

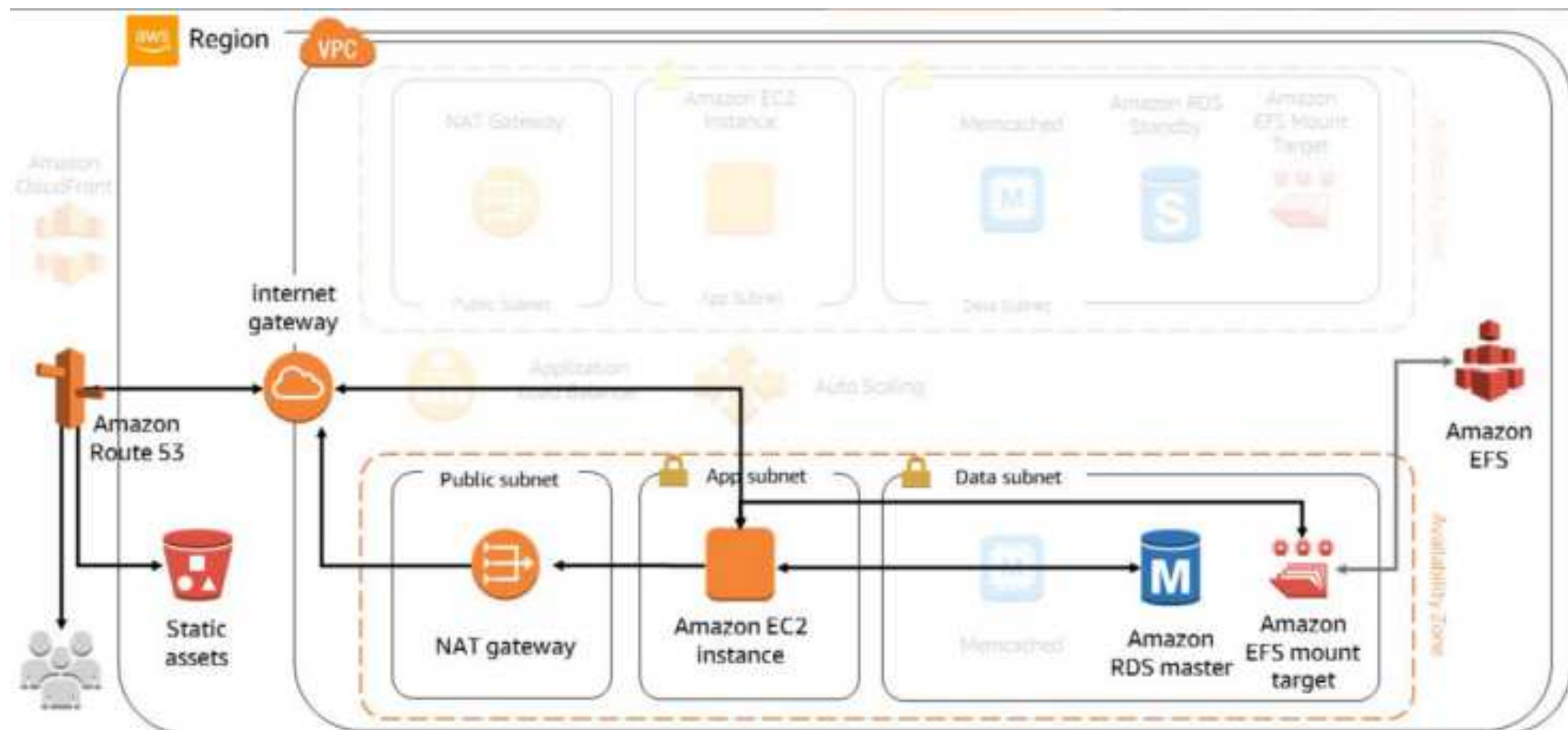


**2.5**

## **Capa de red VPC**

## 2.5 Capa de red VPC

- Virtual Private Cloud y DNS



## 2.5 Capa de red VPC

- Virtual Private Cloud
  - Subredes
  - Gateways
  - Seguridad de red
  - VPC peering
  - Cloud hybrido VPN
- DNS
  - Servicio Route53

## 2.5 Capa de red VPC

- Virtual Private Cloud



Your private network  
space in the AWS Cloud



Provides logical isolation  
for your workloads



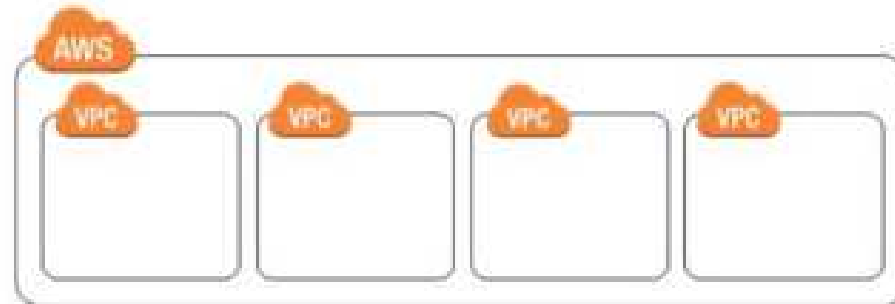
Allows custom access  
controls and security  
settings for your resources

## 2.5 Capa de red VPC

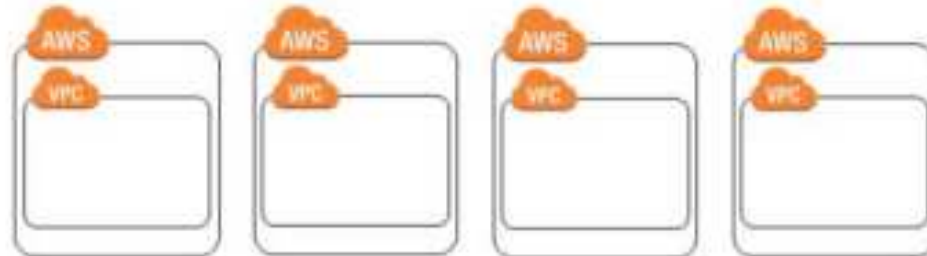
- Una VPC es una red dedicada y aislada para una cuenta AWS
- IPv4 , IPv6
- Permite crear subredes CIDR
- Permite crear reglas de acceso para trafico saliente y entrante
- Cada VPC se despliega en una región
  - **Una VPC puede albergar recursos de diferentes zonas de disponibilidad**

## 2.5 Capa de red VPC

- Patrón multi-vpc



- Patrón multi-cuenta



## 2.5 Capa de red VPC

- 5 VPC por región



**Service Limit:** 5 VPCs per region per account

## 2.5 Capa de red VPC

- Direccionamiento IP
  - Permite direccionamiento privado y publico
  - Permite asociación dinamica o fija
  - No hay cargo económico con direcciones privadas
  - CIDR
- Cada subred reside únicamente en una zona de disponibilidad
- Una zona de disponibilidad puede contener varias subredes

0.0.0.0/0	= All IPs
10.22.33.44/32	= 10.22.33.44
10.22.33.0/24	= 10.22.33.*
10.22.0.0/16	= 10.22.*.*



## 2.5 Capa de red VPC

- Tablas de enrutamiento
  - Cada VPC tiene una tabla por defecto
  - Se pueden crear tablas de enrutamiento
  - Toda subred debe de tener asociada una tabla de enrutamiento
- Utilizar subredes publicas y privadas para limitar la accesibilidad



### Public subnets

- Include a **routing table** entry to an **internet gateway** to support inbound/outbound access to the public internet

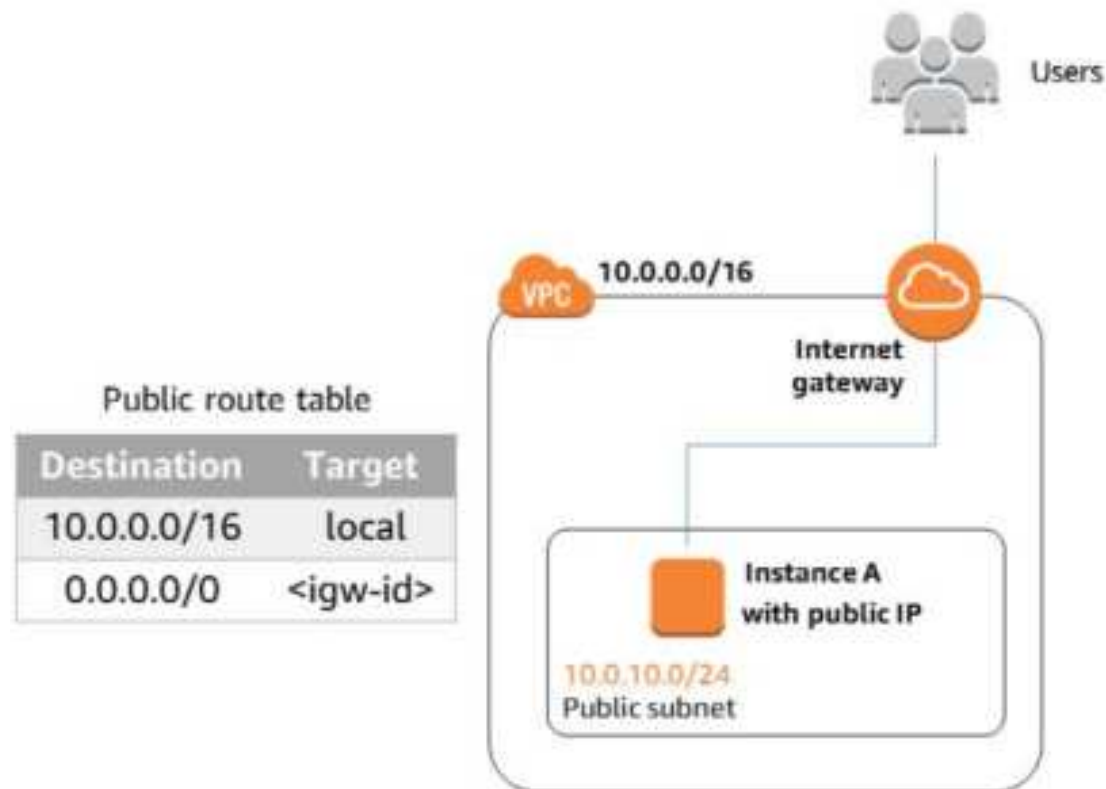


### Private subnets

- **Do not have a routing table entry to an internet gateway**
- Are not directly accessible from the public internet
- Typically use a **NAT gateway** to support restricted, outbound public internet access

