# AWS Technical Essentials

Capítulo 01

**Sesión 04: VPC.**

# Al término de esta sesion, Ud. podrá:

- Conocer el servicio de VPC detalladamente.
- Entender la importancia del funcionamiento de VPC y su integración con los demás servicios de AWS.
- Diseñar servicios con mejores prácticas de seguridad y red en AWS.

# Virtual Private Cloud - VPC

- Permite aprovisionar una sección de la nube de Amazon Web Services (AWS) aislada de forma lógica, en la que puede lanzar recursos de AWS en una red virtual que defina.
- Puede controlar todos los aspectos del entorno de red virtual, incluida la selección de su propio rango de direcciones IP, la creación de subredes y la configuración de tablas de ruteo y puertas de enlace de red.
- Puede usar tanto IPv4 como IPv6 en su VPC para un acceso seguro y fácil a recursos y aplicaciones.

# Virtual Private Cloud - VPC

- Es fácil personalizar la configuración de red de su Amazon Virtual Private Cloud. Por ejemplo, puede crear una subred de cara al público para los servidores web con acceso a Internet y colocar los sistemas de fondo, como bases de datos o servidores de aplicaciones, en una subred de uso privado sin acceso a Internet.
- Puede aprovechar varias capas de seguridad, incluidos grupos de seguridad y listas de control de acceso a red, para ayudar a controlar el acceso a las instancias de Amazon EC2 desde cada subred.

# Virtual Private Cloud - VPC

- Puede tener hasta cinco (5) Amazon VPC no predeterminadas por cuenta de AWS en cada región.
- Puede tener hasta cuatro (4) intervalos IP secundarios por VPC
- Puede crear hasta doscientas (200) subredes en cada Amazon VPC.
- Puede tener hasta cinco (5) direcciones IP elásticas de Amazon VPC por cuenta de AWS y región.
- Puede tener hasta diez (10) conexiones de VPN de hardware por cada Amazon VPC.
- Estos límites pueden ampliarse mediante un caso con AWS.

# Componentes - VPC

- **Subred**: segmento del rango de direcciones IP de una VPC donde es posible colocar grupos de recursos aislados.
- **Puerto de enlace a Internet:** el extremo de Amazon VPC de una conexión a la Internet pública.
- **Gateway NAT**: un servicio administrado y de alta disponibilidad de conversión de direcciones de red (NAT) para que los recursos que tiene en una subred privada obtengan acceso a Internet.
- **Conexión de VPN de hardware**: una conexión de hardware entre su Amazon VPC y el centro de datos, la red de inicio o el centro de colocación.
- **Gateway privada virtual**: el extremo de Amazon VPC en una conexión de VPN.

# Componentes - VPC

- **Gateway de cliente:** el extremo que ocupa el usuario en una conexión de VPN.

- **Router**: los routers interconectan entre sí las subredes y dirigen el tráfico entre puertos de enlace a Internet, gateways privadas virtuales, gateways NAT y subredes.

