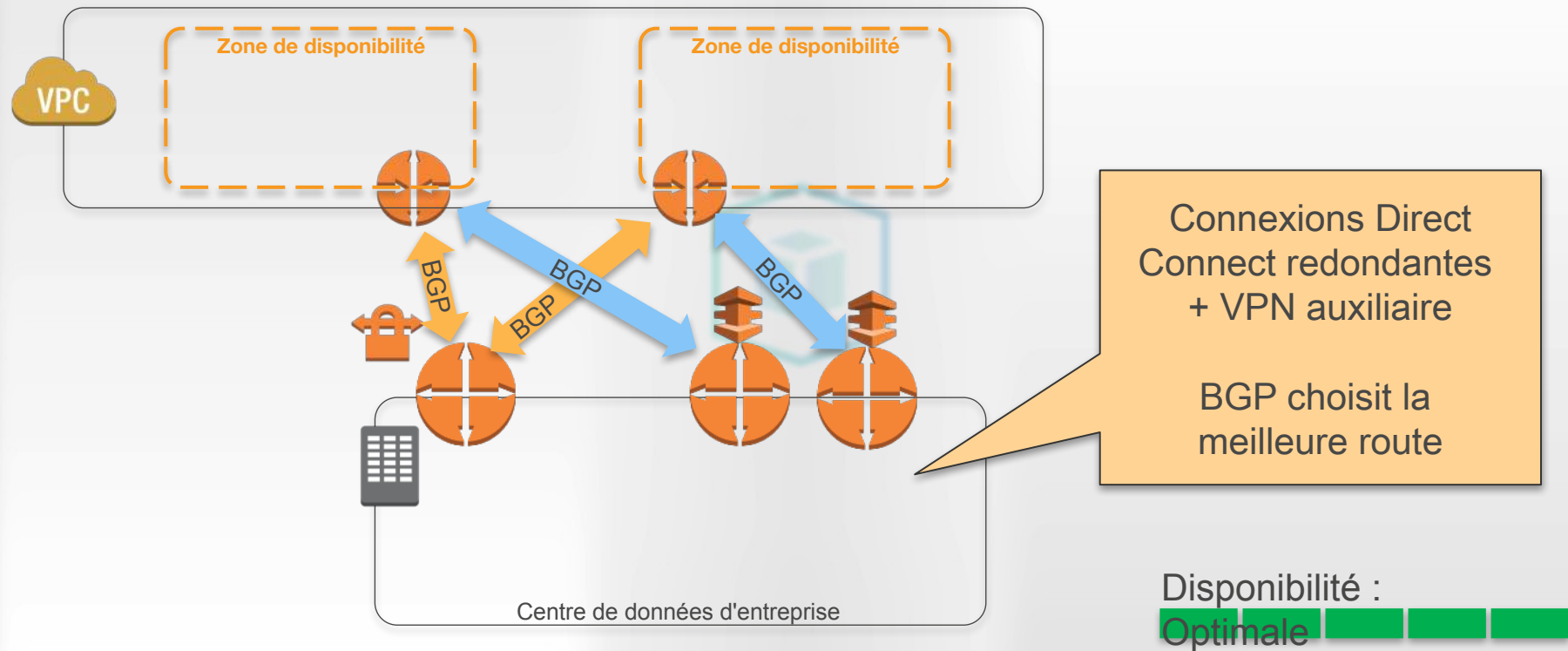


Deux connexions VPN
(4 tunnels IPsec au total)
sur des équipements différents
éliminent le SPOF côté client

Disponibilité :

Améliorée

Bonnes pratiques pour la connexion à distance



Sélection de routes (site client → VGW)

En cas de **connexions multiples**, plusieurs routes vers le VPN Gateway peuvent co-exister sur votre passerelle.

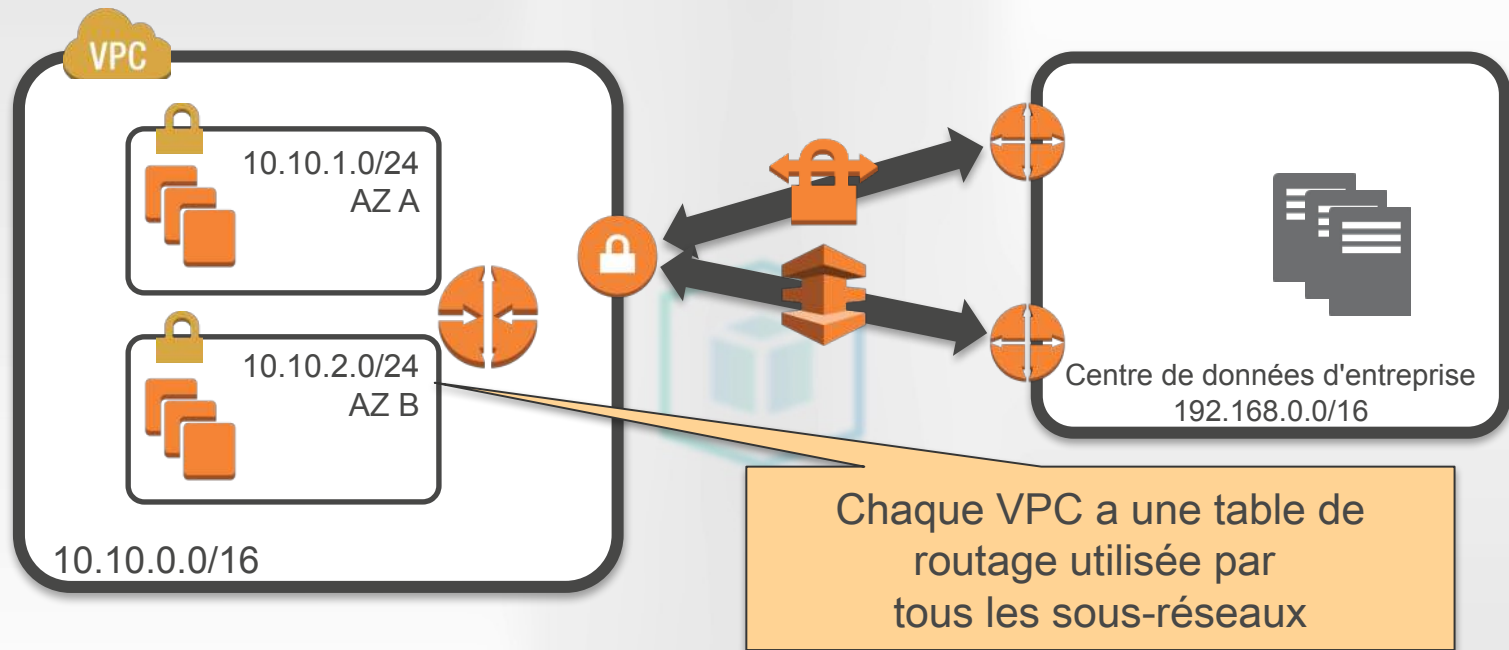
- A vous de jouer.
- Routes statiques : **gare au failover !**
- BGP est la meilleure solution
 - Actif / passif : vous pouvez **privilégier un chemin**, par ex. DX > VPN (Cisco : attributs *WEIGHT* et *LOCAL_PREFERENCE*)
 - Actif / actif : vous pouvez faire du **BGP Multipath** (Cisco : *BGP Link Bandwidth*)

Sélection de routes (VGW → site client)

En cas de **connexions multiples**, plusieurs routes vers la même destination peuvent co-exister sur votre Virtual Private Gateway.

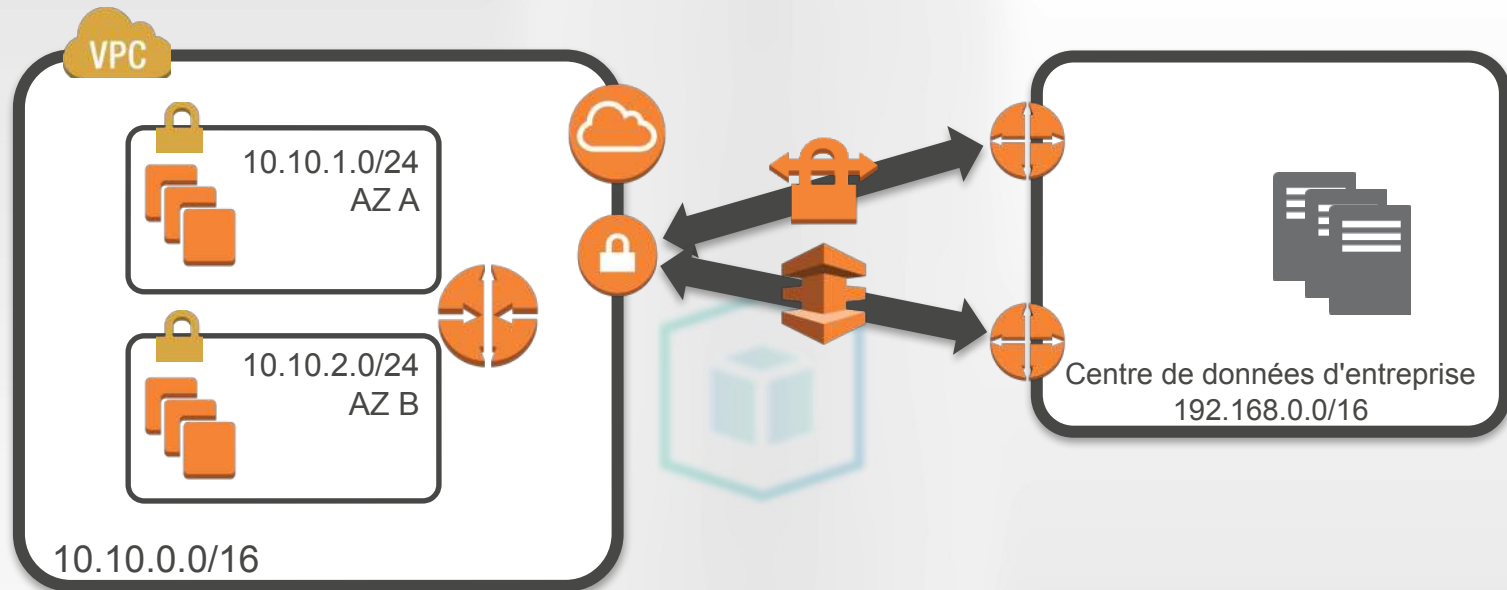
1. Le préfixe IP **le plus spécifique** est privilégié ($10.0.0.0/24 > 10.0.0.0/16$)
2. Égalité du préfixe ? Les routes **statiques** sont préférées aux routes BGP.
3. Routes BGP multiples ? Le chemin d'AS **le plus court** est privilégié.
 - Vous pouvez ajouter le préfixe **AS_PATH** pour défavoriser une route.
 - Lorsque les chemins d'AS sont de même longueur, la comparaison porte sur **l'origine** du chemin (IGP > EGP > inconnue).