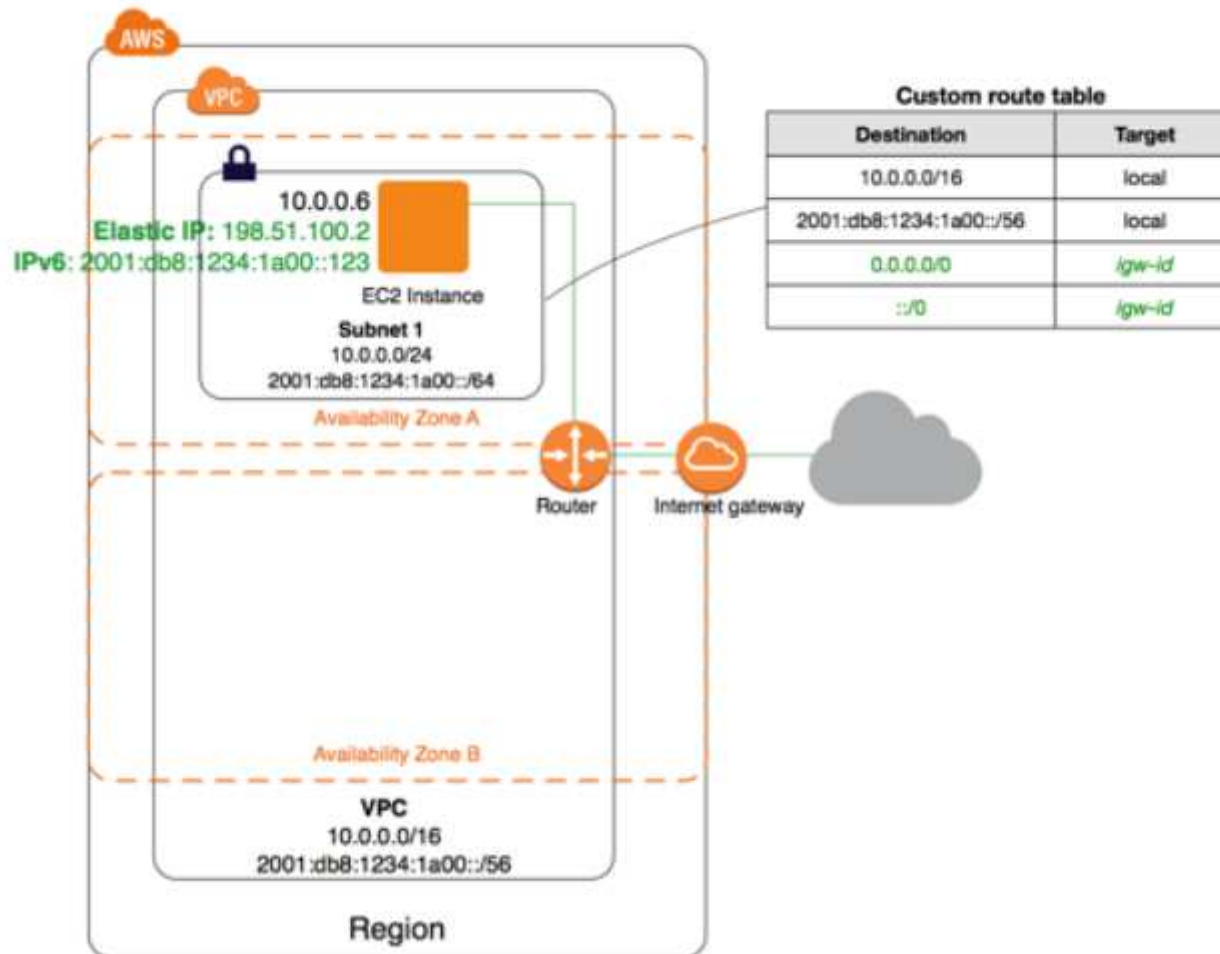
## 2.5 Capa de red VPC

- Gateway hacia Internet



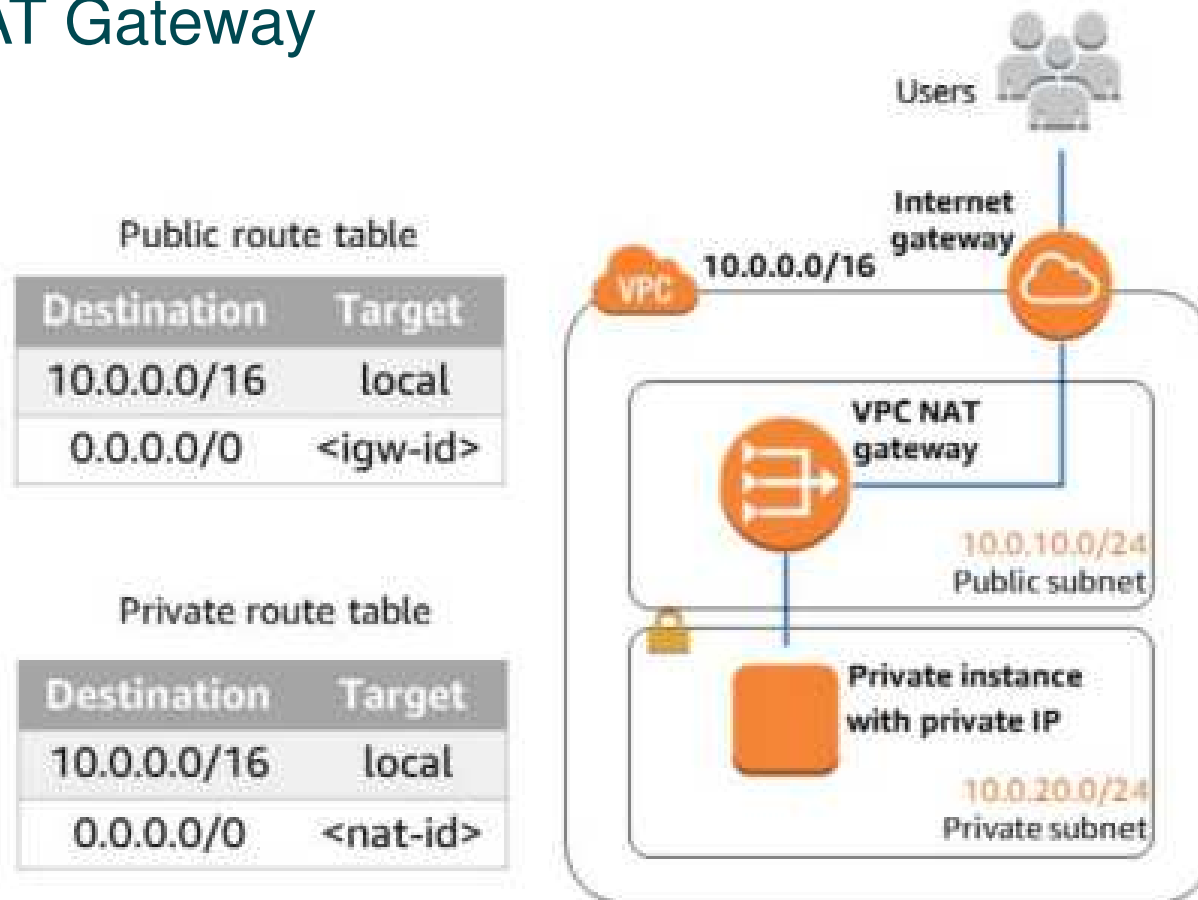
## 2.5 Capa de red VPC

- Escenario con subred pública con InternetGateway



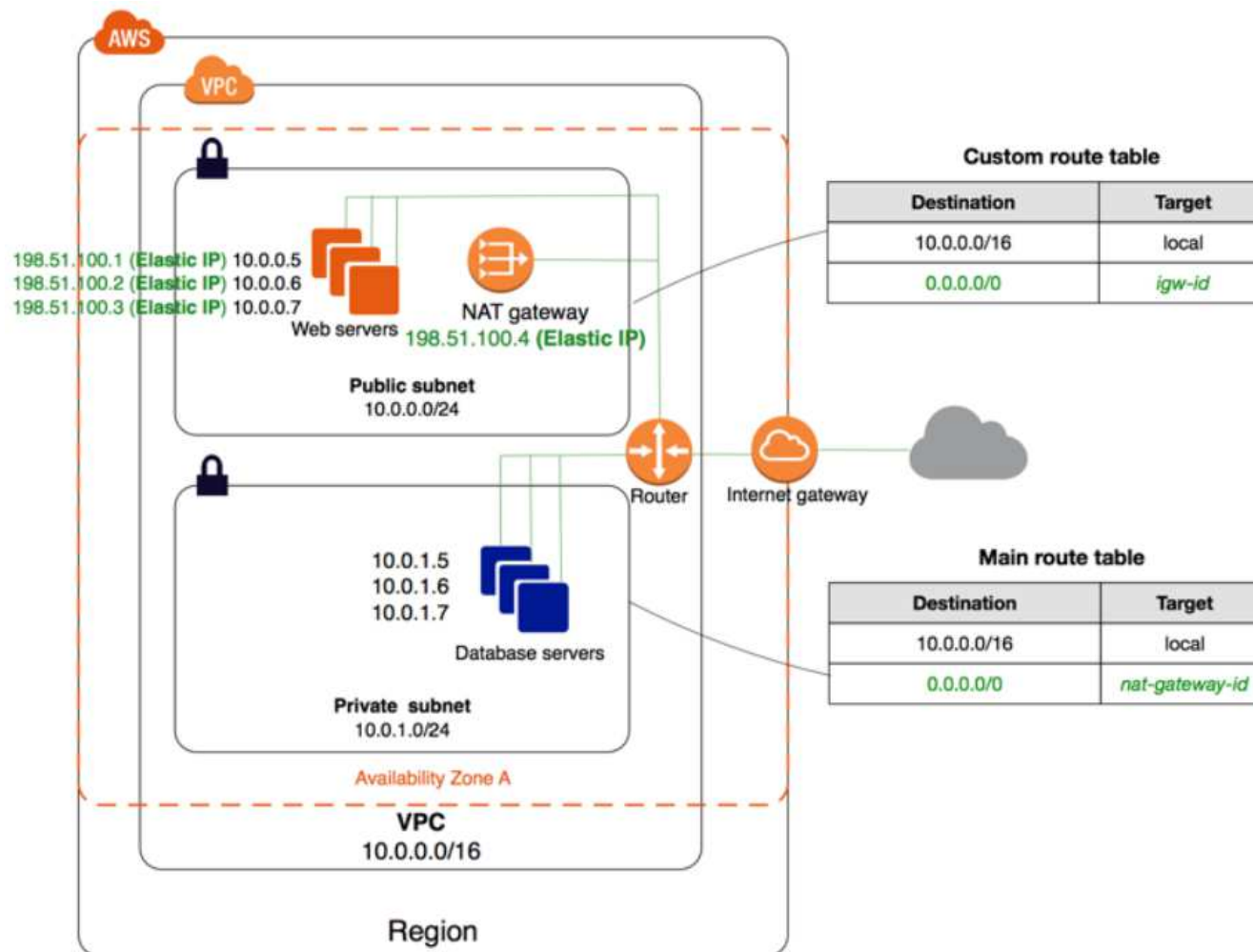
## 2.5 Capa de red VPC

- NAT Gateway



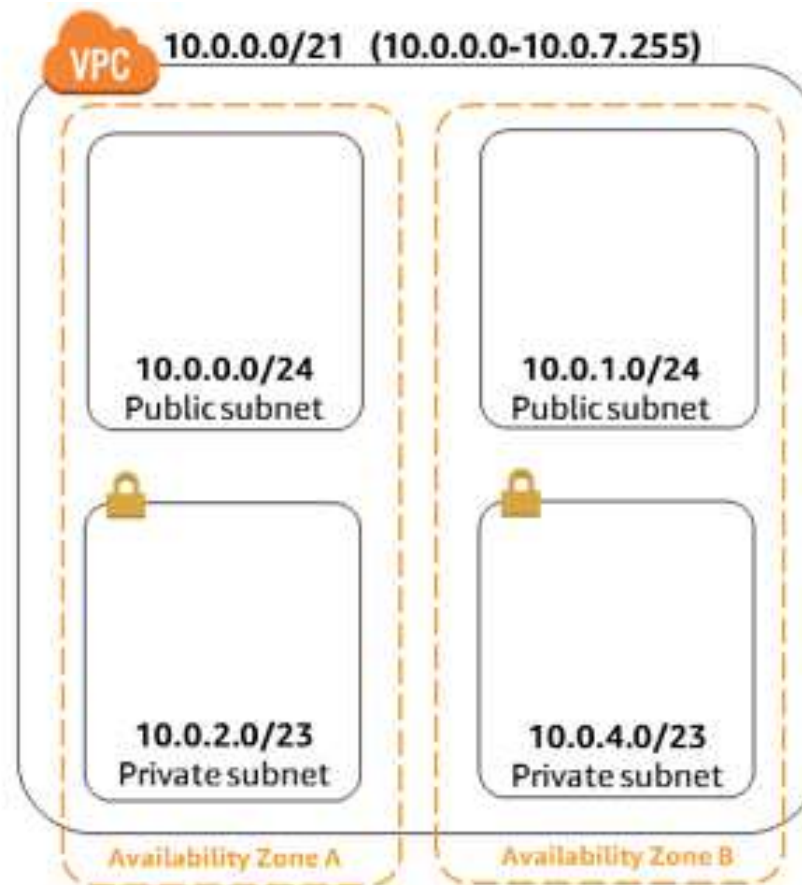
## 2.5 Capa de red VPC

- NAT Gateway



## 2.5 Capa de red VPC

- Configuración base para disponibilidad

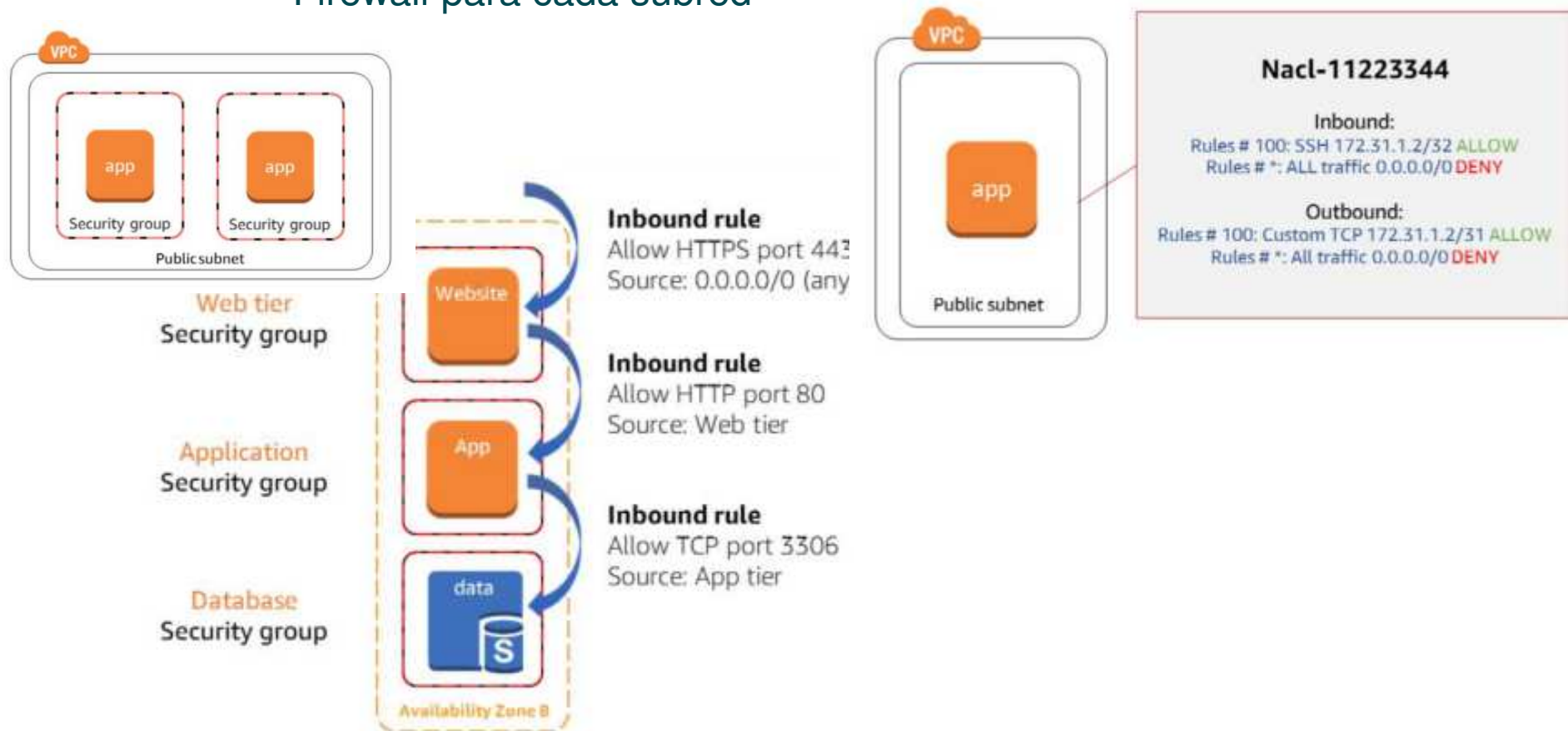


## 2.5 Capa de red VPC

- IP elásticas
  - IP publicas fijas que se reservan/alquilan
  - Tienen un coste aunque no las este utilizando una instancia
  - 5 por región

## 2.5 Capa de red VPC

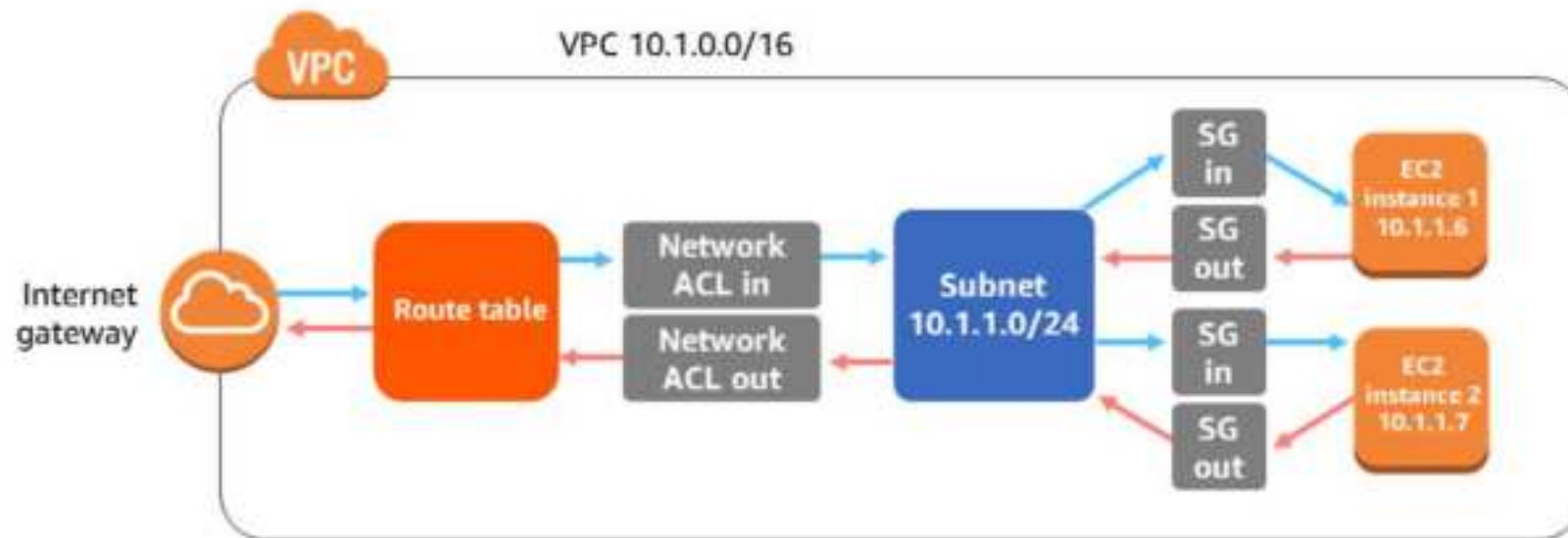
- Seguridad
  - Grupos de seguridad : Se aplican a instancia/recursos
  - Listas de control de acceso de red (ACL)
    - Firewall para cada subred





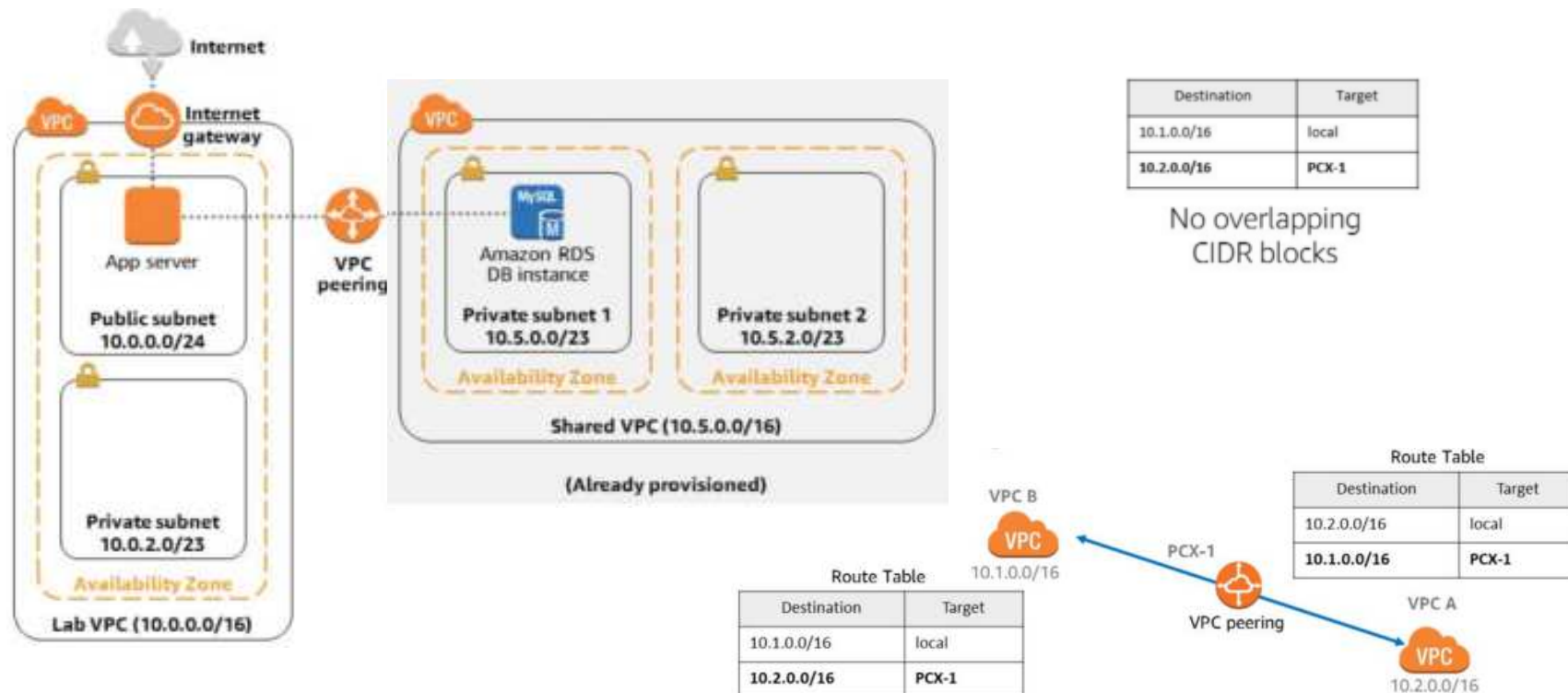
## 2.5 Capa de red VPC

- Seguridad
  - Grupos de seguridad y ACLs



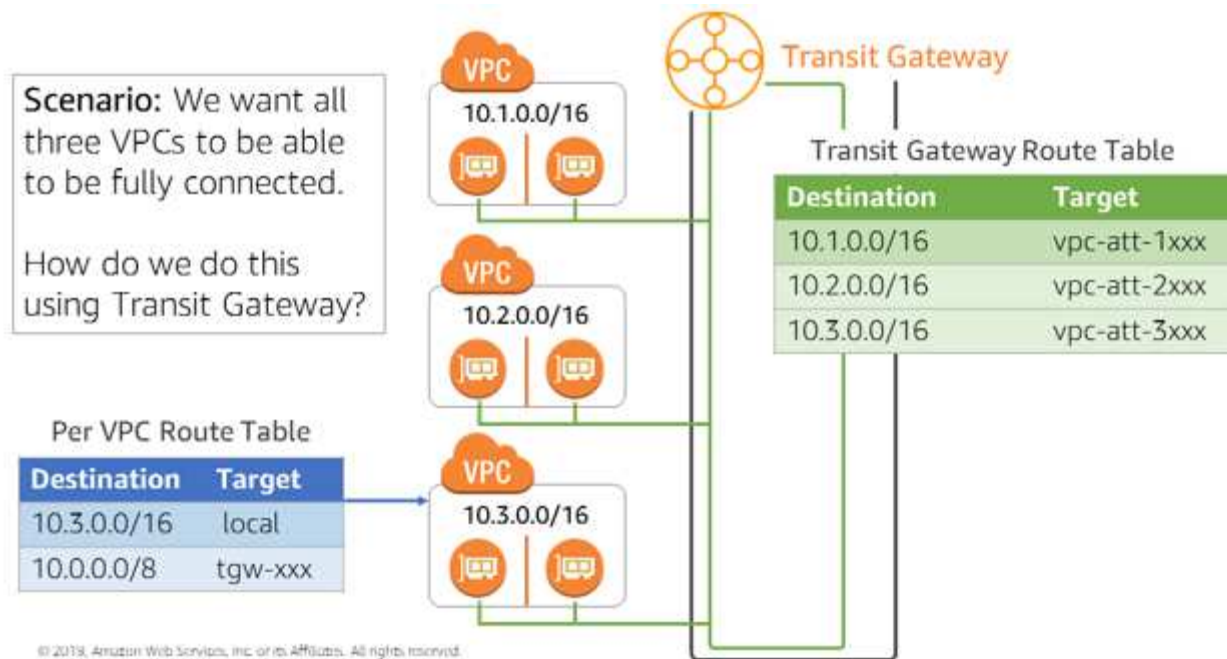
## 2.5 Capa de red VPC

- Conectividad entre VPCs
  - VPC peering : El trafico no sale del backbone de red de AWS
  - Cuidado con el direccionamiento de redes locales
  - Conexión punto a punto