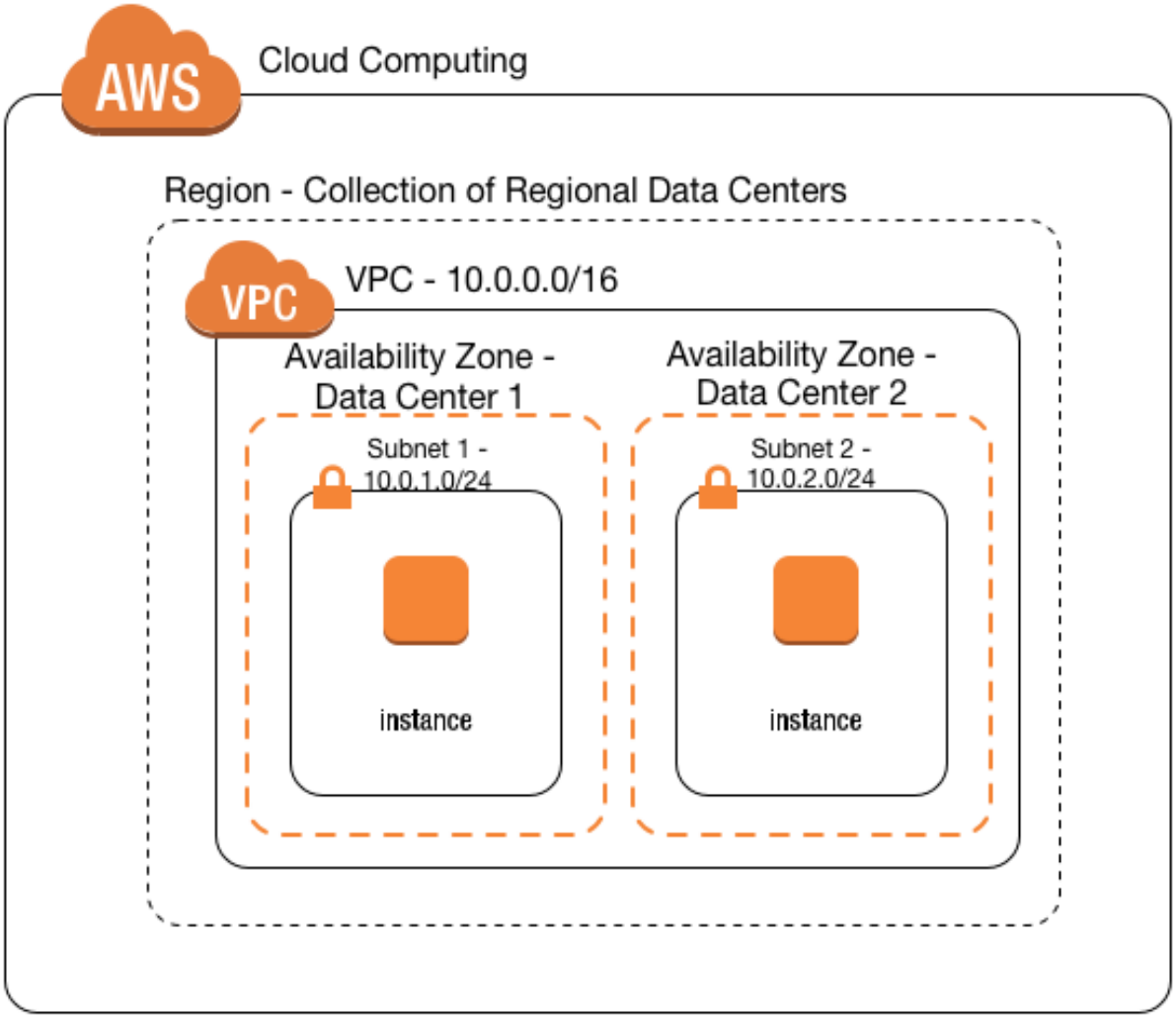
- **Interconexiones**: este tipo de conexión le permite enrutar el tráfico a través de direcciones IP privadas entre dos VPC interconectadas.