Routage : route par défaut



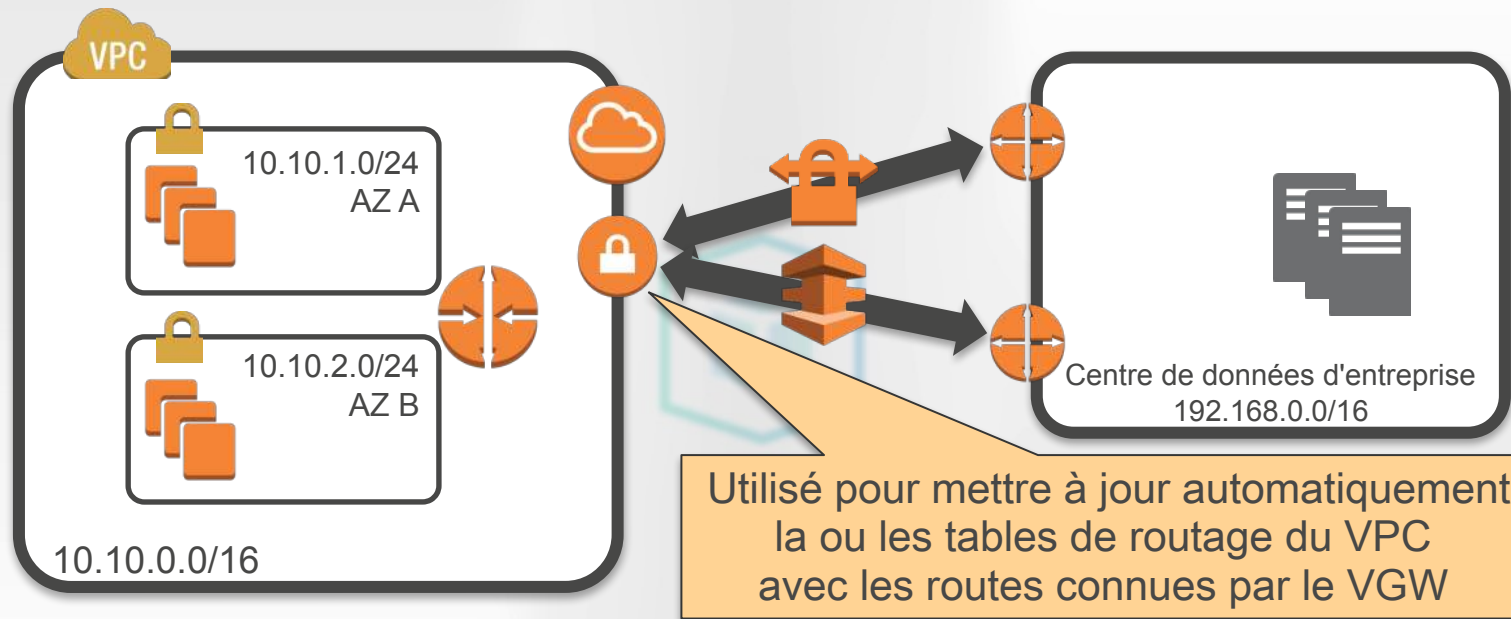
```
aws ec2 create-route --ro rtb-ef36e58a --dest 0.0.0.0/0 --gateway-id vgw-f9da06e7
```

Routage : connectivité privée et publique



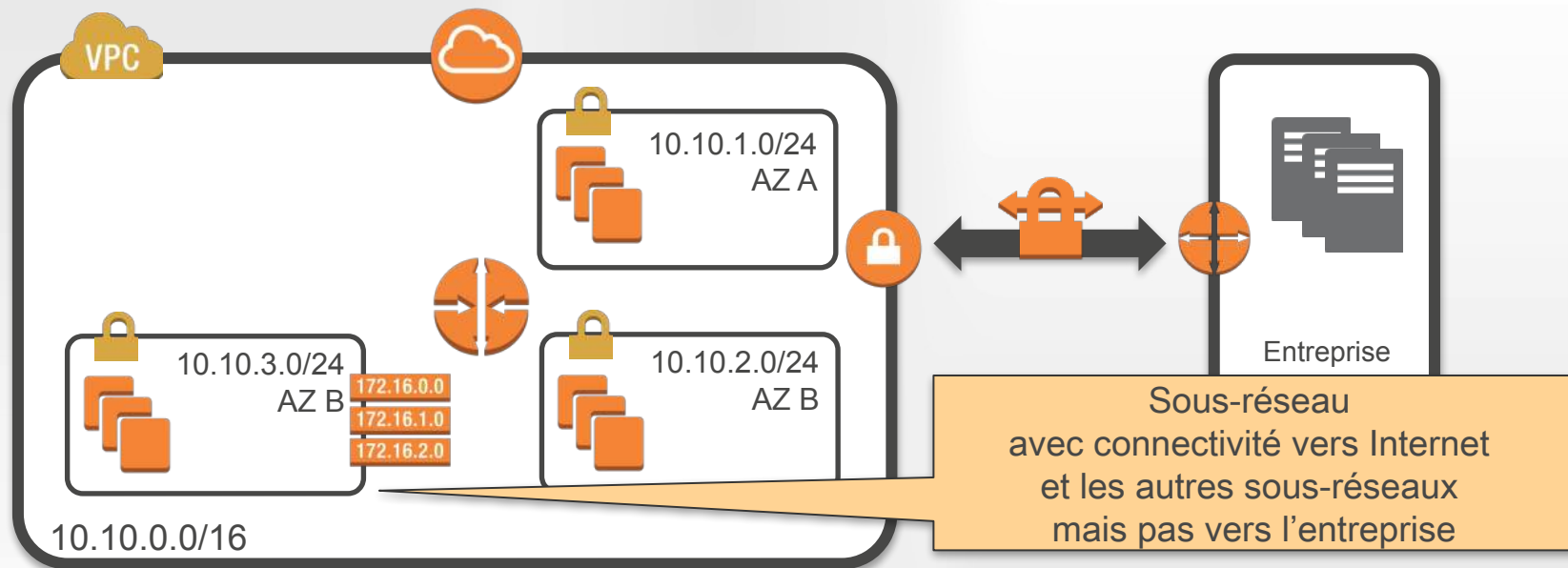
```
aws ec2 create-internet-gateway
aws ec2 attach-internet-gateway --internet igw-5a1ae13f --vpc vpc-c15180a4
aws ec2 delete-route --ro rtb-ef36e58a --dest 0.0.0.0/0
aws ec2 create-route --ro rtb-ef36e58a --dest 0.0.0.0/0 --gateway-id igw-5a1ae13f
aws ec2 create-route --ro rtb-ef36e58a --dest 192.168.0.0/16 --gateway-id vgw-f9da06e7
```

Routage : propagation des routes du VGW vers le VPC



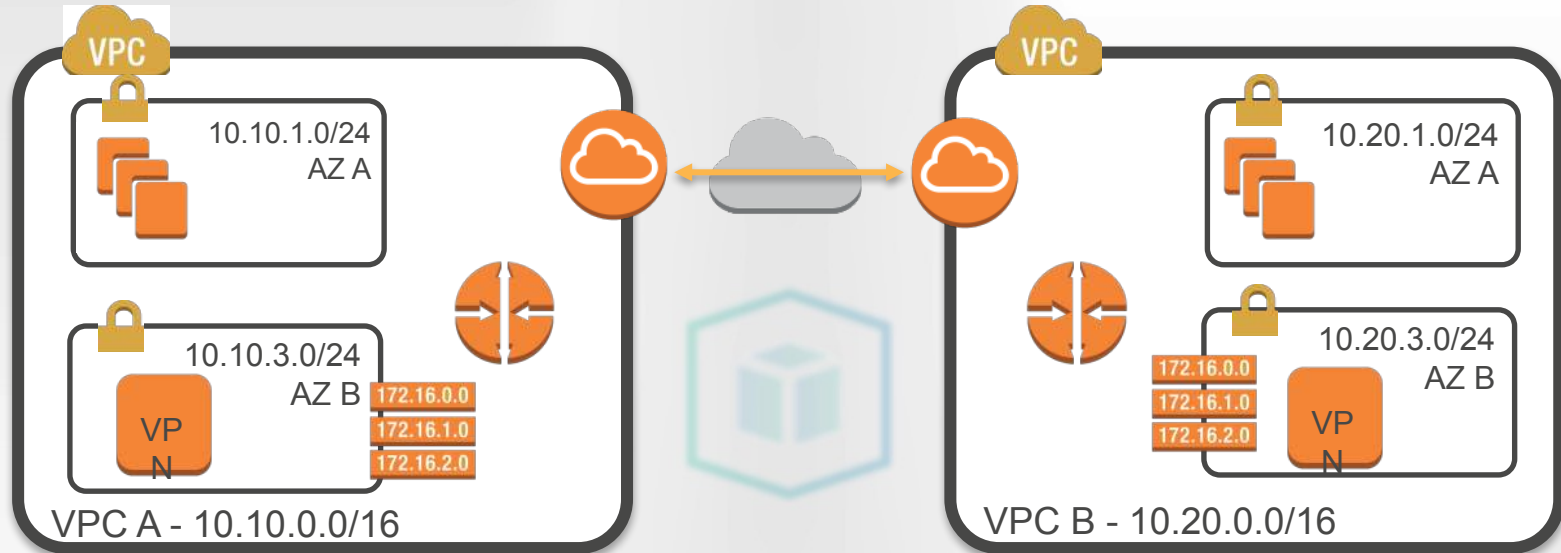
```
aws ec2 delete-route --ro rtb-ef36e58a --dest 192.168.0.0/16
aws ec2 enable-vgw-route-propagation --ro rtb-ef36e58a --gateway-id vgw-f9da06e7
```