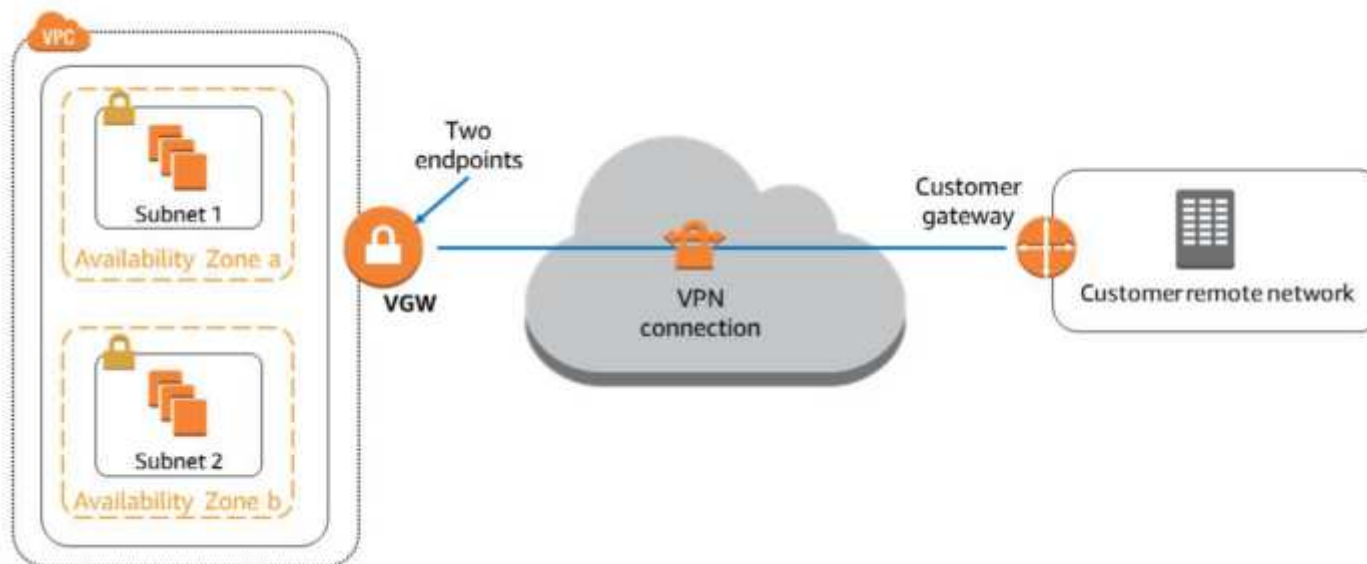
## 2.5 Capa de red VPC

- Conectividad entre VPCs
  - VPC peering vs Transit Gateway



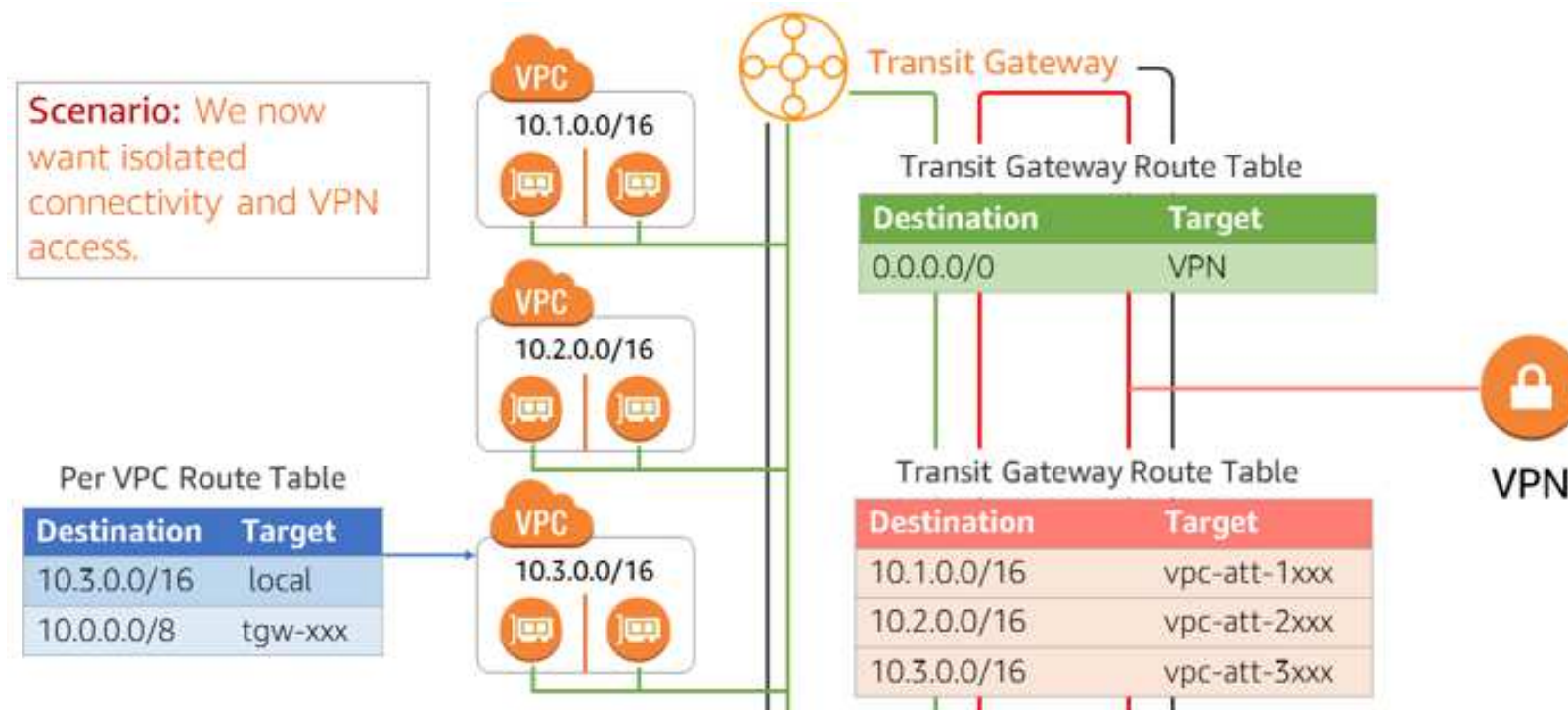
## 2.5 Capa de red VPC

- Conectividad entre VPC y otras redes
  - Virtual Private Gateway
  - Permite la creación de VPN
  - IPsec



## 2.5 Capa de red VPC

- Conectividad entre varias VPC y una red local



## 2.5 Capa de red VPC

- Conectividad entre VPC y otras redes
  - VPC vs AWS Direct Connect
  - Red dedicada, sin atravesar internet
  - Utilizada en situaciones de transferencia de grandes tamaños de datos :seguridad , rendimiento

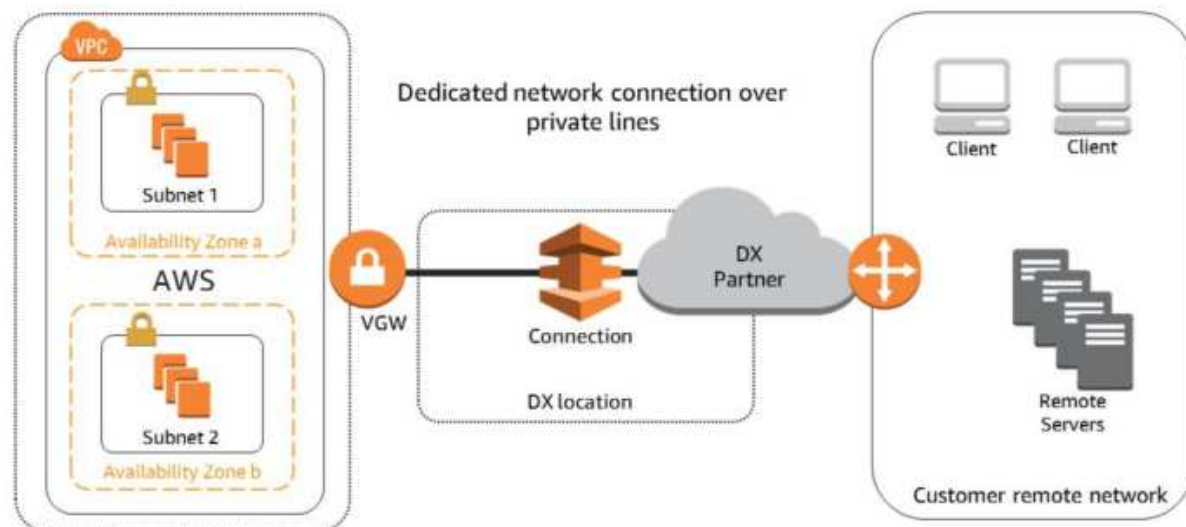
AWS Direct Connect (DX) provides you with a **dedicated, private network connection** of either 1 or 10 Gbps