# Componentes - VPC

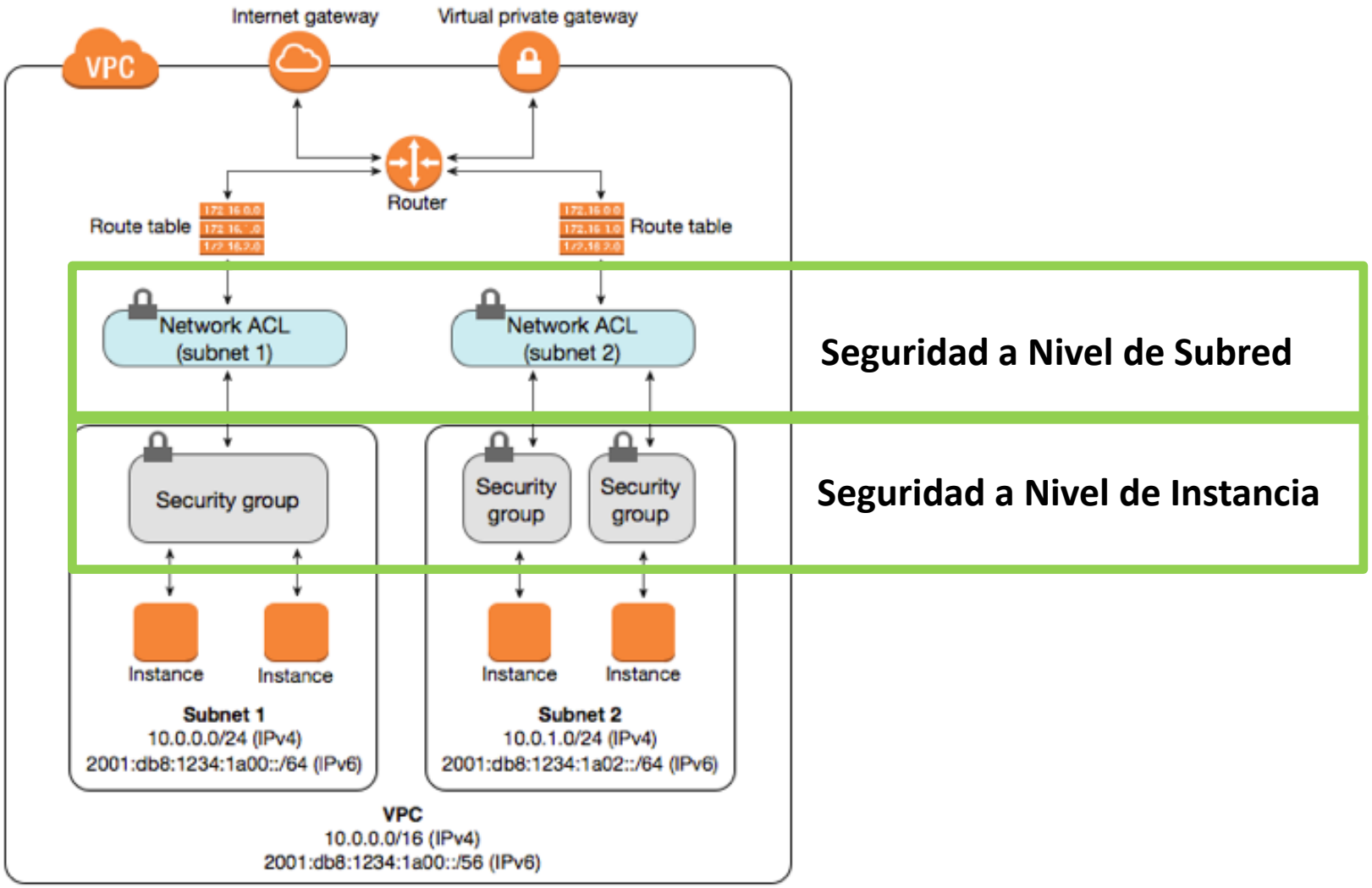
- **Punto de enlace de la VPC**: permite obtener acceso a Amazon S3 desde su VPC sin usar un puerto de enlace a Internet o NAT, así como controlar el acceso mediante las políticas de punto de conexión de la VPC.

- **Gateway de Internet de salida únicamente**: un gateway con estado para brindar acceso de salida únicamente para tráfico IPv6 de la VPC a Internet