Routage : table spécifique à un sous-réseau



```
aws ec2 create-subnet --vpc vpc-c15180a4 --cidr 10.10.3.0/24 --a us-west-2b
aws ec2 create-route-table --vpc vpc-c15180a4
aws ec2 associate-route-table --ro rtb-fc61b299 --subnet subnet-60975a17
aws ec2 create-route --ro rtb-ef36e58a --dest 0.0.0.0/0 --gateway-id igw-5a1ae13f
```

VPN logiciel sur EC2 pour relier deux VPCs



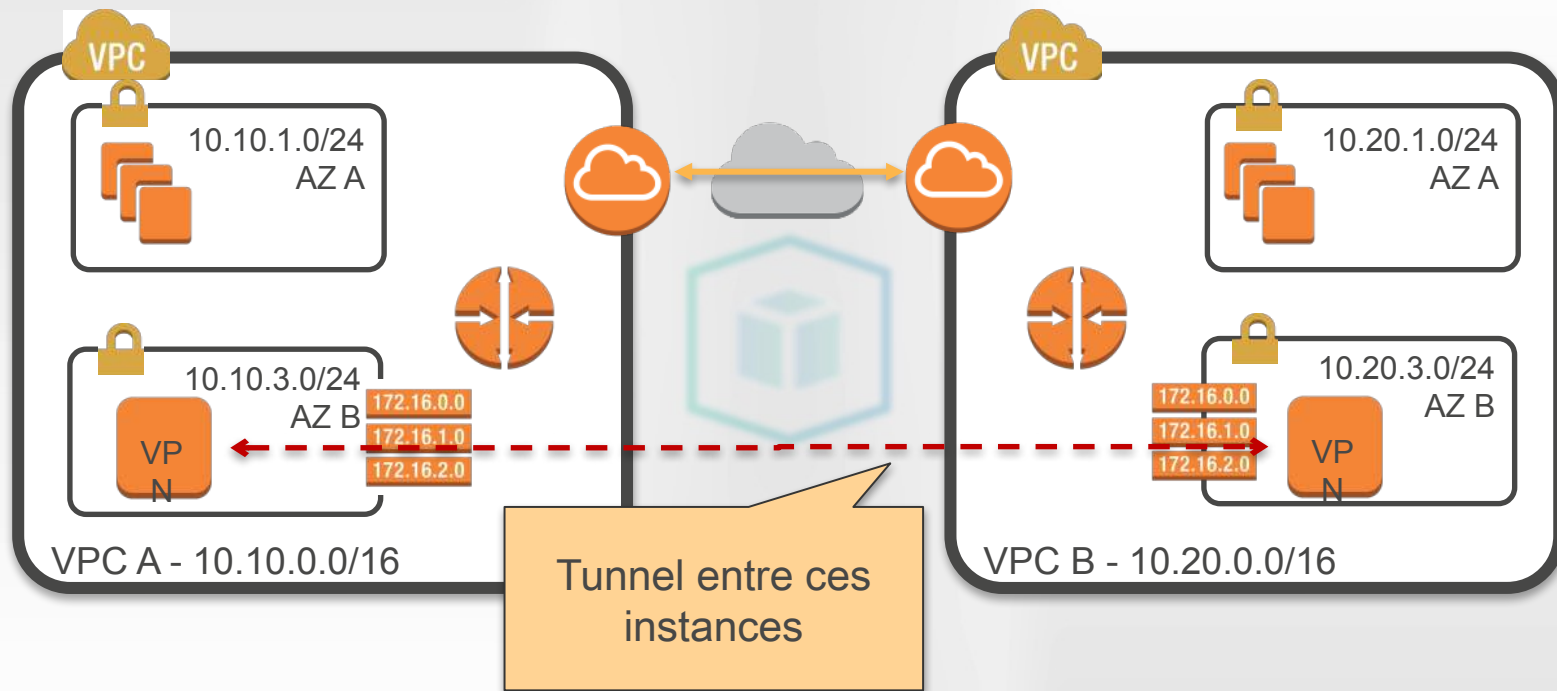
```
# VPC A
```

```
aws ec2 modify-network-interface-attribute --net eni-f832afcc --no-source-dest-check
```

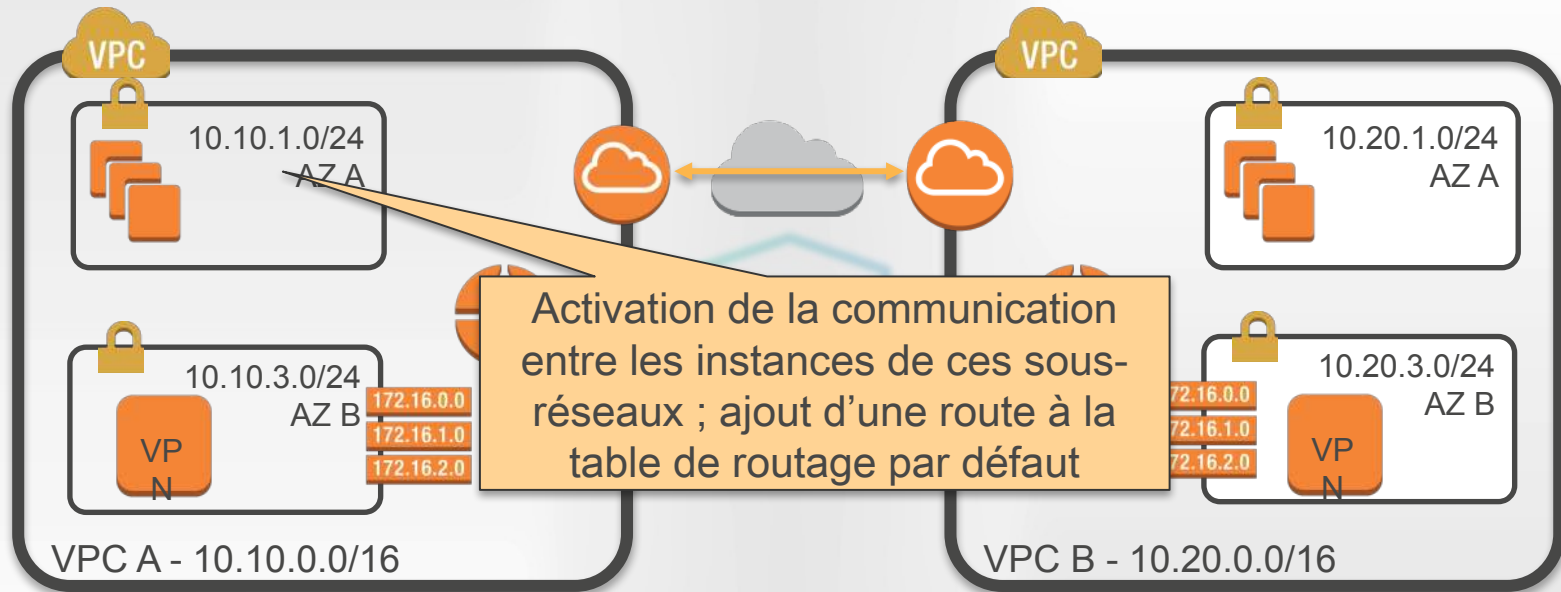
```
# VPC B
```

```
aws ec2 modify-network-interface-attribute --net eni-9c1b693a --no-source-dest-check
```

VPN logiciel sur EC2 pour relier deux VPCs



VPN logiciel sur EC2 pour relier deux VPCs



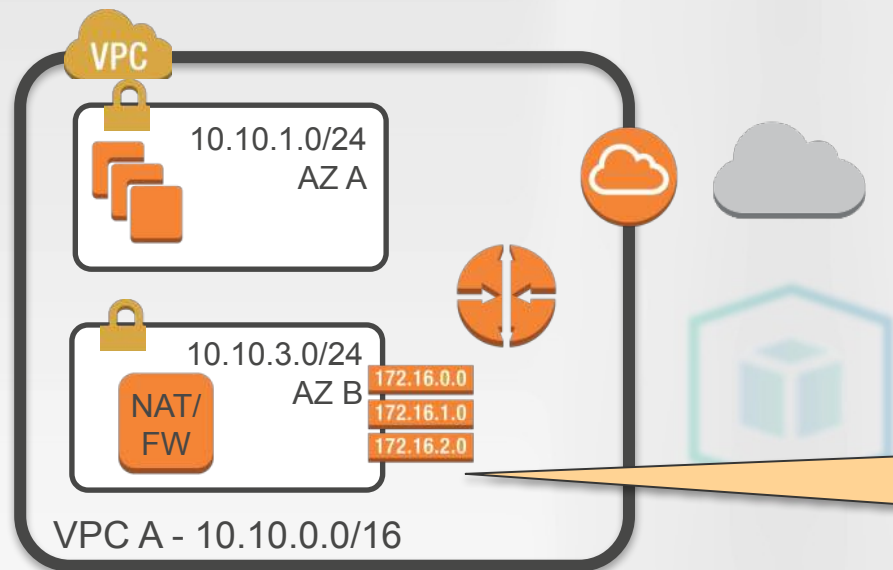
```
# VPC A
```

```
aws ec2 create-route --ro rtb-ef36e58a --dest 10.20.0.0/16 --instance-id i-f832afcc
```

```
# VPC B
```

```
aws ec2 create-route --ro rtb-67a2b31c --dest 10.10.0.0/16 --instance-id i-9c1b693a
```