Reduces data transfer costs

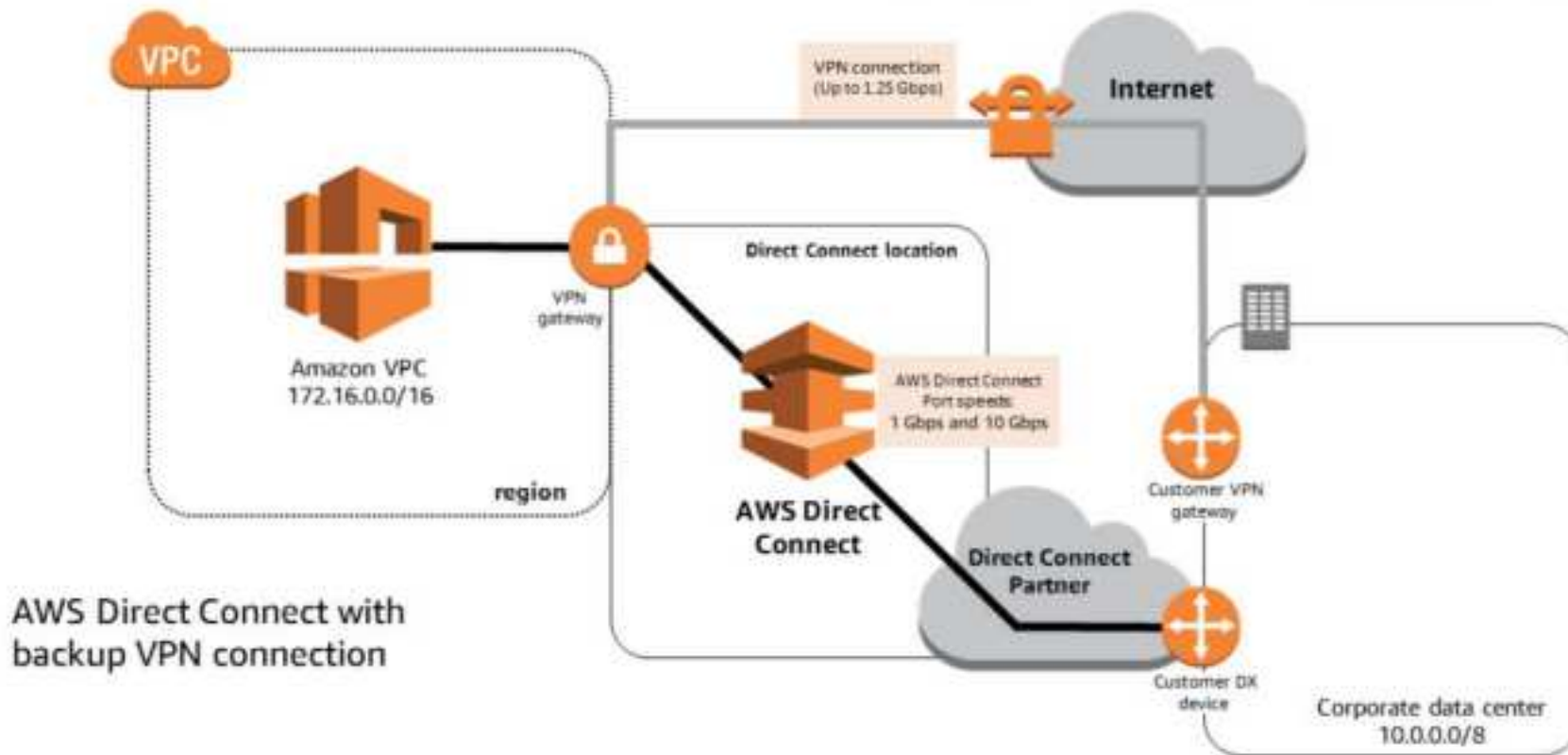


Improve application performance with predictable metrics



## 2.5 Capa de red VPC

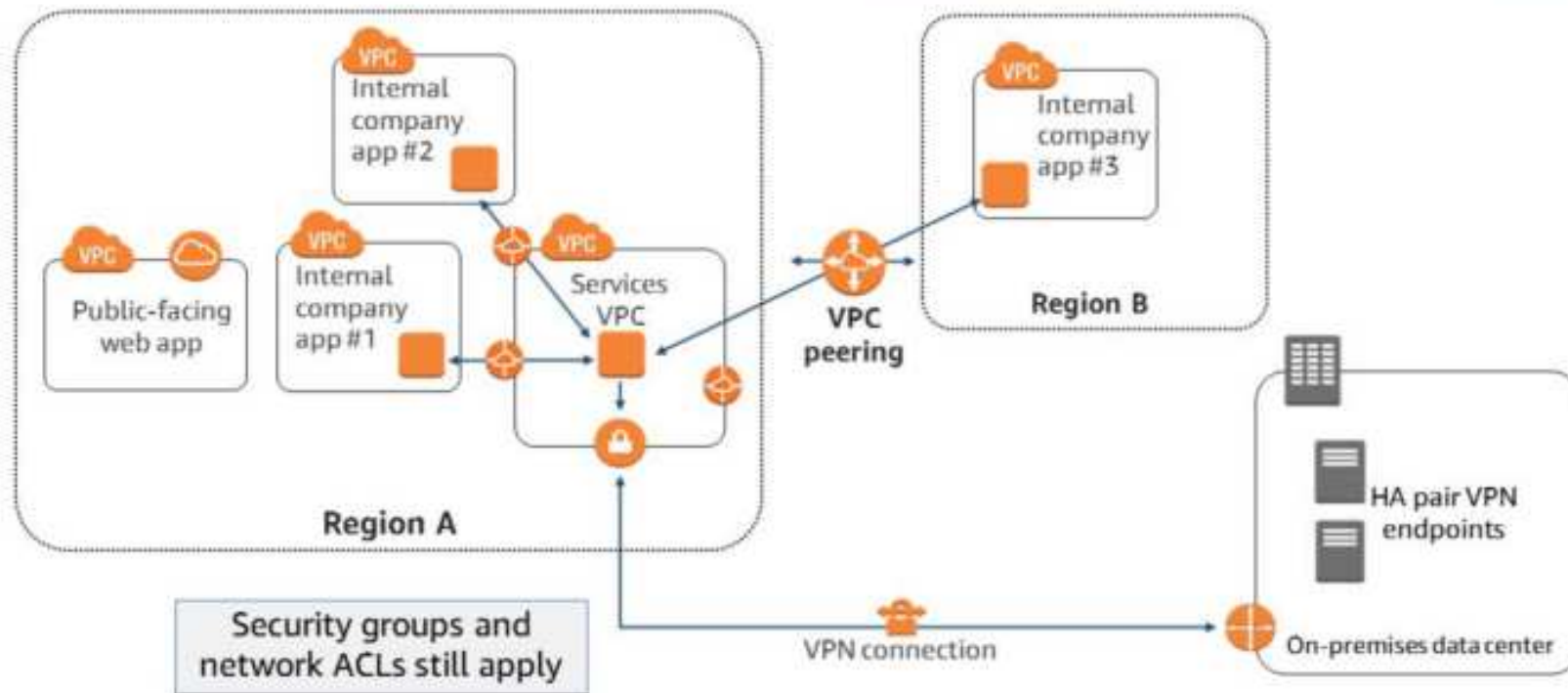
- Conectividad entre VPC y otras redes





## 2.5 Capa de red VPC

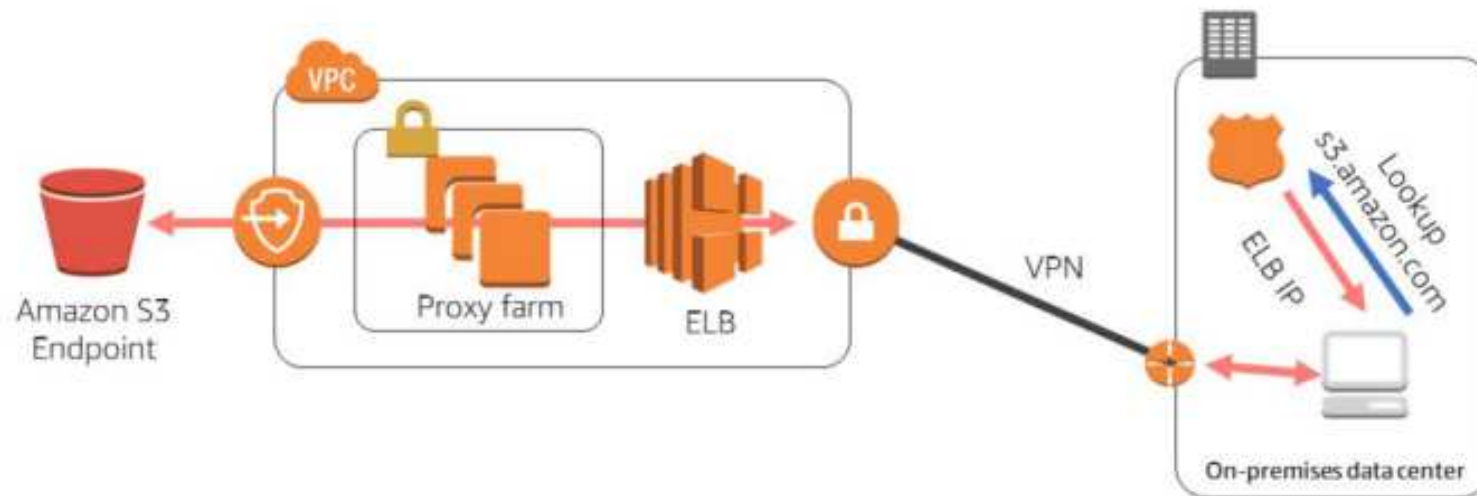
- Ejemplo Cloud Hybrido





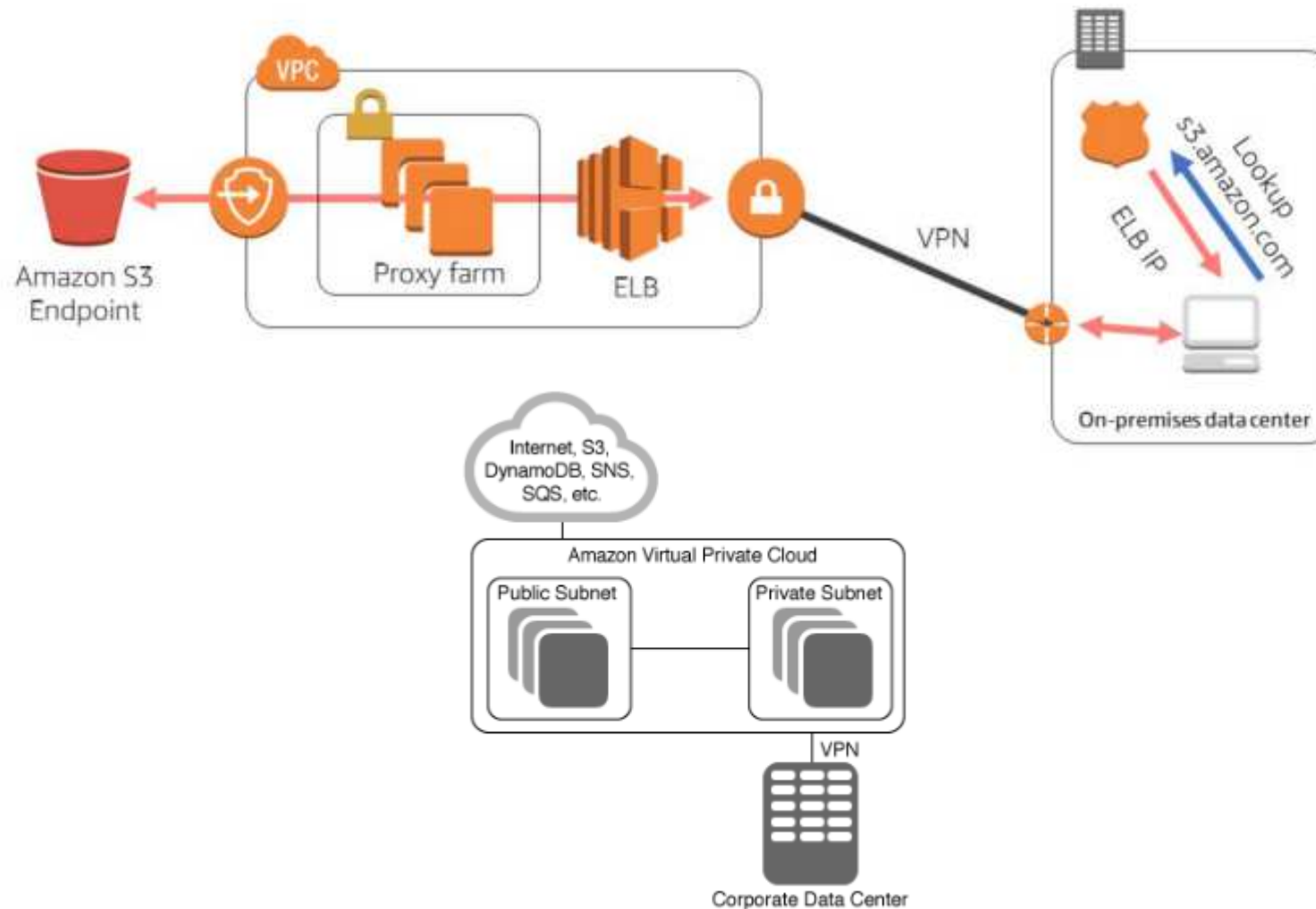
## 2.5 Capa de red VPC

- Acceso a recursos Cloud



## 2.5 Capa de red VPC

- Acceso a recursos Cloud

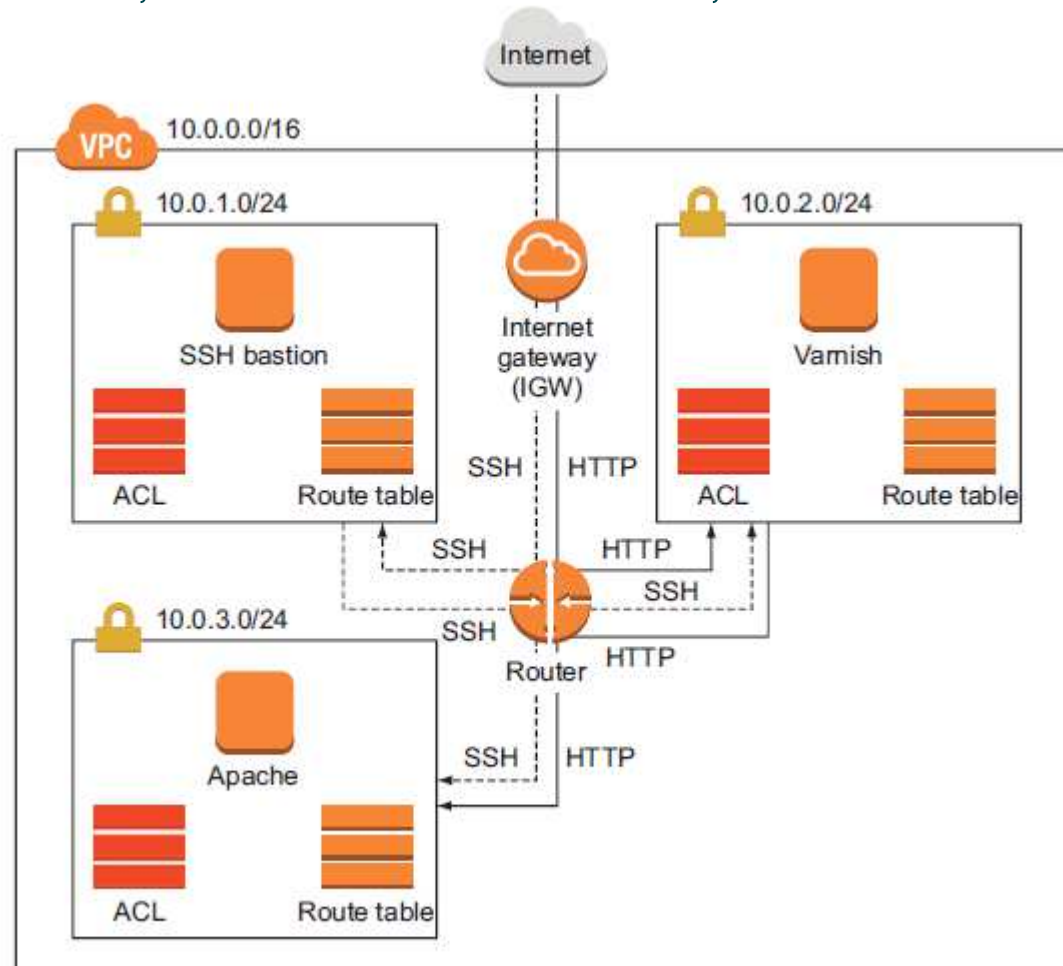


## 2.5 Capa de red VPC

- Escenarios por defecto
  - [https://docs.aws.amazon.com/es\\_es/vpc/latest/userguide/VPC\\_Scenario1.html](https://docs.aws.amazon.com/es_es/vpc/latest/userguide/VPC_Scenario1.html)
    - ☐ Escenario 1: VPC con una única subred pública
    - ☐ Escenario 2: VPC con subredes públicas y privadas (NAT)
    - ☐ Situación 3: VPC con subredes públicas y privadas, y acceso de AWS Site-to-Site VPN
    - ☐ Escenario 4: VPC solo con una subred privada y acceso de AWS Site-to-Site VPN

## 2.5 Capa de red VPC

- Práctica: Bastion , Apache2 & varnish: Subredes publicas , privadas , tablas de enrutamiento, internet Gateway y NAT



## 2.5 Capa de red VPC

- Práctica: Crear VPC : Wizard vs Manual

### Step 1: Select a VPC Configuration

VPC with a Single Public Subnet

**VPC with Public and Private Subnets**

VPC with Public and Private Subnets and Hardware VPN Access

VPC with a Private Subnet Only and Hardware VPN Access

to containing a public  
s configuration adds  
ubnet whose  
are not addressable  
Internet. Instances in  
subnet can establish  
connections to the  
the public subnet  
work Address  
(NAT).

ork with two /24  
ublic subnet  
se Elastic IPs to  
Internet. Private  
ances access the  
Network Address  
(NAT). (Hourly  
NAT devices apply.)

The diagram illustrates the VPC configuration. At the top, a cloud icon represents the Internet, with services like S3, DynamoDB, SNS, and SQS listed. A line connects this cloud to the 'Public Subnet' within the 'Amazon Virtual Private Cloud' box. The 'Public Subnet' contains a stack of server icons and a 'NAT' device. A line connects the 'NAT' device to the 'Private Subnet', which also contains a stack of server icons. The entire setup is labeled 'Amazon Virtual Private Cloud'.

Select

## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
  - Si puede especificar una red dedicada
  - Se le asocia unas opciones por defecto para el DHCP

### Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Name tag	<input type="text" value="VPC_MASTER_PRACTICA4"/>	
IPv4 CIDR block*	<input type="text" value="10.0.0.0/16"/>	
IPv6 CIDR block	<input checked="" type="radio"/> No IPv6 CIDR Block  <input type="radio"/> Amazon provided IPv6 CIDR block	
Tenancy	<input type="text" value="Default"/>	

## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
  - Creación de la dos subredes
    - Publica vs Privada

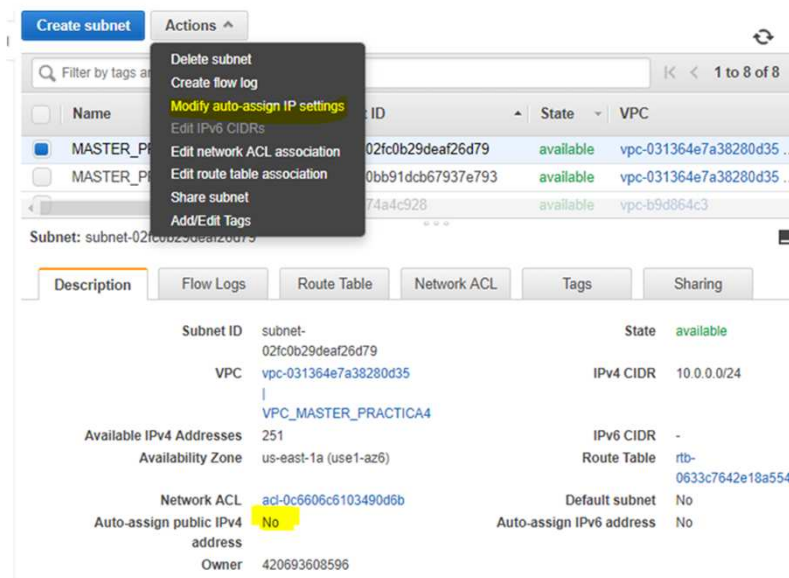
### Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and a /28 netmask. An IPv6 CIDR block must be a /64 CIDR block.

Name tag	<input type="text" value="MASTER_PRACTICA4_S1"/>	
VPC*	<input type="text" value="vpc-031364e7a38280d35"/>	
VPC CIDRs	<div><input type="text" value="Filter by attributes"/><ul style="list-style-type: none"><li>vpc-b9d864c3</li><li>vpc-031364e7a38280d35 VPC_MASTER_PRACTICA4</li></ul></div>	<div>Status Reason</div>
Availability Zone	<input type="text" value="us-east-1a"/>	
IPv4 CIDR block*	<input type="text" value="10.0.0.0/24"/>	

## 2.5 Capa de red VPC


- Práctica: Crear VPC : Manual
  - Convertir una subred en PUBLICA



### Modify auto-assign IP settings

Enable the auto-assign IP address setting to automatically request a public IPv4 or IPv6 address; assign IP settings for an instance at launch time.

Subnet ID subnet-0bb91dcb67937e793

Auto-assign IPv4 ☐ Enable auto-assign public IPv4 address 



## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
  - Crear un InternetGateway y asociarlo al VPC

### Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Name tag

<input type="checkbox"/>	Name	ID	State
<input type="checkbox"/>	MASTER_PRACTICA4_GATEWAY	igw-0983a60c460...	detached
<input checked="" type="checkbox"/>	MASTER_PRACTICA4_GATEWAY	igw-0983a60c460...	attached

Create internet gateway

Actions ^

Filter by tags and attributes

☐ Name

☒ MASTER\_PRACTICA4\_GATEWAY igw-0983a60c460...

☐ igw-6b54b410

Delete internet gateway

Attach to VPC

Detach from VPC

Add/Edit Tags

### Attach to VPC

Attach an internet gateway to a VPC to enable communication with the internet. Specify the VPC you would like to attach below.

VPC\*

► AWS Command Line

\* Required

Filter by attributes	
VPC ID	Name
vpc-031364e7a38280d35	VPC_MASTER_PRACTICA4

## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
  - Antes de configurar las tablas de enrutamiento , las ACL y e NAT para las direcciones privadas se desplegaran tres servidores
    - Uno en cada red
    - 1 servidor SSH Bastion en la red publica con únicamente exponiendo el puerto SSH
    - 1 servidor Varnish/CDN en la segunda red publica exponiendo HTTP/HTTPS y SSH solo al bastion
    - 1 servidor WEB en la red privada exponiendo únicamente HTTP y SSH solo al Bastion
  - Se probara la conectividad a Internet y entre los diferentes servidores

## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
  - Ejemplo Security Group Servidor WEB/Varnish

Assign a security group: ☒ Create a new security group

☐ Select an existing security group

Security group name: SG-WEB-PRIVATE

Description: SG-WEB-PRIVATE

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
SSH ▼	TCP	22	Custom ▼ 10.0.0.0/24
HTTP ▼	TCP	80	Custom ▼ 10.0.1.0/24

## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
  - Conectividad SSH a los tres servidores desde PC
  - Utilizar MTPutty

Filter by tags and attributes or search by keyword 1 to 3 of 3

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
WEB	i-03ad...	t2.micro	us-east-1a	running	2/2 checks ...	None
VARNISH	i-0158...	t2.micro	us-east-1a	running	Initializing	None
BASTION	i-0f917...	t2.micro	us-east-1a	running	2/2 checks ...	None

Instance: **i-0f91767b9c9506083 (BASTION)** Public IP: 34.229.251.195

Description

Status Checks

Monitoring

Tags

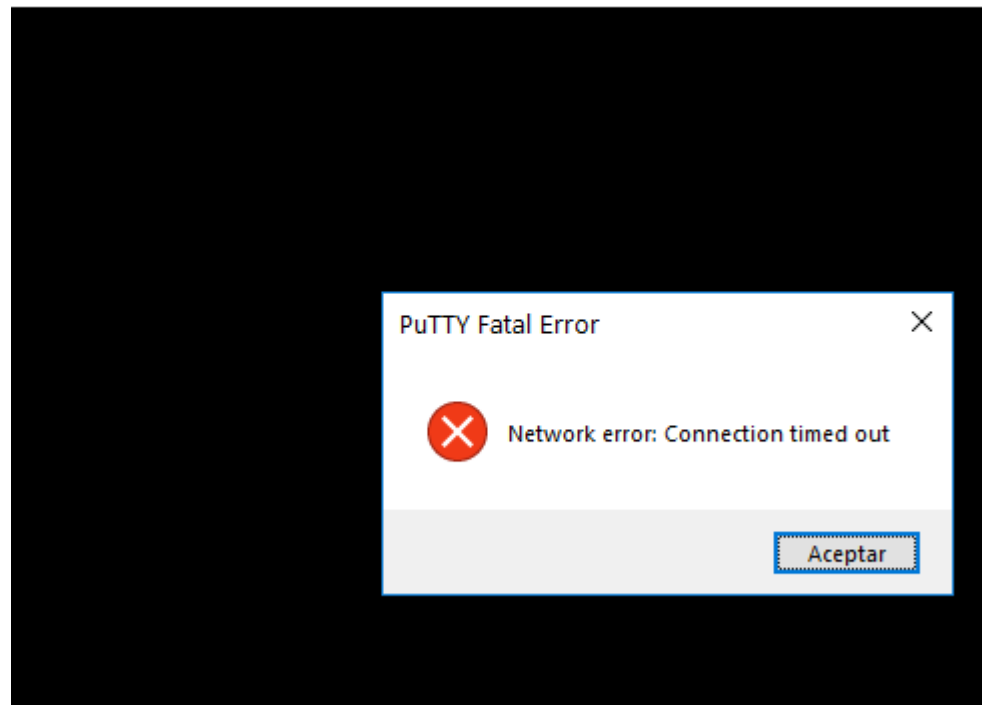
Instance ID	i-0f91767b9c9506083	Public DNS (IPv4)	-
Instance state	running	IPv4 Public IP	34.229.251.195
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-10-0-0-122.ec2.internal
Availability zone	us-east-1a	Private IPs	10.0.0.122
Security groups	launch-wizard-15	Secondary private IPs	

[view inbound rules](#)

## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
  - Probar Conectividad SSH al servidor BASTION
  - ¿Porque no hay conectividad?

 34.229.251.195 - PuTTY



## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
  - Crear tablas de enrutamiento para las tres subredes

Name tag  ⓘ

VPC\*  ↕ ⓘ

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
<input type="text" value="0.0.0.0/0"/> ↕	<input type="text" value="igw-"/> ↕		No

Add route

igw-0983a60c460ef0795    MASTER\_PRACTICA4\_GATEWAY

## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
- Asociar tabla con subred

Create route table Actions

Filter by tags and attributes or search by keyword 1 to 3 of 3

Name	Route Table ID	Explicit subnet association	Main	VPC ID
<input checked="" type="checkbox"/> RUTAS-S1	rtb-0159bbfa4dbddf18e	-	No	vpc-0313
<input type="checkbox"/>	rtb-0633c7642e18a5548	-	Yes	vpc-0313
<input type="checkbox"/>	rtb-6c596213	-	Yes	vpc-b9d8

Route Table: rtb-0159bbfa4dbddf18e

Summary Routes Subnet Associations Route Propagation Tags

Edit subnet associations

Subnet ID	IPv4 CIDR	IPv6 CIDR
None found		

You do not have any subnet associations.