Routage vers un pare-feu logiciel sur EC2



```
aws ec2 modify-network-interface-attribute --net eni-f832afcc --no-source-dest-check
```

```
# La table de routage par défaut dirige le trafic vers l'instance NAT/de pare-feu
```

```
aws ec2 create-route --ro rtb-ef36e58a --dest 0.0.0.0/0 --instance-id i-f832afcc
```

```
# Table de routage pour 10.10.3.0/24 dirige vers Internet
```

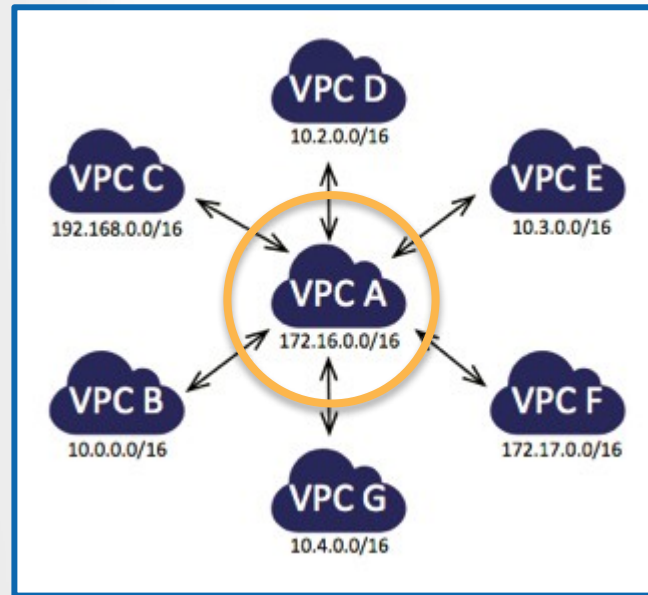
```
aws ec2 create-route --ro rtb-67a2b31c --dest 0.0.0.0/0 --gateway-id igw-5a1ae13f
```

Peering de VPC

Partager un VPC de services grâce au *peering*

Services de base

- Authentification / annuaire
- Monitoring
- Journalisation
- Administration à distance
- Audits de sécurité

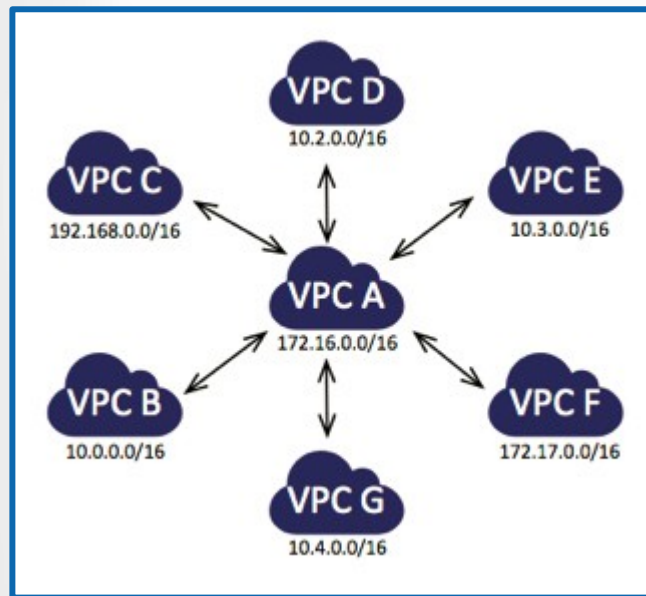


Découper son infrastructure avec le *peering*

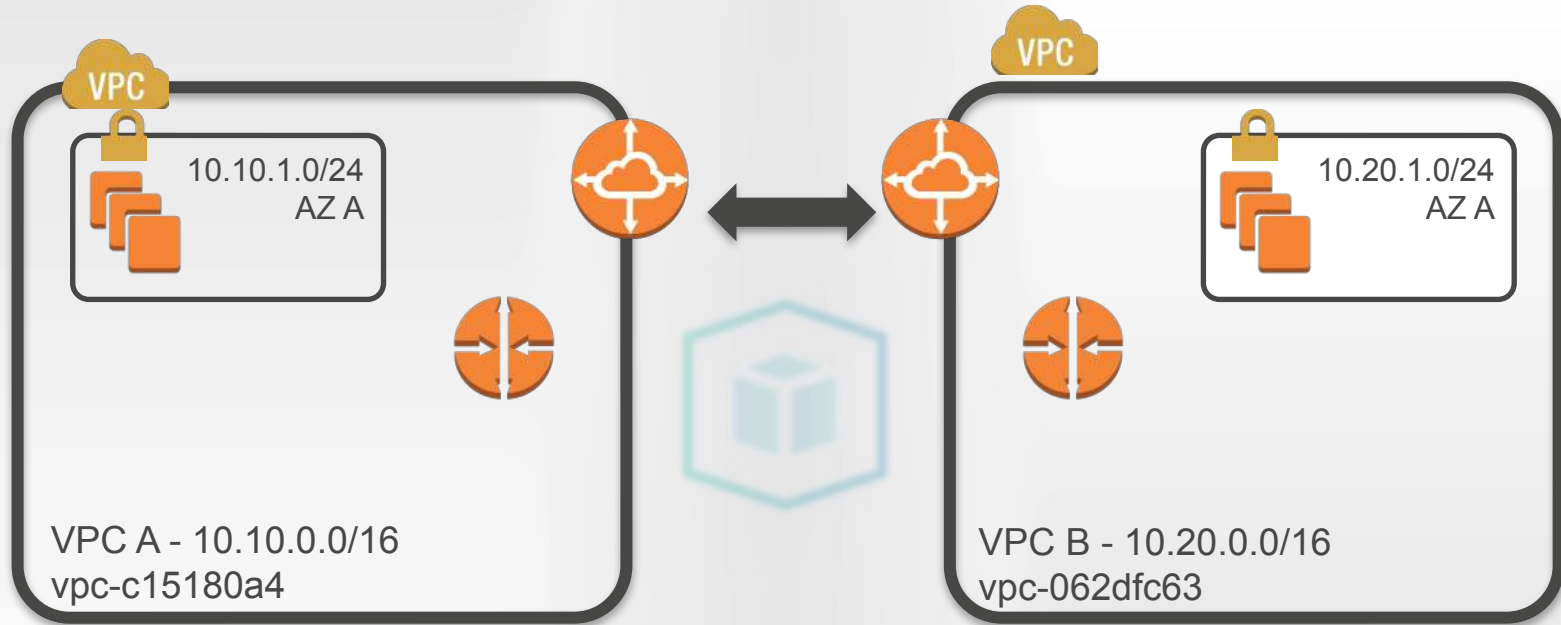
Développement : VPC B

Test : VPC C

Production : VPC D

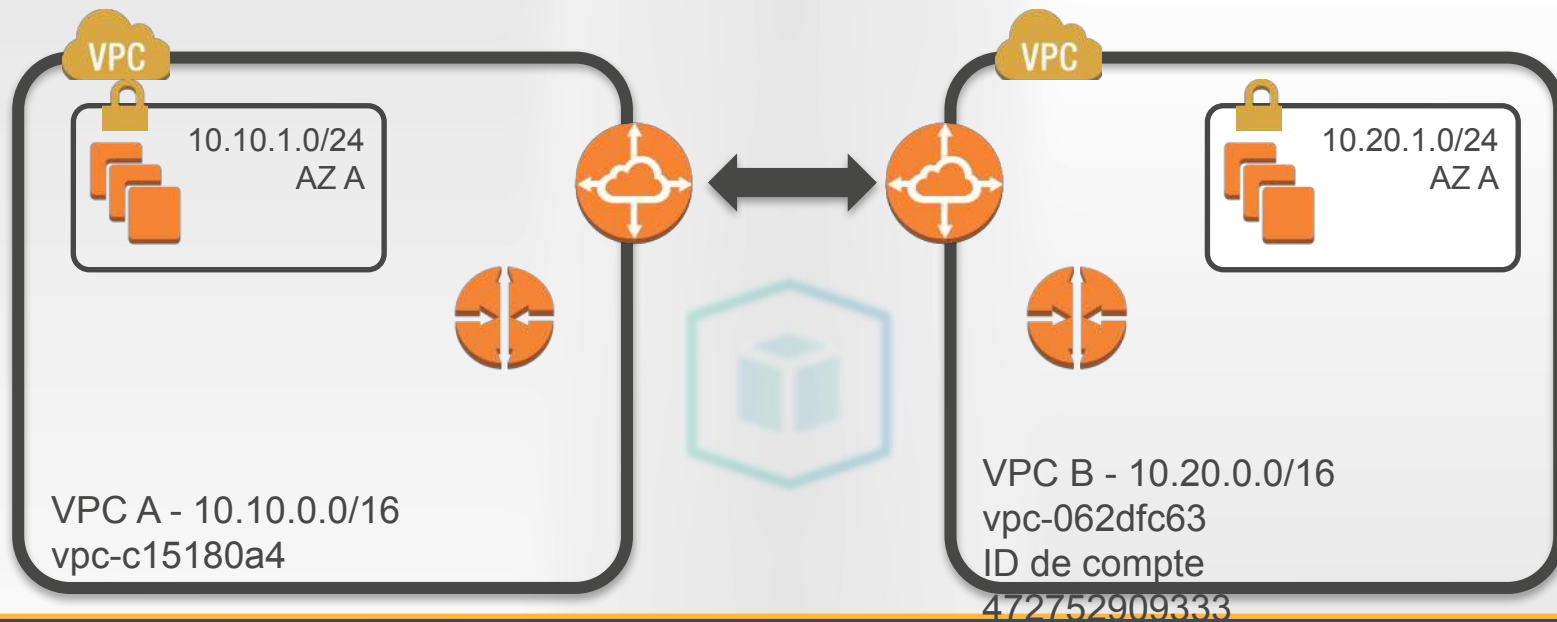


Peering entre VPC du même compte



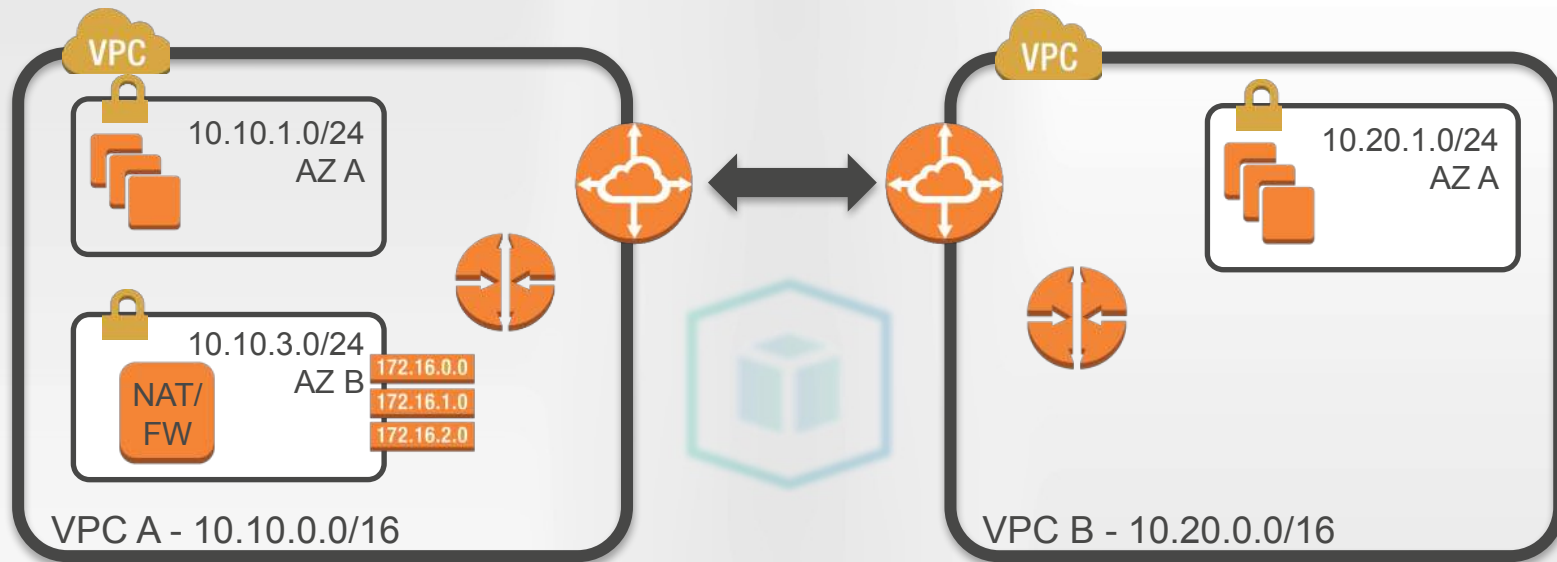
```
aws ec2 create-vpc-peering-connection --vpc-id vpc-c15180a4 --peer-vpc vpc-062dfc63
aws ec2 accept-vpc-peering-connection --vpc-peer pcx-ee56be87
VPC A> aws ec2 create-route --ro rtb-ef36e58a --des 10.20.0.0/16 --vpc-peer pcx-ee56be87
VPC B> aws ec2 create-route --ro rtb-67a2b31c --des 10.10.0.0/16 --vpc-peer pcx-ee56be87
```

Peering entre VPC de comptes différents



```
aws ec2 create-vpc-peering-connection --vpc-id vpc-c15180a4 --peer-vpc vpc-062dfc63
--peer-owner 472752909333
# Dans le compte propriétaire 472752909333
aws ec2 accept-vpc-peering-connection --vpc-peer pcx-ee56be87
```

Peering de VPC avec une pare-feu dans EC2



```
# La table de routage par défaut dirige le trafic peeré vers l'instance pare-feu
aws ec2 create-route --ro rtb-ef36e58a --dest 10.20.0.0/16 --instance-id i-f832afcc

# Table de routage pour 10.10.3.0/24 dirige vers le peer
aws ec2 create-route --ro rtb-67a2b31c --dest 10.20.0.0/16 --vpc-peer pcx-ee56be87
```

Peering de VPC – considérations supplémentaires

Les VPC doivent être dans la même région.

Les plages d'adresses des VPC ne peuvent pas se chevaucher.

Routage : utilisez les adresses privées IPv4 ou IPv6 (depuis Décembre 2016).

Security groups: depuis mars 2016, il est possible de les référencer entre VPCs.

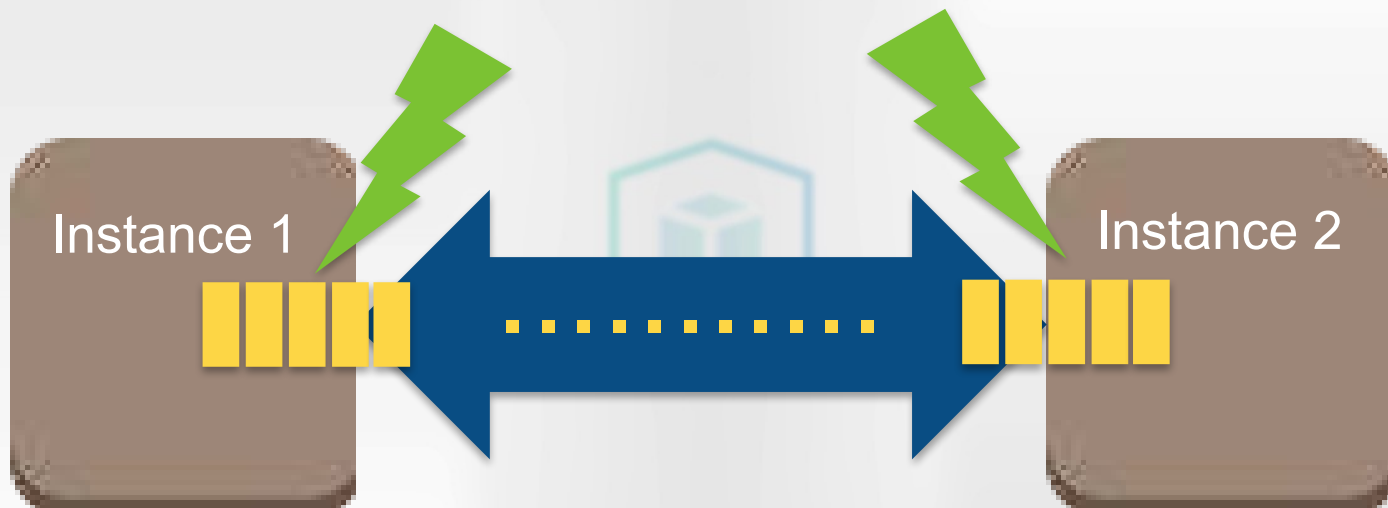
DNS: depuis juillet 2016, il est possible de résoudre les adresses privées entre VPCs.

Pas de transitivité pour VPN, Direct Connect ou les VPC tiers

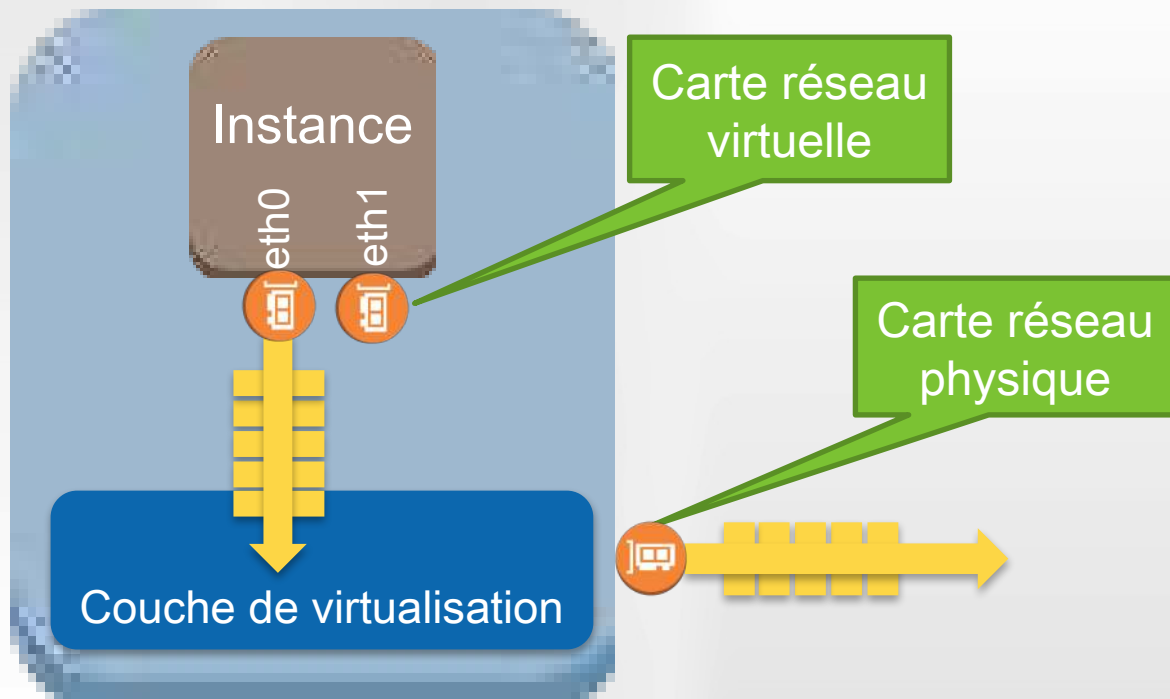
- Exemple : impossible d'accéder au VPC C à partir du VPC A via le VPC B
- Solution : créez un *peering* entre le VPC A vers le VPC C