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-02fc0b29deaf26d7...	10.0.0.0/24	-
subnet-0bb91dcb67937e7...	10.0.1.0/24	-
subnet-02f222ed443cbf20...	10.0.2.0/24	-

Filter by tags and attributes or search by keyword

Name	Route Table ID
<input checked="" type="checkbox"/> RUTAS-S1	rtb-0159bbfa4dbddf18e
<input type="checkbox"/>	rtb-0633c7642e18a5548
<input type="checkbox"/>	rtb-6c596213

Route Table: rtb-0159bbfa4dbddf18e

Summary Routes Subnet Associations

Edit subnet associations


Subnet ID	IPv4 CIDR
subnet-02fc0b29deaf26d7...	10.0.0.0/24

The following subnets have not been explicitly associated with any route table:

Subnet ID	IPv4 CIDR
subnet-0bb91dcb67937e7...	10.0.1.0/24
subnet-02f222ed443cbf20...	10.0.2.0/24

## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
  - Probar Conectividad SSH al servidor BASTION

 ec2-user@ip-10-0-0-122:~

```
sing username "ec2-user".  
uthenticating with public key "imported-openssh-key"
```

```
  _|  _|_ )  
 _| (  /   Amazon Linux 2 AMI  
__|\___|__|
```

```
https://aws.amazon.com/amazon-linux-2/  
ec2-user@ip-10-0-0-122 ~]$
```



## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
  - Actualmente esta asociado el AccessList por defecto se puede especificar mas concreto, especificando uno por subred
  - No os olvidéis del outbound tambien

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Network ACL ID	Associated with	Default
<input checked="" type="checkbox"/>		acl-0c6606c61034...	3 Subnets	Yes
<input type="checkbox"/>	ACL-s1	acl-0d73ef335212...	-	No

Network ACL: acl-0c6606c6103490d6b

Details

Inbound Rules

Outbound Rules

Subnet associations

Edit inbound rules

View All rules

Rule #	Type	Protocol	Port Range	Source
100	ALL Traffic	ALL	ALL	0.0.0.0/0
*	ALL Traffic	ALL	ALL	0.0.0.0/0

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Network ACL ID	Associated with	Default	VPC
<input type="checkbox"/>		acl-0c6606c61034...	2 Subnets	Yes	vpc-031364e7
<input checked="" type="checkbox"/>	ACL-s1	acl-0d73ef335212...	subnet-02fc0b29d...	No	vpc-031364e7
<input type="checkbox"/>		acl-0b3572	6 Subnets	Yes	vpc-b9d864c1

Network ACL: acl-0d73ef3352122b67a

Details

Inbound Rules

Outbound Rules

Subnet associations

Tags

Edit inbound rules

View All rules

Rule #	Type	Protocol	Port Range	Source	Allow / D
101	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Network ACL ID	Associated with	Default
<input type="checkbox"/>		acl-0c6606c61034...	2 Subnets	Yes
<input checked="" type="checkbox"/>	ACL-s1	acl-0d73ef335212...	subnet-02fc0b29d...	No
<input type="checkbox"/>		acl-0b3572	6 Subnets	Yes

Network ACL: acl-0d73ef3352122b67a

Details

Inbound Rules

Outbound Rules

Subnet associations

Tags

Edit inbound rules

View All rules

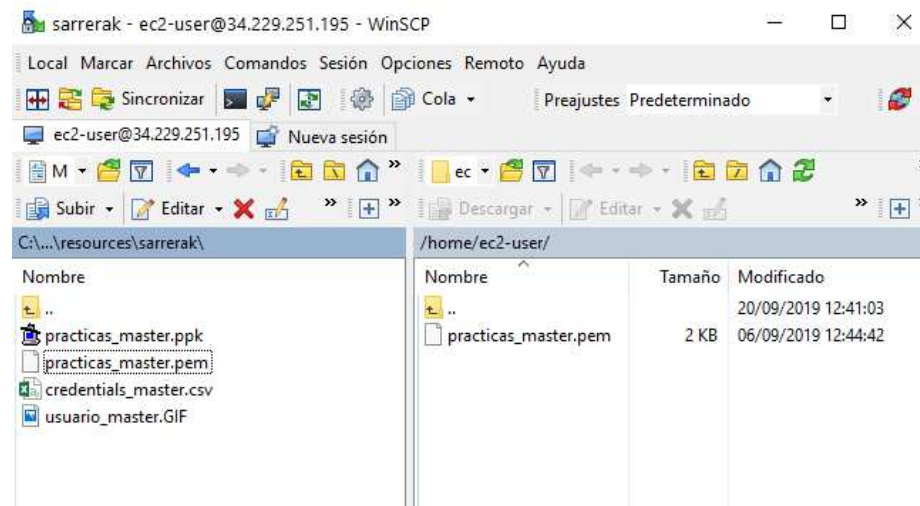
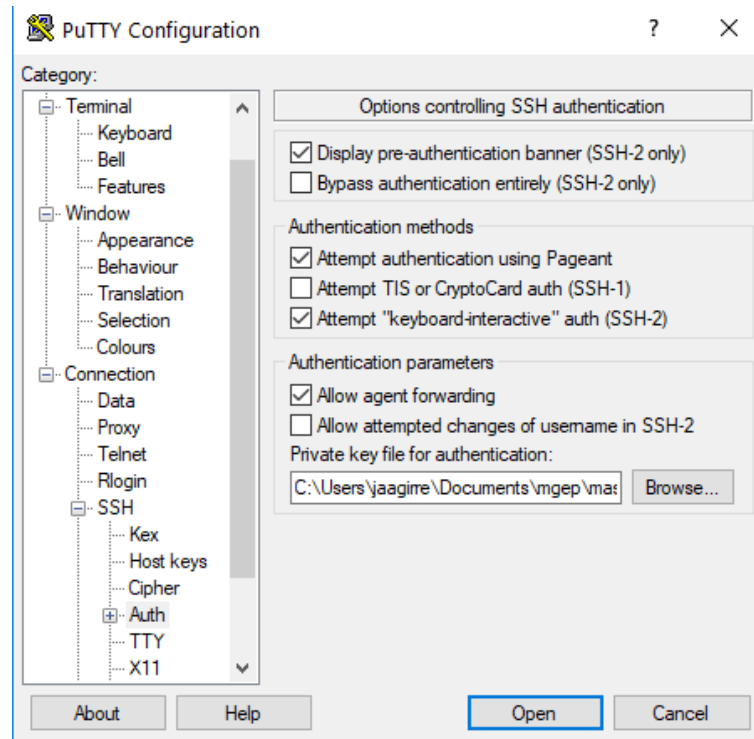
Rule #	Type	Protocol	Port Range	Source	Allow / D
101	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
  - SSH desde PC -> BASTION = OK
  - SSH desde PC -> VARNISH = X (debido al security group)
    - Probar a modificar el security group de SSH cambiando la subred 10.0.0.0 -> 0.0.0.0 (Ahora OK)
  - SSH desde PC -> WEB = X
    - Probar a modificar el security group de SSH cambiando la subred 10.0.0.0 -> 0.0.0.0 (Sigue X, **porque no dispone una IP publica**)
    - Solo se le puede acceder desde un ordenador de laguna de las tres subredes
    - Tampoco puede instalar nada porque el IG no trabaja para el , por eso requiere un servidor NAT en la red publica, que le ofrezca una IP pública

## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
  - Conectarse vía SSH a los servidores mediante el BASTION
  - Configurar reenvío de agente en PUTTY
  - Copiar el fichero .pem a BASTION (mediante scp)



## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
- Probar conectividad entre el BASTION y las otras maquinas
- Ping activar icmp en los accesList y securitygroups

```

Authenticating with public key "imported-openssh-key"
Last login: Fri Sep 20 13:22:28 2019 from 193.146.78.97

  _ | _ | _ )
  _ | ( _ _ /   Amazon Linux 2 AMI
  _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
7 package(s) needed for security, out of 10 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-1-59 ~]$ ping 10.0.1.59
PING 10.0.1.59 (10.0.1.59) 56(84) bytes of data.
64 bytes from 10.0.1.59: icmp_seq=1 ttl=255 time=0.017 ms
64 bytes from 10.0.1.59: icmp_seq=2 ttl=255 time=0.030 ms
^C
--- 10.0.1.59 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1026ms
rtt min/avg/max/mdev = 0.017/0.023/0.030/0.008 ms
[ec2-user@ip-10-0-1-59 ~]$ ping 10.0.0.91
PING 10.0.0.91 (10.0.0.91) 56(84) bytes of data.
64 bytes from 10.0.0.91: icmp_seq=1 ttl=255 time=0.489 ms
64 bytes from 10.0.0.91: icmp_seq=2 ttl=255 time=0.468 ms
64 bytes from 10.0.0.91: icmp_seq=3 ttl=255 time=0.518 ms
^C
--- 10.0.0.91 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2053ms
rtt min/avg/max/mdev = 0.468/0.491/0.518/0.032 ms
[ec2-user@ip-10-0-1-59 ~]$ █

```

```

Servers, Start page X  ec2-user@ip-10-0-0-91:~ X
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"
Last login: Fri Sep 20 14:26:47 2019 from 193.146.78.97

  _ | _ | _ )
  _ | ( _ _ /   Amazon Linux 2 AMI
  _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-91 ~]$ ping 10.0.0.91
PING 10.0.0.91 (10.0.0.91) 56(84) bytes of data.
64 bytes from 10.0.0.91: icmp_seq=1 ttl=255 time=0.015 ms
64 bytes from 10.0.0.91: icmp_seq=2 ttl=255 time=0.029 ms
^C
--- 10.0.0.91 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 0.015/0.022/0.029/0.007 ms
[ec2-user@ip-10-0-0-91 ~]$ █

```

## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
- Conectar SSH desde el BASTION a los demás servidores
- Probar a instalar aplicaciones en los servidores
- En el bastion activar el agente ssh
  - \$eval `ssh-agent`
  - \$ssh-add ./practicas\_master.pem
  - \$ssh -i practicas\_master.pem -A 10.0.1.59

```
ec2-user@ip-10-0-0-91 ~]$ ssh -i practicas_master.pem -A 54.85.73.134
C
ec2-user@ip-10-0-0-91 ~]$ ssh -i practicas_master.pem -A 10.0.1.59
Last login: Fri Sep 20 14:29:58 2019 from 10.0.0.91

  ____|  __|\____|__ )
  _|\___| (___| /   Amazon Linux 2 AMI
  ___| \___|____|___|

https://aws.amazon.com/amazon-linux-2/
1 package(s) needed for security, out of 10 available
Run "sudo yum update" to apply all updates.
ec2-user@ip-10-0-1-59 ~]$
```

## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
- Probar a instalar aplicaciones en los servidores
  - BASTION = OK
  - VARNISH = OK
  - WEB = X (¿porque?)

```

(~/2) mod_http2-1.15.1-1.amzn2.x86_64.rpm
-----
Total
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : apr-1.6.3-5.amzn2.0.2.x86_64
  Installing : apr-util-bdb-1.6.1-5.amzn2.0.2.x86_64
  Installing : apr-util-1.6.1-5.amzn2.0.2.x86_64
  Installing : httpd-tools-2.4.39-1.amzn2.0.1.x86_64
  Installing : generic-logos-httpd-18.0.0-4.amzn2.noarch
  Installing : mailcap-2.1.41-2.amzn2.noarch
  Installing : httpd-filesystem-2.4.39-1.amzn2.0.1.noarch
  Installing : mod_http2-1.15.1-1.amzn2.x86_64
  Installing : httpd-2.4.39-1.amzn2.0.1.x86_64
  Verifying  : apr-util-1.6.1-5.amzn2.0.2.x86_64
  Verifying  : apr-util-bdb-1.6.1-5.amzn2.0.2.x86_64
  Verifying  : httpd-tools-2.4.39-1.amzn2.0.1.x86_64
  Verifying  : httpd-2.4.39-1.amzn2.0.1.x86_64
  Verifying  : httpd-filesystem-2.4.39-1.amzn2.0.1.noarch
  Verifying  : mod_http2-1.15.1-1.amzn2.x86_64
  Verifying  : apr-1.6.3-5.amzn2.0.2.x86_64
  Verifying  : mailcap-2.1.41-2.amzn2.noarch
  Verifying  : generic-logos-httpd-18.0.0-4.amzn2.noarch

Installed:
  httpd.x86_64 0:2.4.39-1.amzn2.0.1

Dependency Installed:
  apr.x86_64 0:1.6.3-5.amzn2.0.2          apr-util.x86_64 0:1.6.1-5.amzn2.0.2
  apr-util-bdb.x86_64 0:1.6.1-5.amzn2.0.2  generic-logos-httpd-18.0.0-4.amzn2.noarch
  httpd-filesystem.noarch 0:2.4.39-1.amzn2.0.1  httpd-tools.x86_64 0:2.4.39-1.amzn2.0.1
  mailcap.noarch 0:2.1.41-2.amzn2.noarch  mod_http2.x86_64 1:1.15.1-1.amzn2.x86_64

Complete!
[ec2-user@ip-10-0-1-59 ~]$ sudo yum install httpd

```

```

-1.ec2.archive.ubuntu.com:80 (54.152.129.43), connection timed out Could not connect to
com:80 (54.165.17.230), connection timed out Could not connect to us-east-1.ec2.archive.ub
connection timed out Could not connect to us-east-1.ec2.archive.ubuntu.com:80 (34.203
E: Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/c/curl/libcurl4_7.58.0-
connect to us-east-1.ec2.archive.ubuntu.com:http:
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
ubuntu@ip-10-0-2-39:~$
ubuntu@ip-10-0-2-39:~$

```

```

security.ubuntu.com:80 (91.189.88.149), CO
2), connection timed out Could not connect
W: Failed to fetch http://ppa.launchpad.net
launchpad.net:80 (91.189.95.83), connection
W: Failed to fetch http://ppa.launchpad.net
pad.net:http:
W: Some index files failed to download. Th
ubuntu@ip-10-0-2-39:~$

```

## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
  - Para que los servidores sin IP publicas puedan acceder a internet , por ejemplo , para realizar instalaciones, se necesita un servidor NAT
    - Instancia EC2 NAT de AWS
    - Servidor EC2 con instalando software de NAT (o un AMI con NAT)
      - Deshabilitar la opción de red de la instance  
***source/destination checks by default***
  - Requiere una IP elástica
  - Ubicado en subred publica



Región: EE.UU., Este (Ohio) ±


---

Precio por gateway de NAT (USD/hora)	Precio por GB de datos procesados (USD)
0,045 USD	0,045 USD

---


create a NAT gateway and assign it an Elastic IP address. [Learn more.](#)

Subnet\* subnet-02fc0b29deaf26d79  

Elastic IP Allocation ID\* eipalloc-08c9c4f3e123530ce 

[Create New EIP](#)

New EIP (3.228.200.96) creation successful.





## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
  - Una vez creado en NAT Gateway modificar la tabla de rutado de la subred privada para crear la ruta a internet
  - ¿Porque sigue sin poder instalar nada?

[illegible]



## 2.5 Capa de red VPC

- Práctica: Crear VPC : Manual
  - Hay que dejar abiertas las respuesta a nosotros , repsuestas con puertos mayores de 1024
  - No olvidar hacerlo en los das subredes : la publica con NAT y la privada

<input checked="" type="checkbox"/>	ACL-s1	acl-0d73ef335212...	subnet-02fc0b29d...	No	vpc-031364e7a38280d35   VPC_MASTER_PRACTICA4	420693608
<input type="checkbox"/>		acl-0fb85f72	6 Subnets	Yes	vpc-b9d864c3	420693608

Network ACL: acl-0d73ef3352122b67a

Details

Inbound Rules

Outbound Rules

Subnet associations

Tags

Edit inbound rules

View All rules

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
101	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
102	ALL Traffic	ALL	ALL	10.0.0.0/16	ALLOW
103	Custom TCP Rule	TCP (6)	1024 - 65535	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

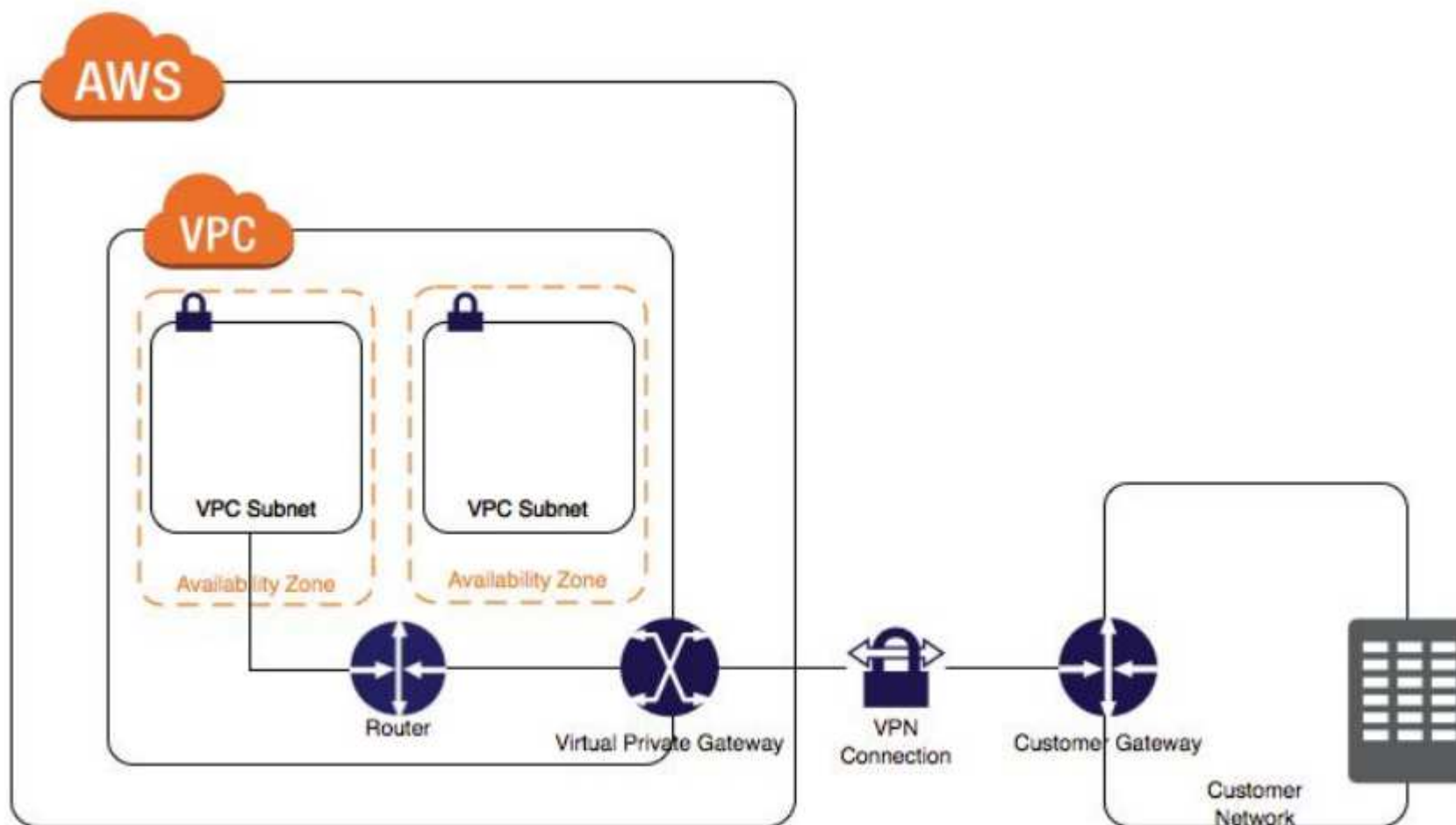
```

tu.com:80 (91.189.88.31), connection timed out
on timed out Could not connect to security.ubuntu
ecurity.ubuntu.com:80 (91.189.88.173), connectio
8), connection timed out Could not connect to se
Failed to fetch http://ppa.launchpad.net/ondrej
chpad.net:80 (91.189.95.83), connection timed o
Failed to fetch http://ppa.launchpad.net/ondrej
ad.net:http:
Some index files failed to download. They have
untu@ip-10-0-2-39:~$ sudo apt-get update
et:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic InRelease
et:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-updates InRelease
et:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-backports InRelease
et:4 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
et:5 http://ppa.launchpad.net/ondrej/apache2/ubuntu bionic InRelease
et:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/main amd64
et:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/main Trans
et:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/restricted