Enhanced Networking

Latence : paquets par seconde



Traitement des paquets dans Amazon EC2 : VIF

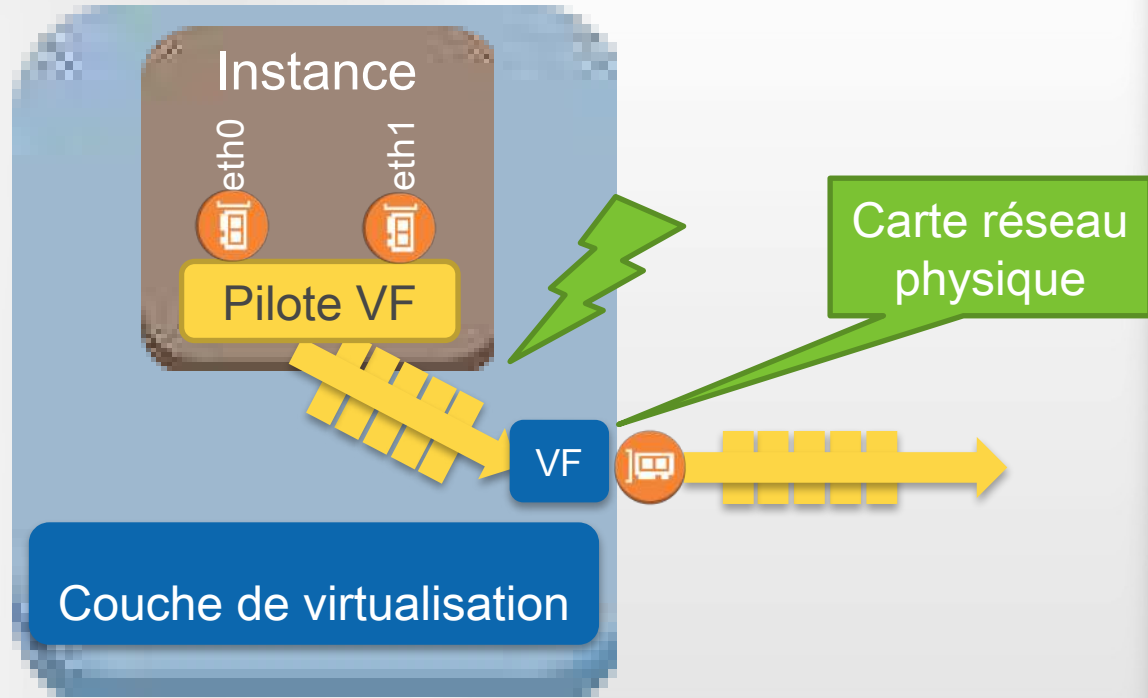


Traitement des paquets dans Amazon EC2 : SRIOV (Single Root I/O Virtualization)

Les paquets ne traversent **plus** la couche de virtualisation.

Le pilote réseau de votre instance a **directement** accès à l'interface physique.

Il doit être **configuré** sur votre instance.



Latence entre instances



SR-IOV : Est-ce prêt ?



Pour un grand nombre d'AMI récentes, *Enhanced Networking* est déjà activé :

- AMI Amazon Linux les plus récentes
- AMI Windows Server 2012 R2

Aucune configuration nécessaire

SRIOV : Est-ce prêt ? (Linux)

Non

```
[ec2-user@ip-10-0-3-70 ~]  
$ ethtool -i eth0
```

```
driver: vif  
version:  
firmware-version:  
bus-info: vif-0  
...
```

Oui !

```
[ec2-user@ip-10-0-3-70 ~]$  
ethtool -i eth0
```

```
driver: ixgbev   
version: 2.14.2+amzn  
firmware-version: N/A  
bus-info: 0000:00:03.0
```

```
...
```

Support de SRIOV

- Familles d'instances :
C3, C4, I2, D2, R3, R4, M4, P2, X1
- Virtualisation HVM
- Version de noyau obligatoire
 - Linux : 2.6.32+
 - Windows : Server 2008 R2+
- Pilote VF approprié
 - Linux : module ixgbev 2.14.2+
 - Windows : Pilote de fonction virtuel Intel® 82599



Activation *Enhanced* Networking (Amazon Linux)

```
C:\>aws ec2 describe-images --image-id ami-e965ba80
```

DescribeImages	
Images	
Architecture	x86_64
Description	Amazon Linux AMI x86_64 HVM EBS
Hypervisor	xen
ImageId	ami-e965ba80
ImageLocation	amazon/amzn-ami-hvm-2012.03.1.x86_64-ebs
ImageOwnerAlias	amazon
ImageType	amazon/amzn-ami-hvm-2012.03.1.x86_64-ebs
State	available
VirtualizationType	hvm
BlockDeviceMappings	
DeviceName	/dev/sda1
Ebs	
DeleteOnTermination	True
Encrypted	False
SnapshotId	snap-9db2e1e7
VolumeSize	8
VolumeType	standard

amzn-ami-hvm-2012.03.1.x86_64-ebs

hvm

Activation *Enhanced Networking* (Amazon Linux)

```
C:\>aws ec2 describe-instance-attribute --  
instance-id i-37c5d1d9 --attribute  
sriovNetSupport
```

```
-----  
| DescribeInstanceAttribute |  
+-----+-----+  
| InstanceId | i-37c5d1d9 |  
+-----+-----+
```

Pas encore !

Activation *Enhanced Networking* (Amazon Linux)

Using username "ec2-user".

Authentification avec la clé publique "imported-openssh-key"

```
__|  __|_ )  
_| (  /   AMI Amazon Linux  
__|\__|__|
```

Accédez à `/usr/share/doc/system-release/` pour consulter les dernières notes de publication.

Il y a 46 mises à jour de sécurité sur 254 disponibles au total.

Exécutez "sudo yum update" pour appliquer toutes les mises à jour.

La version Amazon Linux 2014.09 est disponible.

```
[ec2-user@ip-10-0-3-125 ~]$ sudo yum update
```

Plug-ins chargés : fastestmirror, priorities, security, update-motd

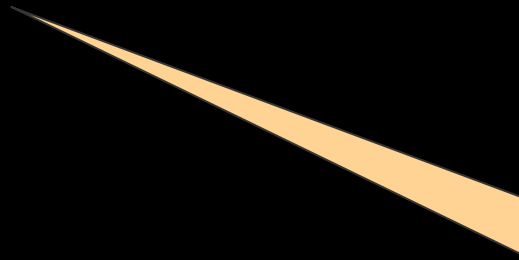
Le chargement du miroir accéléré depuis le fichier hôte mis en cache

...

Mise à jour du
système
d'exploitation

Activation *Enhanced Networking* (Amazon Linux)

```
C:\>aws ec2 reboot-instances --instance-id  
i-37c5d1d9
```



Redémarrer
(Mise à jour du
système
d'exploitation)

Activation *Enhanced Networking* (Amazon Linux)

```
C:\>aws ec2 stop-instances --instance-id  
i-37c5d1d9
```

...




Arrêter l'instance

Activation *Enhanced Networking* (Amazon Linux)

```
C:\>aws ec2 stop-instances --instance-id  
i-37c5d1d9
```

...

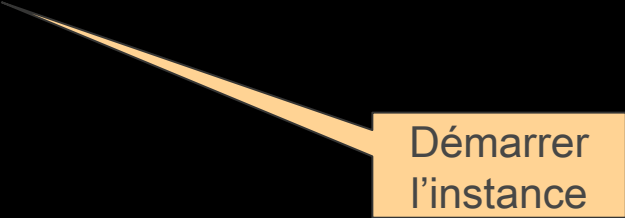
```
C:\>aws ec2 modify-instance-attribute --  
instance-id i-37c5d1d9 --sriov-net-support  
simple
```



Activer SRIOV
Impossible d'annuler

Activation *Enhanced Networking* (Amazon Linux)

```
C:\>aws ec2 start-instances --instance-id i-37c5d1d9
```



Démarrer
l'instance

Activation *Enhanced Networking* (Amazon Linux)

```
C:\>aws ec2 start-instances --instance-id i-37c5d1d9
```

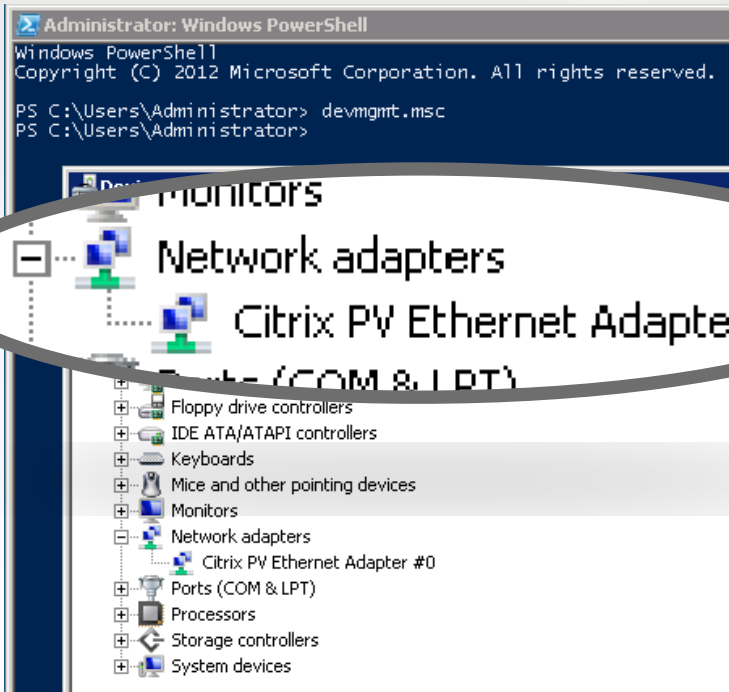
```
C:\>aws ec2 describe-instance-attribute --instance-id i-37c5d1d9 --attribute sriovNetSupport
```

```
-----  
| DescribeInstanceAttribute |  
+-----+-----+  
| InstanceId | i-37c5d1d9 |  
+-----+-----+  
||           SriovNetSupport           ||  
|+-----+-----+|  
|| Value      | simple ||  
|+-----+-----+|
```

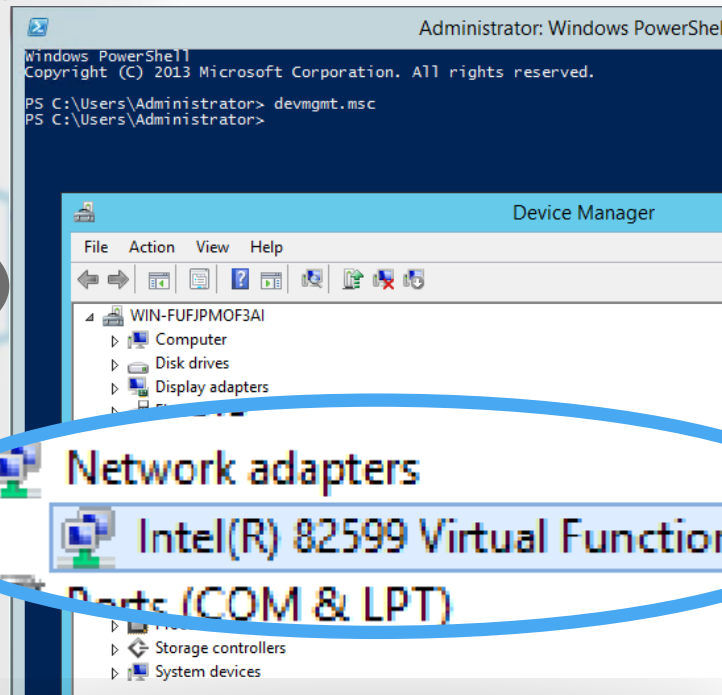
C'est parti !

SRIOV : Est-ce prêt ? (Windows)

Non



Oui !



Activation *Enhanced* Networking (Windows)



Intel® Network Adapter Driver for Windows Server 2012 R2*

Version: 21.1 (Latest)

Date: 10/11/2016

Available Downloads

Windows Server 2012 R2*

Language: English

Size: 77.57 MB

MD5:

be178e39d982723e6505aa6b2e062573

PROWinx64.exe

Detailed Description

Not sure if this is the right driver or software for your component? Run [Intel® Driver Update Utility](#) to automatically detect driver or software updates.

Purpose

Installs base drivers, Intel® PROSet Software for Windows* Device Manager, advanced networking services for teaming and VLANs (ANS), and SNMP for Intel® Network Adapters for Windows Server 2012 R2*.

See the **release notes** for installation instructions, supported hardware, what is new, bug fixes, and known issues.

Activation *Enhanced Networking* (Windows)

Ajouter le pilote Windows

```
PS C:\temp> pnputil -a .  
\PROWinx64\PROXGB\Winx64\NDIS63\vxn63x64.inf
```

Utilitaire Microsoft PnP

Traitement inf : vxn63x64.inf

Package de pilote ajouté avec succès.

Nom publié : oem6.inf

Nombre total de tentatives : 1

Nombre d'importations réussies : 1

Points de terminaison VPC pour Amazon S3

Points de terminaison VPC pour Amazon S3

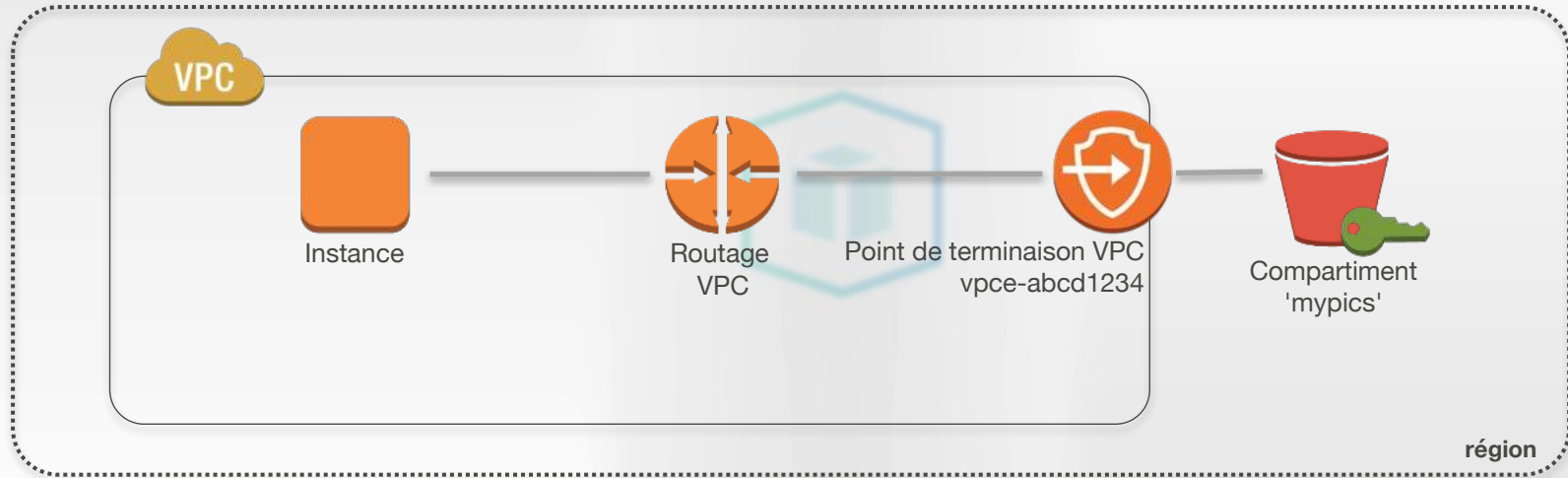


Utile pour les sous-réseaux privés qui n'ont **pas d'accès direct à Internet**, voire pas d'accès du tout

Possibilité d'utiliser S3 à l'intérieur du VPC, **sans passer par Internet** (via VPN ou Direct Connect)

Optimisation de la **bande passante**, meilleures **performances** et **sécurité** accrue

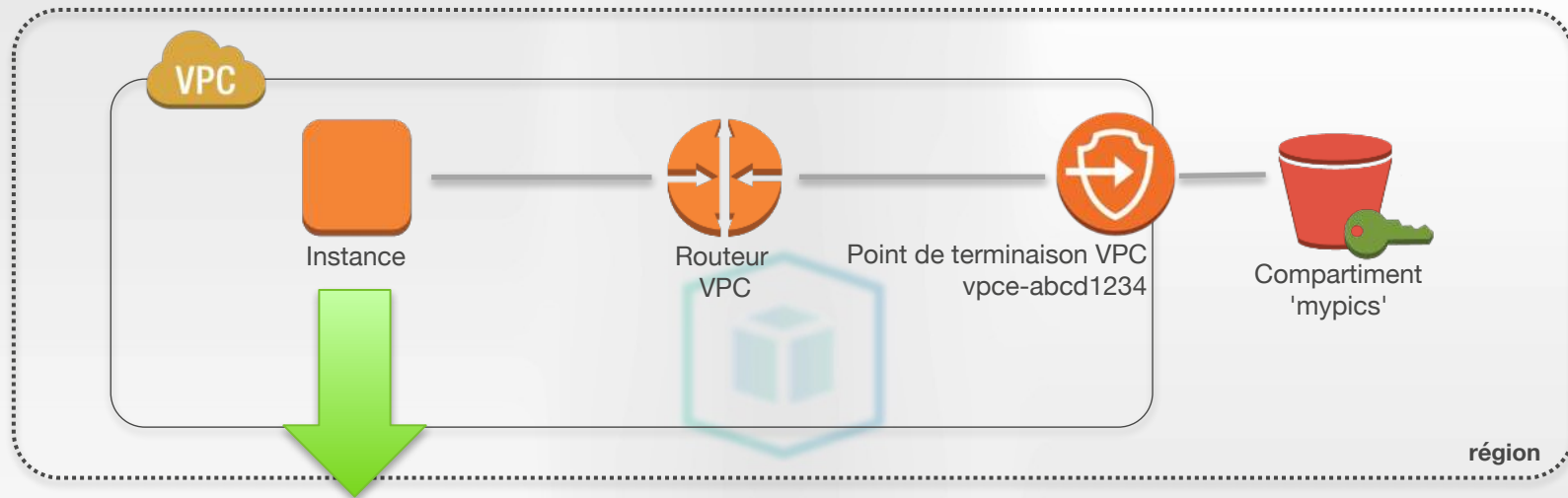
Points de terminaison VPC pour Amazon S3



Création d'un point de terminaison VPC

```
ec2-create-vpc-endpoint  
vpc-1a2b3c4d  
-s com.amazonaws.us-west-2.s3  
-r rtb-11aa22bb  
--policy-document mypolicy.json
```