```

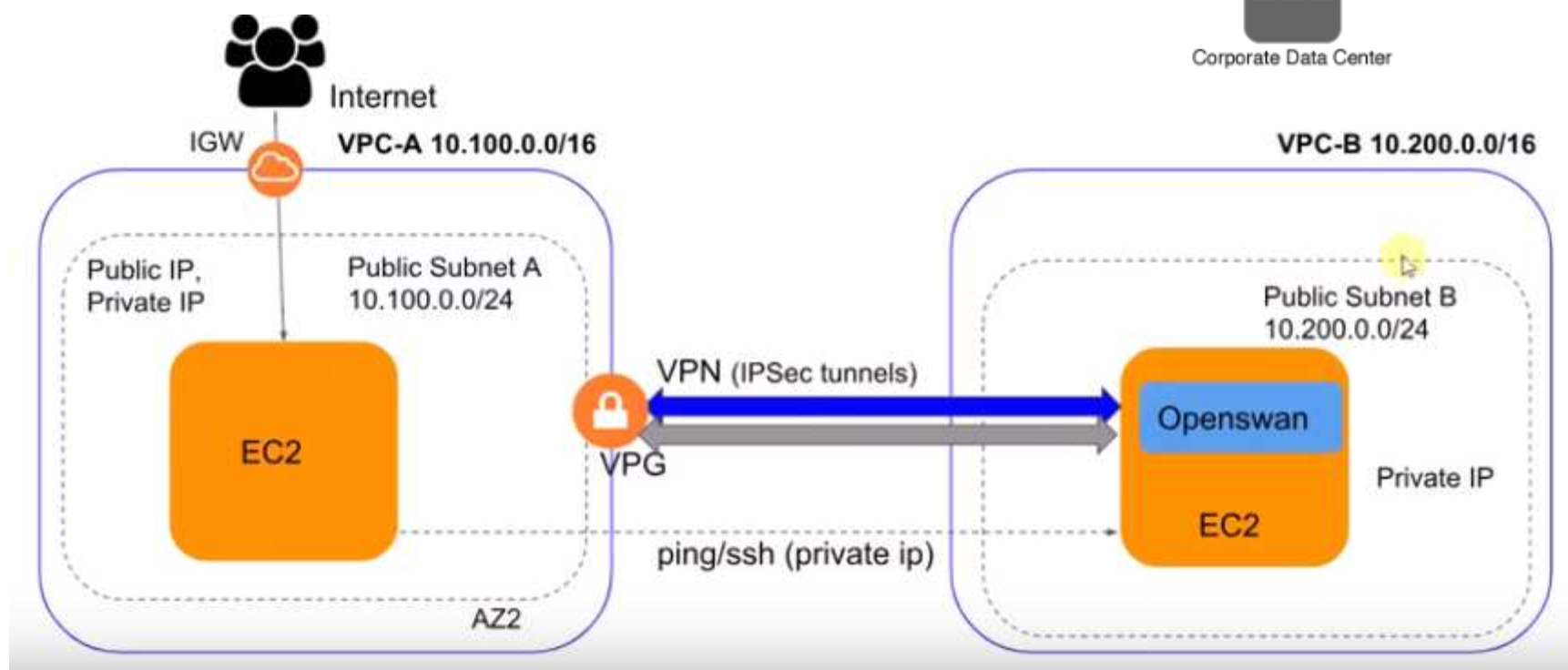
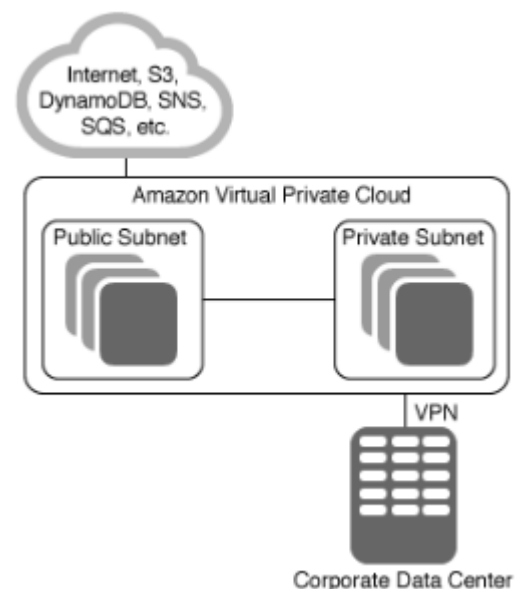
## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud : VPN
  - Conectando un data center con nuestros servicios CLOUD en un VPC



## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud : VPN
  - Conectando un data center con nuestros servicios CLOUD en un VPC



## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud : VPN
  1. Crear la VPC-A en la región N. Virginia
  2. Crear la VPC-B en la región de Irlanda
  3. Lanzar una instancia pública EC2 en VPC-A
  4. Lanzar una instancia publica EC2 en VPC-B que actuara como un router VPN
  5. Instalar y configurar el software OPENSAM VPN en la instancia EC2 del VPC-B
  6. Crear y configurar un Virtual Gateway y Customer Gateway en la red VPC-A
  7. Crear un tunel VPN en VPC-A
  8. Exportar la configuración desde VPC-A y configurar el router OPENSAM de VPC-B
  9. Comenzar el túnel IPSec desde VPC-B
  10. Verificar la conectividad

## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud : VPN
  1. Crear la VPC-A en la región N. Virginia
  2. Crear la VPC-B en la región de Irlanda
  3. Lanzar una instancia pública EC2 en VPC-A
  4. Lanzar una instancia publica EC2 en VPC-B que actuara como un router VPN
  5. Instalar y configurar el software OPENSAM VPN en la instancia EC2 del VPC-B
  6. Crear y configurar un Virtual Gateway y Customer Gateway en la red VPC-A
  7. Crear un tunel VPN en VPC-A
  8. Exportar la configuración desde VPC-A y configurar el router OPENSAM de VPC-B
  9. Comenzar el túnel IPsec desde VPC-B
  10. Verificar la conectividad

## **2.5 Capa de red VPC**

- Práctica: Hybrid-cloud : **Crear la VPC-A en la región N. Virginia y lanzar instancias EC2**
- Esta VPC tendrá el rol de de alojar los recursos CLOUD de la empresa
- Se utilizara el VPC de la práctica anterior con dos subredes y tres maquinas (para probar la vpn es suficiente con el bastion)

## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud : **Crear la VPC-B en la región de Irlanda y lanzar instancias EC2**
- Los servidores de esta VPC simularán los servicios on-premise de la empresa
- Este se ubica en otra región para forzar su comunicación por internet
- Cuidado con las IP (no puede haber overlapping)

Name tag  ⓘ

IPv4 CIDR block\*  ⓘ

IPv6 CIDR block ☒ No IPv6 CIDR Block ⓘ  
☐ Amazon provided IPv6 CIDR block

## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud : **Crear la VPC-B en la región de Irlanda y lanzar instancias EC2**
- Crear subred privada del data-center
  - Para que el router tenga una ip pública

### Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between /16 and /28 and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag  ⓘ

VPC\*  ⓘ

VPC CIDRs	CIDR	Status	Sta
	10.1.0.0/16	associated	

Availability Zone  ⓘ

IPv4 CIDR block\*  ⓘ



## 2.5 Capa de red VPC

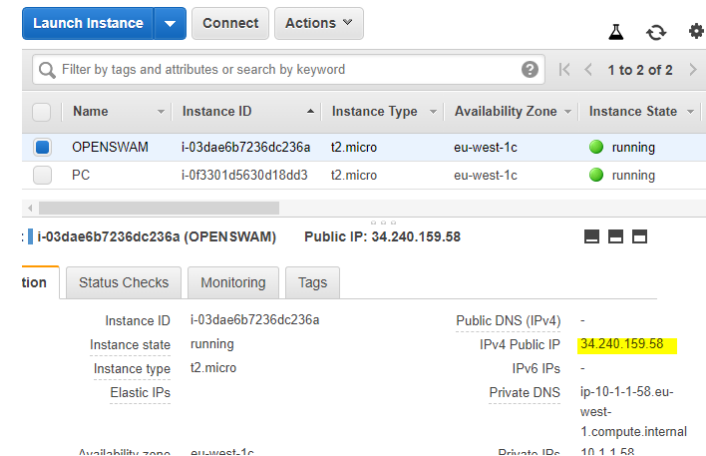
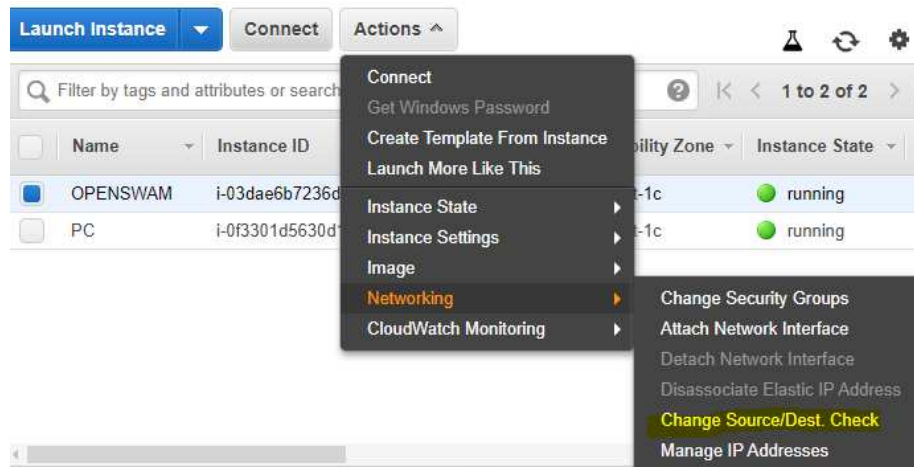
- Práctica: Hybrid-cloud : **Crear la VPC-B en la región de Irlanda y lanzar instancias EC2**
- Lanzar dos instancias una con IP pública y otra solo con privada
  - La pública será para el servidor OPENSWAN
  - La privada para simular un PC de un trabajador
  - Configurar bien los security groups

### Edit inbound rules

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
All TCP ▼	TCP	0 - 65535	Custom ▼ 10.0.0.0/8
SSH ▼	TCP	22	Custom ▼ 0.0.0.0/0
All ICMP - IPv ▼	ICMP	0 - 65535	Custom ▼ 10.0.0.0/8

## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud : **Instalar y configurar el software OPENSAM VPN en la instancia EC2 del VPC-B**
  - \$yum update
  - \$yum install openswan
- Desactivar en la instancia EC2 “check source/destiny IP”
  - De forma que el servidor IPSEC trabaje de forma promiscua y pueda trabajar como NAT
- Recordad la IP publica del servidor
  - Esta IP se utilizara para crear el túnel IPsec



## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud : **Crear y configurar un Virtual Gateway y Customer Gateway en la red VPC-A**

Create Virtual Private Gateway Actions

Filter by tags and attributes or search by keyword 1 to 1 of 1

Name	ID	State	Type	VPC
MASTER-PR...	vgw-05361675faeedefd1	attaching	ipsec.1	vpc-031364e7a38280d35   V

Virtual Private Gateway: vgw-05361675faeedefd1

Details Tags

ID	vgw-05361675faeedefd1	State	attaching
Type	ipsec.1	VPC	vpc-031364e7a38280d35   VPC_MASTER_PRACTICA4
ASN (Amazon side)	64512		

## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud : **Crear y configurar un Virtual Gateway y Customer Gateway en la red VPC-A**
- Crear el customer Gateway , creando el enrutamiento hacia el servidor OPENSAN del data center
  - Utilizar la IP publica del servidor VPN OPENSAN del data center

### Create Customer Gateway

Specify the Internet-routable IP address for your gateway's external interface; the address must be static and translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous private ASN (such as those in the 64512-65534 range).

Name  ⓘ

Routing ☐ Dynamic  
☒ Static

IP Address  ⓘ

## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud : **Crear y configurar un Virtual Gateway y Customer Gateway en la red VPC-A**
  - Crear la conexión utilizando el VPN y el CGW creado previamente
  - Y especificare el enrutamiento estático hacia la subred privada del data center

### Create VPN Connection

Select the virtual private gateway and customer gateway that you would like to connect via a VPN connection. You must have entered and your customer gateway information already.

Name tag  ⓘ

Virtual Private Gateway  ▼ ↺

Customer Gateway ☒ Existing  
☐ New

Customer Gateway ID  ▼ ↺

Routing Options ☐ Dynamic (requires BGP)  
☒ Static

Static IP Prefixes

IP Prefixes	Source	State
<input type="text" value="10.1.0.0/16"/>	-	-

ⓘ

## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud : **Crear y configurar un Virtual Gateway y Customer Gateway en la red VPC-A**
  - Actualizar las rutas de enrutamiento de la red VPC-A para que agregue el VPN
    - Ir a la tabla de enrutamiento de todas las subredes y propagar la ruta al VPN

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with 'Servicios', 'Grupos de recursos', and a user profile 'kudeatza'. Below this, a 'Create route table' button is visible. A search bar contains 'search : rtb-0159b...'. A table lists route tables, with 'RUTAS-S1' selected. An 'Actions' dropdown menu is open, showing options: 'Set Main Route Table', 'Delete Route Table', 'Edit subnet associations', 'Edit route propagation' (highlighted in yellow), 'Edit routes', and 'Add/Edit Tags'. Below the table, the details for 'Route table rtb-0159bbfa4dbddf18e' are shown. Under the 'Route propagation' section, a 'Virtual Private Gateway' is listed with the ID 'vgw-05361675faeedefd1' and the name 'MASTER-PRACTICAS-HYBRID'. A 'Propagate' button is next to it, and a checkmark icon is visible at the bottom right.

## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud : **Crear un tunel VPN en VPC-A**
  - **Descargar configuracion para openswan**

```
conn Tunnel1
  authby=secret
  auto=start
  left=%defaultroute
  leftid=34.240.159.58 right=3.86.130.224
  type=tunnel
  ikelifetime=8h
  keylife=1h
  phase2alg=aes128-sha1;modp1024
  ike=aes128-sha1;modp1024
  auth=esp //eliminar esta linea
  keyingtries=%forever
  keyexchange=ike
  leftsubnet=<LOCAL NETWORK>
  rightsubnet=<REMOTE NETWORK>
  dpddelay=10
  dpdtimeout=30
  dpdaction=restart_by_peer
```

**Download Configuration** ×

Please choose the configuration to download based on your type of customer gateway

Vendor  ⓘ

Platform  ⓘ

Software  ⓘ

---

Cancel Download

## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud :**Exportar la configuración desde VPC-A y configurar el router OPENSWAM de VPC-B**
- Chequear y crear la siguiente configuración

```
# fichero /etc/ipsec.conf  
Include /etc/ipsec.d/*.conf
```

```
# fichero /etc/ipsec.d/aws-vpn.conf  
conn Tunnel1  
    authby=secret  
    auto=start  
    left=%defaultroute  
    leftid=34.240.159.58    right=3.86.130.224  
    type=tunnel  
    ikelifetime=8h  
    keylife=1h  
    phase2alg=aes128-sha1;modp1024  
    ike=aes128-sha1;modp1024  
    keyingtries=%forever  
    keyexchange=ike  
    leftsubnet=<LOCAL NETWORK>  
    rightsubnet=<REMOTE NETWORK>  
    dpddelay=10  
    dpdtimeout=30  
    dpdaction=restart_by_peer
```



## **2.5 Capa de red VPC**

- Práctica: Hybrid-cloud :**Exportar la configuración desde VPC-A y configurar el router OPENSWAM de VPC-B**
- **Configurar el secreto de encriptación**
  - **Utilizar configuración de VPN descargada**

# fichero /etc/ipsec.d/aws-vpn.secrets

34.240.159.58 3.86.130.224: PSK "3Exyuh1R6YGaSjd1RU71K0BecyfsXCvR"

## **2.5 Capa de red VPC**

- Práctica: Hybrid-cloud :**Exportar la configuración desde VPC-A y configurar el router OPENSWM de VPC-B**
- **Configurar el reenvio de paquetes e ipsec**
  - Modificar **/etc/sysctl.conf** con la siguiente información
  - **Reiniciar los servicios de red**
    - **\$sudo service network restart**

```
net.ipv4.ip_forward = 1  
net.ipv4.conf.all.accept_redirects = 0  
net.ipv4.conf.all.send_redirects = 0
```

## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud :Arrancar servidor OPENSWAM
  - \$sudo chkconfig ipsec on
  - \$sudo service ipsec start
  - \$sudo service ipsec status

```
[ec2-user@ip-10-1-1-58 ~]$ sudo service ipsec status
Redirecting to /bin/systemctl status ipsec.service
● ipsec.service - Internet Key Exchange (IKE) Protocol Daemon for IPsec
   Loaded: loaded (/usr/lib/systemd/system/ipsec.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2019-09-24 13:34:35 UTC; 43s ago
     Docs: man:ipsec(8)
           man:pluto(8)
           man:ipsec.conf(5)
   Process: 4172 ExecStartPre=/usr/sbin/ipsec --checknflag (code=exited, status=0/SUCCESS)
   Process: 4165 ExecStartPre=/usr/sbin/ipsec --checknss (code=exited, status=0/SUCCESS)
   Process: 3557 ExecStartPre=/usr/libexec/ipsec/_stackmanager start (code=exited, status=0/SUCCESS)
   Process: 3555 ExecStartPre=/usr/libexec/ipsec/addconn --config /etc/ipsec.conf --checkconfig (code=exited, status=0/SUCCESS)
 Main PID: 4187 (pluto)
   Status: "Startup completed."
   CGroup: /system.slice/ipsec.service
           └─4187 /usr/libexec/ipsec/pluto --leak-detective --config /etc/ipsec.conf --nofork

Sep 24 13:34:36 ip-10-1-1-58.eu-west-1.compute.internal pluto[4187]: | setup callback for interface eth0:500 fd 16
Sep 24 13:34:36 ip-10-1-1-58.eu-west-1.compute.internal pluto[4187]: loading secrets from "/etc/ipsec.secrets"
Sep 24 13:34:36 ip-10-1-1-58.eu-west-1.compute.internal pluto[4187]: loading secrets from "/etc/ipsec.d/aws-vpn.secrets"
Sep 24 13:34:36 ip-10-1-1-58.eu-west-1.compute.internal pluto[4187]: "Tunnell" #1: initiating Main Mode
Sep 24 13:34:36 ip-10-1-1-58.eu-west-1.compute.internal pluto[4187]: "Tunnell" #1: STATE_MAIN_I2: sent MI2, expecting MR2
Sep 24 13:34:36 ip-10-1-1-58.eu-west-1.compute.internal pluto[4187]: "Tunnell" #1: STATE_MAIN_I3: sent MI3, expecting MR3
Sep 24 13:34:36 ip-10-1-1-58.eu-west-1.compute.internal pluto[4187]: "Tunnell" #1: Peer ID is ID_IPV4_ADDR: '3.86.130.224'
Sep 24 13:34:36 ip-10-1-1-58.eu-west-1.compute.internal pluto[4187]: "Tunnell" #1: STATE_MAIN_I4: ISAKMP SA established {auth=PRE
Sep 24 13:34:36 ip-10-1-1-58.eu-west-1.compute.internal pluto[4187]: "Tunnell" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+U
Sep 24 13:34:36 ip-10-1-1-58.eu-west-1.compute.internal pluto[4187]: "Tunnell" #2: STATE_QUICK_I2: sent QI2, IPsec SA established
Hint: Some lines were ellipsized, use -l to show in full.
```

## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud : **Verificar la conectividad**

The screenshot displays the AWS Management Console interface for a VPN connection. At the top, a table lists the VPN connection with the following details:

Name	VPN ID	State	Virtual Private Gateway	Transit Gateway
VPN-CONN...	vpn-0b15fda74a188d40b	available	vgw-05361675faeedefd1   MAS...	-

Below this, the 'VPN Connection: vpn-0b15fda74a188d40b' section is shown. It includes tabs for 'Details', 'Tunnel Details' (which is selected), 'Static Routes', and 'Tags'. Under the 'Tunnel Details' tab, the 'Tunnel State' section contains a table with the following data:

Tunnel Number	Outside IP Address	Inside IP CIDR	Status	Status Last Changed
Tunnel 1	3.86.130.224	169.254.199.176/30	UP	September 24, 2019 at 3:37
Tunnel 2	3.226.162.140	169.254.187.156/30	DOWN	September 24, 2019 at 12:4

The 'Status' column in the tunnel state table is highlighted with a yellow circle, showing 'UP' for Tunnel 1 and 'DOWN' for Tunnel 2.

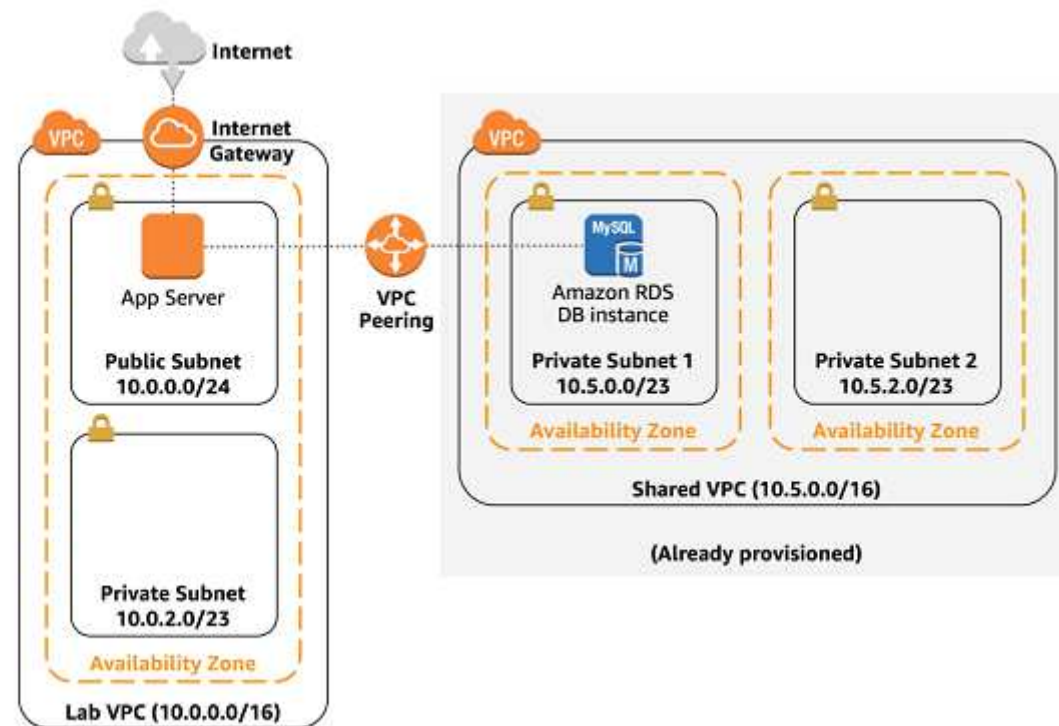
## 2.5 Capa de red VPC

- Práctica: Hybrid-cloud : **Verificar la conectividad**

```
[ec2-user@ip-10-1-1-58 ~]$ ping 10.0.0.91
PING 10.0.0.91 (10.0.0.91) 56(84) bytes of data.
64 bytes from 10.0.0.91: icmp_seq=1 ttl=254 time=67.4 ms
64 bytes from 10.0.0.91: icmp_seq=2 ttl=254 time=67.4 ms
64 bytes from 10.0.0.91: icmp_seq=3 ttl=254 time=67.3 ms
64 bytes from 10.0.0.91: icmp_seq=4 ttl=254 time=67.6 ms
64 bytes from 10.0.0.91: icmp_seq=5 ttl=254 time=67.3 ms
64 bytes from 10.0.0.91: icmp_seq=6 ttl=254 time=67.4 ms
64 bytes from 10.0.0.91: icmp_seq=7 ttl=254 time=67.4 ms
64 bytes from 10.0.0.91: icmp_seq=8 ttl=254 time=67.5 ms
64 bytes from 10.0.0.91: icmp_seq=9 ttl=254 time=67.3 ms
^C
--- 10.0.0.91 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8013ms
rtt min/avg/max/mdev = 67.330/67.448/67.692/0.240 ms
```

## 2.5 Capa de red VPC

- Práctica: Conectar 2 VPC utilizando el backbone de AWS



## 2.5 Capa de red VPC

- Práctica: Conectar 2 VPC utilizando el backbone de AWS
- Una vez creados los VPC , las subredes
- Y configurados los security groups y accesslist
- Crear un “Peering Connection”



### Create Peering Connection

Peering connection name tag

Select a local VPC to peer with

VPC (Requester)\*

CIDRs	CIDR	Status	Status Reason
	10.0.0.0/16	● associated	

Select another VPC to peer with

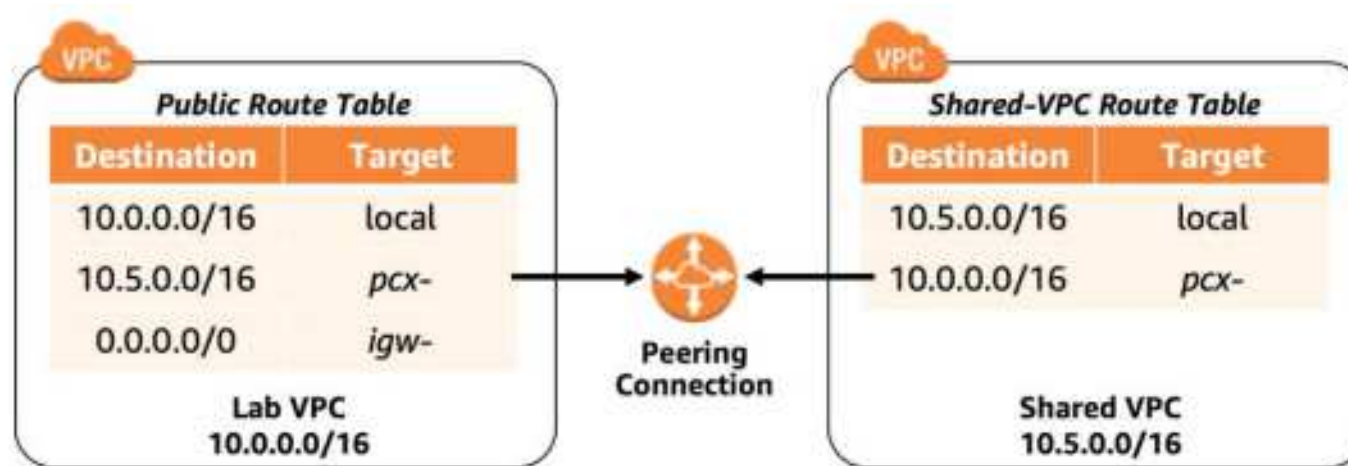
Account ☒ My account ☐ Another account

Region ☒ This region (us-east-1) ☒ Another Region

VPC (Acceptor)\*

## 2.5 Capa de red VPC

- Práctica: Conectar 2 VPC utilizando el backbone de AWS
- Configurar las tablas de enrutamiento





## 2.5 Capa de red VPC

- Práctica: Conectar 2 VPC utilizando el backbone de AWS
- Configurar las tablas de enrutamiento

### Edit routes

Destination	Target	Status
10.0.0.0/16	local	active
0.0.0.0/0	igw-0983a60c460ef0795	active
10.1.0.0/16		

Add route

\* Required

Egress Only Internet Gateway  
Instance  
Internet Gateway  
NAT Gateway  
Network Interface  
**Peering Connection**  
Transit Gateway  
Virtual Private Gateway

## 2.5 Capa de red VPC

- Práctica: Conectar 2 VPC utilizando el backbone de AWS
- Configurar las tablas de enrutamiento en las subredes de cada VPC
  - A continuación están en dos subredes de dos VPC diferentes

Destination	Target	Status
10.0.0.0/16	local	active
0.0.0.0/0	igw-0983a60c460ef0795	active
10.1.0.0/16	pcx-0a85c1c52ce55e22d	

Destination	Target	Status	Propagated	
10.1.0.0/16	local	active	No	
0.0.0.0/0	igw-062f2c61	active	No	✕
10.0.0.0/16	pcx-0a85c1c52ce55e22d		No	✕

## 2.5 Capa de red VPC

- Práctica: Conectar 2 VPC utilizando el backbone de AWS
- Probando conectividad
  - Antes de probar el “Peering connection” debe de ser aceptada



Name	Peering Connection	Status
VPC-MATE...	pcx-0a85c1c52ce...	Pending Acce...

Destination	Target	Status
10.1.0.0/16	local	active
0.0.0.0/0	igw-062f2c61	active
10.0.0.0/16	pcx-0a85c1c52ce55e22d	blackhole



## **2.5 Capa de red VPC**

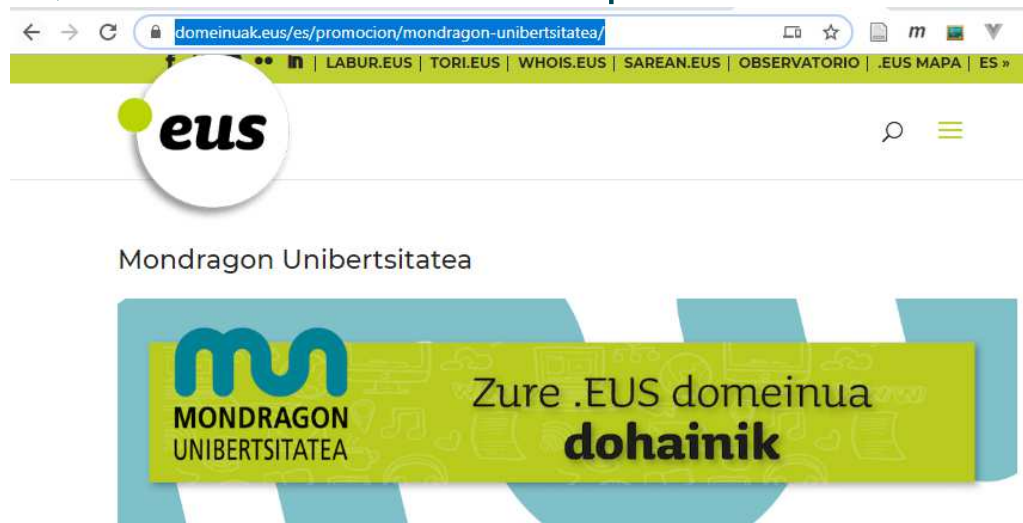
- Práctica: DNS Route 53

## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - Servicio de nombres
  - Registro de dominios
  - Gestión de trafico
  - Monitorización de disponibilidad

## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - Registro de dominios
  - AWS , también ofrece la compra de dominios



Gracias al acuerdo de colaboración suscrito entre Mondragon Unibertsitatea y la Fundación PuntuEUS, los integrantes de los siguientes colectivos contarán con condiciones especialmente ventajosas para adquirir los dominios .EUS:

- **Los estudiantes de Mondragon Unibertsitatea tendrán un código de descuento con el que podrán registrar gratis** sus dominios .EUS. Los alumnos disfrutarán de esta ventaja mientras mantengan la condición de alumnos, y podrán usar dicho dominio en los sitios web que pongan en marcha para sus proyectos académicos, blogs personales o actividades de ocio.
- **Los ex alumnos y los trabajadores de Mondragon Unibertsitatea obtendrán un código de descuento del 25 %** para registrar el dominio .EUS.

Si eres miembro de alguno de esos colectivos, rellena este formulario, y te enviaremos el código de descuento que necesitas para registrar el dominio .EUS, así como las instrucciones para hacerlo.

[Solicitar código de descuento](#)

## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - Registro de dominios
  - AWS , también ofrece la compra de dominios

1: Buscar un dominio  
2: Detalles de contacto  
3: Verificar y comprar

### Elegir un nombre de dominio

adibidea .net - 11,00 \$ [Comprobar](#)

#### Disponibilidad de 'adibidea.net'

Nombre de dominio	Estado	Precio /1 año	Acción
adibidea.net	✓ Disponible	11,00 \$	<a href="#">Añadir al carro</a>

#### Sugerencias de dominios relacionados

Nombre de dominio	Estado	Precio /1 año	Acción
adibdata.com	✓ Disponible	12,00 \$	<a href="#">Añadir al carro</a>
adibdata.net	✓ Disponible	11,00 \$	<a href="#">Añadir al carro</a>
adibidea.ninja	✓ Disponible	18,00 \$	<a href="#">Añadir al carro</a>

## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - Una vez obtenido el dominio se debe de crear un HOSTED ZONE
    - Permite realizar la configuración para que se enrute el trafico a la IP donde se quiere alojar el dominio
    - Redirigir el tráfico de Internet de example.com a la dirección IP de un host de su centro de datos
    - Redirigir el correo electrónico de ese dominio (ichiro@example.com) a un servidor de correo (mail.example.com)
    - Redirigir el tráfico para un subdominio llamado operations.tokyo.example.com a la dirección IP de un host diferente



## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - Configurando registro de dominio para un HOSTED ZONE
    - dinahosting
  - Siendo un servidor de EC2 de AWS

Quiero hacer un... Host IP

Registro A  .jaagirre.eus

Ej.: 24

### Listado de registros

Tipo		Host	Valor
A	<input type="checkbox"/>	www	3.88.30.76

Exportar ▴

Importar ▴

## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - Configurando registro de dominio par aun HOSTED ZONE
  - Siendo un servidor de EC2 de AWS

Quiero hacer un... Host IP

Registro A  .jaagirre.eus

Ej.: 241

### Listado de registros

Tipo		Host	Valor
A	<input type="checkbox"/>	www	3.88.30.76

Exportar ▴

Importar ▴

jaagirre.eus x Practicas Master - Beste Word... x +

→ No es seguro | jaagirre.eus

Bilatu ...

**Bilatu**

**Azken bidalke**

Kaixo mundua!1

**Iruzkin berriak**

WordPress iruzkingile bat(e)k Kaixo mundua!1 bidalketan

**Artxiboak**

2019(e)ko iraila

## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - AWS HOSTED ZONE : Tipos de Registros
- **Registros A (dirección)** – Asocian un nombre de dominio o uno de subdominio a la dirección IPv4 (por ejemplo, 192.0.2.3) del recurso correspondiente.
- **Registros AAAA (dirección)** – Asocian un nombre de dominio o uno de subdominio a la dirección IPv6 (por ejemplo 2001:0db8:85a3:0000:0000:abcd:0001:2345) del recurso correspondiente.
- **Registros de servidor de correo (MX)** – Dirigen tráfico a servidores de correo.
- **Registros CNAME** – Redirigen el tráfico de un nombre de dominio (example.net) a otro nombre de dominio (example.com).
- **Registros para otros tipos de registros DNS admitidos** – Para consultar una lista de tipos de registros admitidos, consulte [Tipos de registros de DNS admitidos](#).

## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - AWS HOSTED ZONE : Modificando servidores DNS
    - Crear un HOSTED\_ZONE para el dominio ejemplo.eus
    - Migrando de dinahosting -> ROUTE 53
    - Requiere decir en dinahost los nuevos servidores de DNS de AWS
    - Y a partir de ese momento los gestionaremos desde ROUTE53

☆ Establecer DNS

---

### DNS por defecto

☒ Quiero utilizar los DNS de dinahosting

### DNS propios

DNS 1

ns.dinahosting.com

DNS 2

ns2.dinahosting.com

DNS 3

ns3.dinahosting.com

DNS 4

ns4.dinahosting.com

DNS 5

DNS 6

## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - AWS HOSTED ZONE : Route53 : Modificando servidores DNS
    - HOSTED ZONE AWS

The screenshot displays the AWS Route 53 console interface. On the left, a list of hosted zones is shown. The zone 'jaagirre.eus.' is selected, and its records are displayed in a table. The table has columns for 'Nombre', 'Tipo', and 'Valor'. The records are:

Nombre	Tipo	Valor
jaagirre.eus.	NS	ns-582.awsdns-08.net. ns-1211.awsdns-23.org. ns-1542.awsdns-00.co.uk. ns-304.awsdns-38.com.
jaagirre.eus.	SOA	ns-582.awsdns-08.net. awsd
www.jaagirre.eus.	A	3.88.30.76

On the right, the 'Editar el conjunto de registros' (Edit record set) panel is shown for the 'www.jaagirre.eus.' record. The 'Nombre' is 'www.jaagirre.eus.', the 'Tipo' is 'A: dirección IPv4', and the 'Alias' is 'No'. The 'TTL (segundos)' is set to 300. The 'Valor' is '3.88.30.76'. Below the value field, there is a note: 'Dirección IPv4. Escriba varias direcciones en líneas distintas. Ejemplo: 192.0.2.235 198.51.100.234'. The 'Política de direccionamiento' is set to 'Simple'.

## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - AWS HOSTED ZONE : Route53 : Modificando servidores DNS
    - Indicar a dinahost que la información de DNS del dominio lo gestionara AWS
    - Tarda un tiempo en actualizar la información

☐ Quiero utilizar los DNS de dinahosting

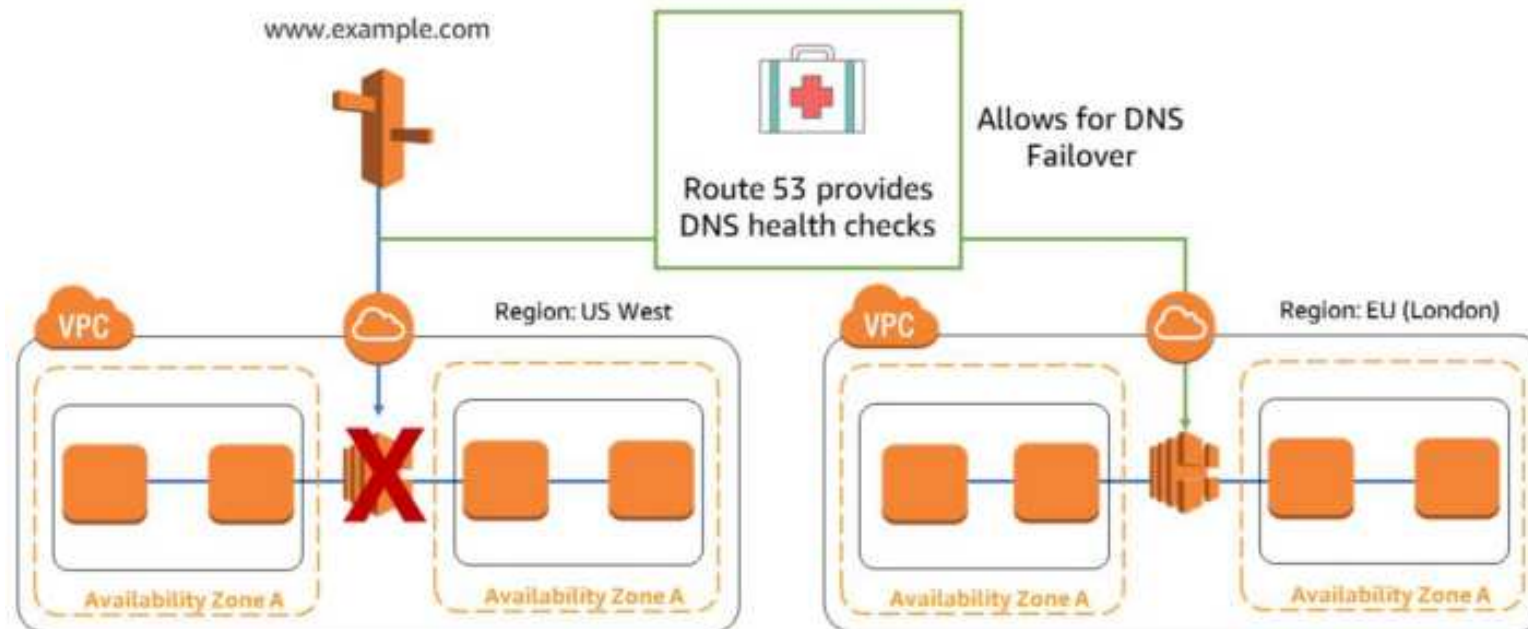
DNS propios

DNS 1	DNS 2
<input type="text" value="ns-582.awsdns-08.net"/>	<input type="text" value="ns-1211.awsdns-23.org"/>
DNS 3	DNS 4
<input type="text" value="ns-1542.awsdns-00.co.uk"/>	<input type="text" value="ns-304.awsdns-38.com"/>
DNS 5	DNS 6
<input type="text"/>	<input type="text"/>

Guardar

## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - Políticas de enrutamiento
    - Servicio de healthcheck y disponibilidad



## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - Políticas de enrutamiento
    - Servicio de healthcheck
    - Politica de enrutamiento
      - Regla ponderada
      - Regla de geolocalización
      - Regla de latencia



## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - Servicio de healthcheck

### Paso 1: Configurar la comprobación de estado

Paso 2: Recibir una notificación cuando se produzca un fallo en la comprobación de estado

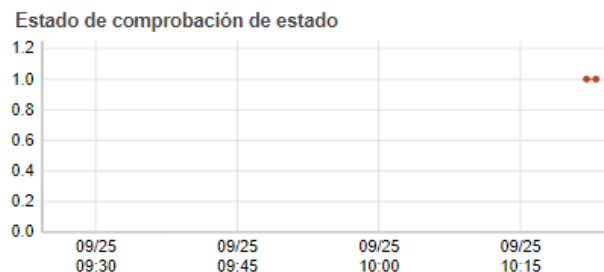
Filtrar por palabra clave		<< < 1 a 1 de 1 comprobaciones
Nombre	Estado	
<input checked="" type="checkbox"/> Primary web server	<div><div></div></div> <span>hace 15 minutos</span> <span>ahora</span> <span>Buen estado</span>	

Información	<b>Monitorización</b>	Alarmas	Etiquetas	Comprobadores de estado
-------------	-----------------------	---------	-----------	-------------------------

Haga clic en un gráfico para ver una vista expandida. [Ver métricas en CloudWatch](#)

Comprobaciones de estado ■ Primary web server

Intervalo de tiempo Última hora Actualizar



### Configurar la comprobación de estado

Las comprobaciones de estado de Route 53 le permiten realizar un seguimiento del estado de sus recursos cuando se produce una interrupción.

Nombre  ⓘ

Qué se debe monitorizar Punto de enlace

### Monitorizar un punto de enlace

Varios comprobadores de estado de Route 53 intentarán establecer una conexión TCP con el siguiente

Especificar el punto de enlace por Dirección IP

Protocolo HTTP ⓘ

Dirección IP  ⓘ

Nombre de anfitrión  ⓘ

Puerto \*  ⓘ

Ruta

### Configuración avanzada

URL  ⓘ

## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - Políticas de enrutamiento : Configurar Registro A con commutacion por error

<input type="checkbox"/>	www.jaagirre.eus.	A	3.88.30.76
<input type="checkbox"/>	www.jaagirre.eus.	A	18.204.21.97

Nombre del conjunto de registros

Cualquier tipo ☐ Solo con alias ☐ Solo ponderados

Mostrando de 1 a 5 de un total de 5

<input type="checkbox"/>	Nombre	Tipo	Valor
<input type="checkbox"/>	jaagirre.eus.	A	3.88.30.76
<input type="checkbox"/>	jaagirre.eus.	NS	ns-1211.awsdns-23.org. ns-582.awsdns-08.net. ns-1542.awsdns-00.co.uk ns-304.awsdns-38.com.
<input type="checkbox"/>	jaagirre.eus.	SOA	ns-582.awsdns-08.net.
<input checked="" type="checkbox"/>	www.jaagirre.eus.	A	3.88.30.76
<input type="checkbox"/>	www.jaagirre.eus.	A	18.204.21.97

**Editar el conjunto de registros**

Nombre: www.jaagirre.eus.

Tipo: A: dirección IPv4

Alias: ☒ Sí ☐ No

TTL (segundos): 300 1 m 5 m 1 h 1 d

Valor: 3.88.30.76

Dirección IPv4. Escriba varias direcciones en líneas distintas.  
Ejemplo:  
192.0.2.235  
198.51.100.234

Política de direccionamiento: Conmutación por enrutamiento

Route 53 responde a las consultas mediante conjuntos de registros principales si tienen un estado correcto o, de lo contrario, mediante conjuntos de registros secundarios. [Más información](#)

Tipo de registro de conmutación por error: ☒ Principal

ID de conjunto: www-Principal

Asociar a comprobación de estado: ☒ Sí ☐ No

Al responder a las consultas, Route 53 puede omitir los recursos que no superen las comprobaciones de estado. [Más información](#)

Comprobación de estado que se va a asociar: **adiidea**

## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - Políticas de enrutamiento : Crear registro secundario

**Editar el conjunto de registros**

**Nombre:**

**Tipo:**

**Alias:** ☐ Sí ☒ No

**TTL (segundos):**  1 m 5 m 1 h 1 d

**Valor:**

Dirección IPv4. Escriba varias direcciones en líneas distintas.  
Ejemplo:  
192.0.2.235  
198.51.100.234

**Política de direccionamiento:**

Route 53 responde a las consultas mediante conjuntos de registros principales si tienen un estado correcto o, de lo contrario, mediante conjuntos de registros secundarios. [Más información](#)

**Tipo de registro de conmutación por error:** ☐ Principal ☒ Secundario





**ID de conjunto:**



**Asociar a comprobación de estado:** ☐ Sí ☒ No

Nombre	Tipo	Valor
jaagirre.eus.	A	3.88.30.76
jaagirre.eus.	NS	ns-1211.awsdn ns-582.awsdn ns-1542.awsdn ns-304.awsdn
jaagirre.eus.	SOA	ns-582.awsdn
www.jaagirre.eus.	A	3.88.30.76
www.jaagirre.eus.	A	18.204.21.97

## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - Políticas de enrutamiento : Verificar funcionamiento de regla

	wordpress	i-0978...	t2.micro	us-east-1a	 stopped
	web_seco	i-0f87e...	t2.micro	us-east-1c	 running

Nombre	Estado
<input checked="" type="checkbox"/> Primary web server	 hace 31 minutos  ahora <b>Incorrecto</b>

Información	<b>Monitorización</b>	Alarmas	Etiquetas	Comprobadores d
-------------	-----------------------	---------	-----------	-----------------

Haga clic en un gráfico para ver una vista expandida. [Ver métricas en CloudWatch](#)

Comprobaciones de estado  Primary web server


Intervalo de tiempo Última hora Actualizar

Estado de comprobación de estado




Comprobadores de estado que indican el estado del punto de enlace (%)



ALARM: "Primary\_web\_server-awsroute53-a58ecfb0-898f-4cd2-1 Virginia)  Sarrera-ontzia x

**AWS Notifications** <no-reply@sns.amazonaws.com>  
hartzaileak: ni

 ingeles > euskara [Itzuli mezua](#)

You are receiving this email because your Amazon CloudWatch Alarm "Primary\_web\_server-awsroute53-a58ecfb0-898f-4cd2-1 Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 datapoint [0.0 (25/09/19 08:48:00) 08:49:08 UTC".

View this alarm in the AWS Management Console:

[https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#s=Alarms&alarm=Primary\\_web\\_HealthCheckStatus](https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#s=Alarms&alarm=Primary_web_HealthCheckStatus)

Alarm Details:

- Name: Primary\_web\_server-awsroute53-a58ecfb0-898f-4cd2-855f-31a433977e50-Low-HealthCh
- Description:
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 datapoint [0.0 (25/09/19 08:48:00)] was less than the threshc
- Timestamp: Wednesday 25 September, 2019 08:49:08 UTC
- AWS Account: 420693608596

Threshold:

- The alarm is in the ALARM state when the metric is LessThanThreshold 1.0 for 60 seconds.

## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - Políticas de enrutamiento : Verificar funcionamiento de regla
  - La recuperación tarda unos **5 minutos**

<input type="checkbox"/>	web_seco	i-0f87e...	t2.micro	us-east-1c	<span style="color: green;">●</span> running	✓ 2/2 checks
<input checked="" type="checkbox"/>	wordpress	i-0978...	t2.micro	us-east-1a	<span style="color: green;">●</span> running	✓ 2/2 checks

Nombre	Estado
<input checked="" type="checkbox"/> adiidea	<span style="color: green;">■</span> hace 30 minutos ahora Buena
<input type="checkbox"/> Primary web server	<span style="color: red;">■</span> hace una hora ahora Incorrec

Información Monitorización Alarmas Etiquetas Comprueba

Haga clic en un gráfico para ver una vista expandida. [Ver métricas en CloudV](#)

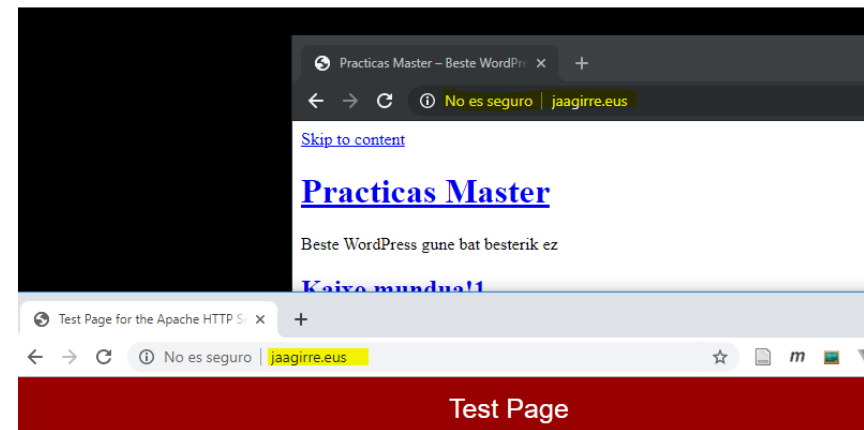
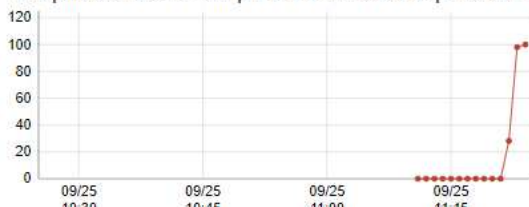
Comprobaciones de estado ■ adiidea

Intervalo de tiempo Última hora Actualizar

Estado de comprobación de estado



Comprobadores de estado que indican el estado del punto de enlace (%)



This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

### If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting [www.example.com](http://www.example.com), you should send e-mail to "webmaster@example.com".

### If you are the website administrator:

You may now add content to the directory `/var/www/`. Note that until you do so, people visiting your website see this page, and not your content. To prevent this from ever being used, follow the instructions in the `/etc/httpd/conf.d/welcome.conf`.

You are free to use the image below on web sites powered by the Apache HTTP Server:



## 2.5 Capa de red VPC

- DNS : Servicio Route53
- Políticas de enrutamiento

Panel

[Zonas hospedadas](#)

Comprobaciones de estado

Flujo de tráfico

**Políticas de tráfico**

Registros de política

Dominios

Dominios registrados

Solicitudes pendientes

Resolver

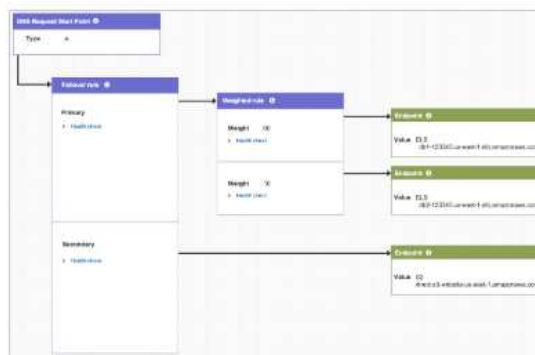
VPCs

Puntos de enlace de entrada

Puntos de enlace de salida

Reglas

Le damos la bienvenida al flujo de tráfico



El editor visual de flujo de tráfico le permite crear configuraciones de direccionamiento sofisticadas para sus recursos utilizando tipos de direccionamiento existentes, como la conmutación por error y la geolocalización. Guarde la configuración como una política de tráfico y, a continuación, utilícela para crear uno o varios registros de política. Cada registro de política direcciona las consultas DNS de un dominio o subdominio especificado.

Puede crear varias versiones de la misma política de tráfico y utilizar versiones diferentes para implementar o restaurar los cambios de configuración.

[Más información](#)

[Crear la política de tráfico](#)

### Conceptos



Editor visual

Utilice un editor visual intuitivo para crear configuraciones complejas y guárdelas como políticas de tráfico.

[Ver documentación](#)



Versões de la política de tráfico

Cree varias versiones de una política de tráfico y utilice el control de versiones para implementar o restaurar las actualizaciones.

[Ver documentación](#)



Registros de política

Cree registros de política para asociar políticas de tráfico a nombres de dominio o subdominio.

[Ver documentación](#)



## 2.5 Capa de red VPC

- DNS : Servicio Route53
  - Políticas de enrutamiento