Points de terminaison VPC pour Amazon S3

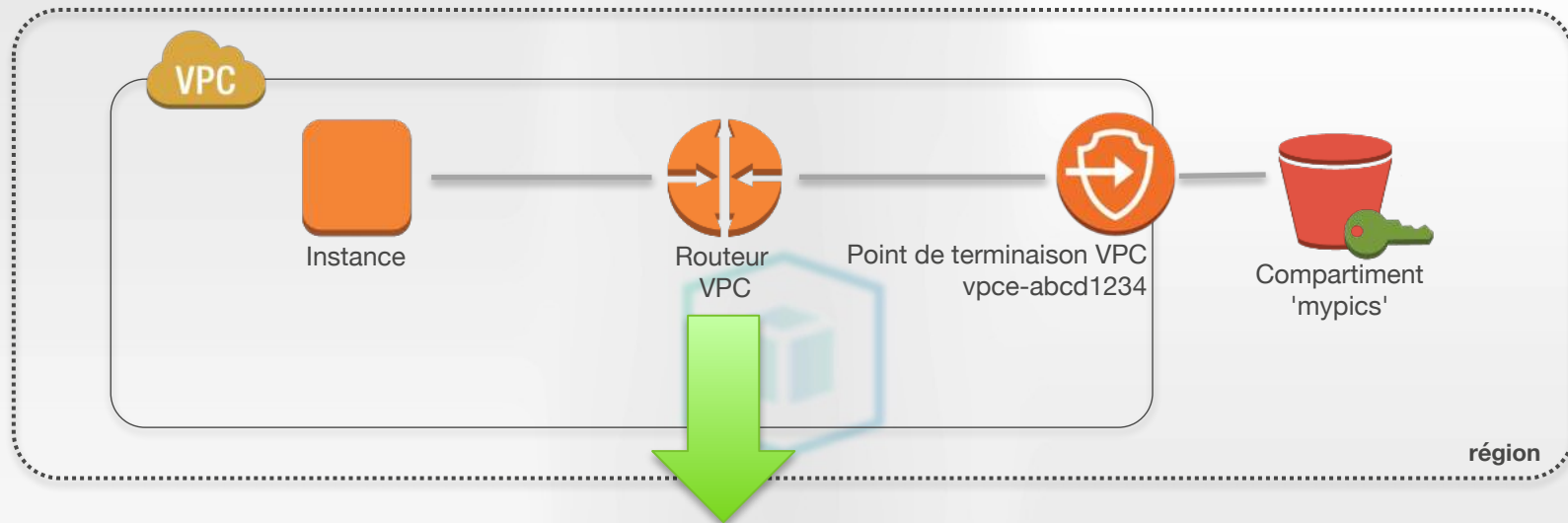


L'application résout `mypics.s3.amazonaws.com`

Le DNS répond avec les adresses IP habituelles d'Amazon S3

L'application se connecte à l'adresse IP sélectionnée

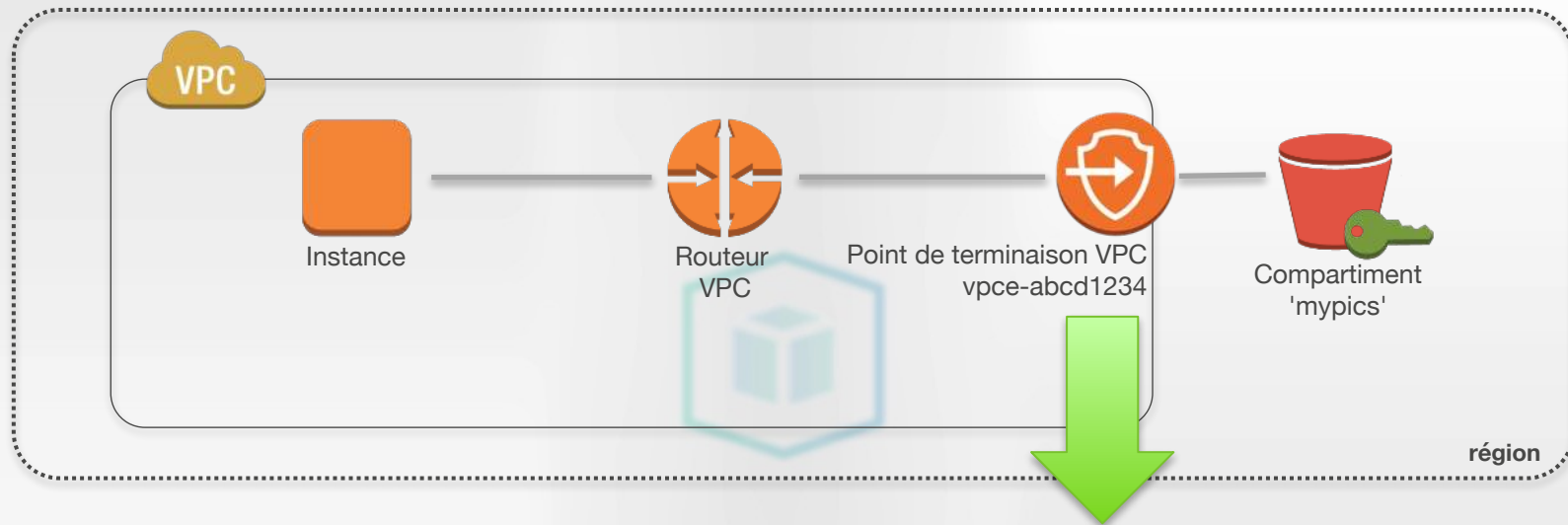
Points de terminaison VPC pour Amazon S3



Liste de préfixe
com.amazonaws.us-west-1.s3

Destination	Cible
pl-1a2b3c4d	vpce-abcd1234

Points de terminaison VPC pour Amazon S3



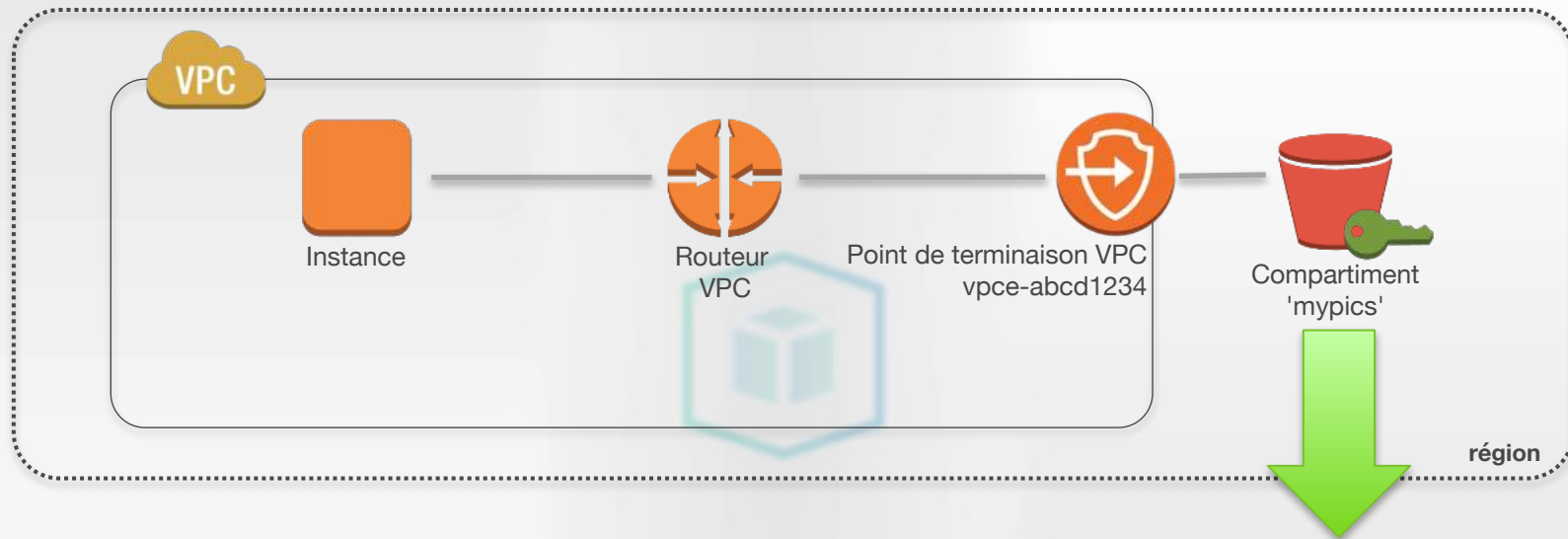
Stratégie IAM sur le point de terminaison VPC vpce-abcd1234

- Autoriser l'accès au compartiment 'mypics'
- Refuser l'accès aux autres compartiments

Stratégie IAM de point de terminaison VPC

```
{ "Statement": [  
  {  
    "Sid": "Access-to-specific-bucket-only",  
    "Principal": "*",  
    "Action": [ "s3:GetObject", "s3:PutObject"  
    ],  
    "Effect": "Allow",  
    "Resource": ["arn:aws:s3:::mypics",  
                  "arn:aws:s3:::mypics/*"]  
  }  
]
```

Points de terminaison VPC pour Amazon S3



Stratégie IAM sur le compartiment 'mypics'

- Autoriser l'accès à partir de `vpce-abcd1234`
- Refuser tous les autres

Stratégie IAM de compartiment S3

```
{ "Version": "2012-10-17", "Id": "Policy1415115909152",  
  "Statement": [  
    {  
      "Sid": "Access-to-specific-VPCE-only",  
      "Principal": "*",  
      "Action": "s3:*",  
      "Effect": "Deny",  
      "Resource": ["arn:aws:s3:::mypics",  
                   "arn:aws:s3:::mypics/*"],  
      "Condition": {  
        "StringNotEquals": {  
          "aws:sourceVpce": "vpce-abcd1234"  
        }  
      }  
    }  
  ] }
```

TIRED.



JUST TIRED.

quickmeme.com

Ressources complémentaires



AWS re:Invent 2016: Tuesday Night Live with James Hamilton

<https://www.youtube.com/watch?v=AyOAJFNPAAbA>

AWS re:Invent 2016: Creating Your Virtual Data Center: VPC Fundamentals and Connectivity (NET201)

<https://www.youtube.com/watch?v=UI2NsPNh9Ik>

AWS re:Invent 2016: NEW LAUNCH IPv6 in the Cloud: Protocol and AWS Service Overview (NET204)

<https://www.youtube.com/watch?v=Uvgyxncu9MY>

AWS re:Invent 2016: NextGen Networking: New Capabilities for Amazon's Virtual Private Cloud (NET303)

<https://www.youtube.com/watch?v=G24h4PuAOrs>

AWS re:Invent 2016: Extending Datacenters to the Cloud (NET305)

<https://www.youtube.com/watch?v=F2AWkGem7Sw>

AWS re:Invent 2016: Another Day, Another Billion Packets (NET401)

<https://www.youtube.com/watch?v=St3SE4LWhKo>

AWS re:Invent 2016: Deep Dive: AWS Direct Connect and VPNs (NET402)

<https://www.youtube.com/watch?v=Qep11X1r1QA>

Merci !

Julien Simon

Principal Technical Evangelist, AWS

julsimon@amazon.fr

@julsimon

Lundi

- Bonnes pratiques d'authentification avec AWS IAM
- Chiffrez vos données avec AWS

Mardi

- Fireside chat avec Matthieu Bouthors et Julien Simon
- Re:Invent update 1

Mercredi

- Deep dive : Amazon Virtual Private Cloud
- Bonnes pratiques anti-DDoS

Jeudi

- Re:Invent update 2
- Gérez les incidents de sécurité avec AWS CloudTrail

Vendredi

- Automatisez vos audits de sécurité avec Amazon Inspector
- Bonnes pratiques de sécurité sur AWS