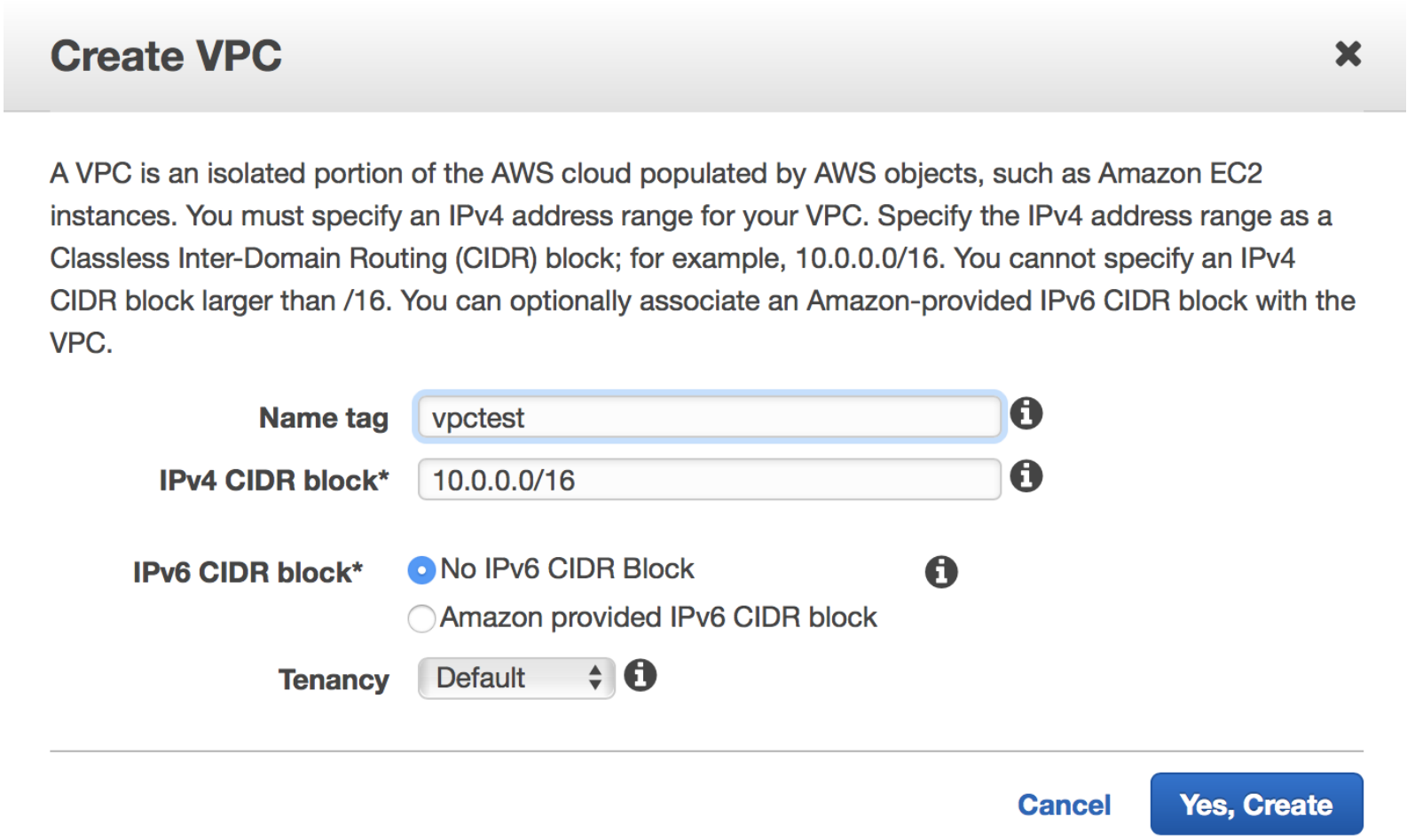
# Componentes - VPC



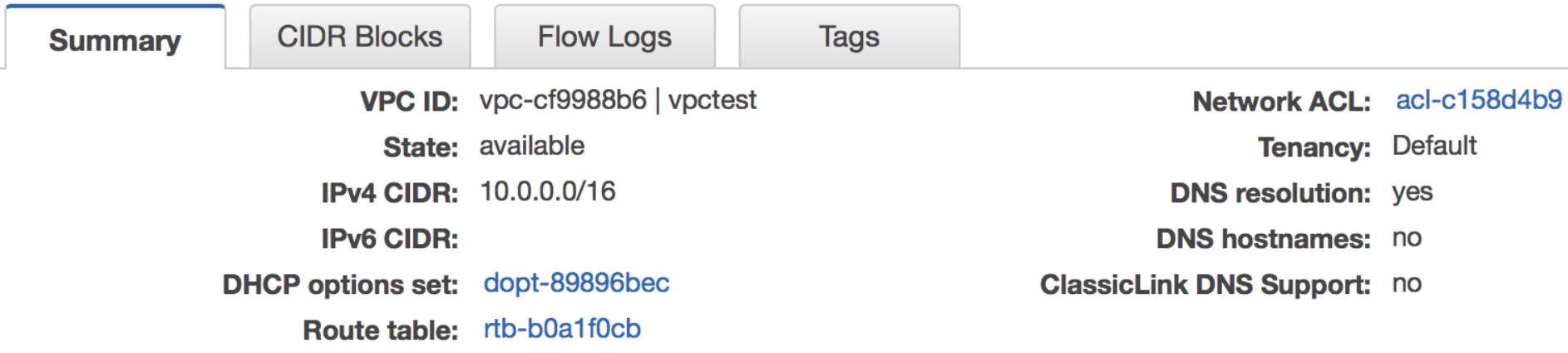
# Componentes - VPC



# Componentes - VPC



# Componentes - VPC



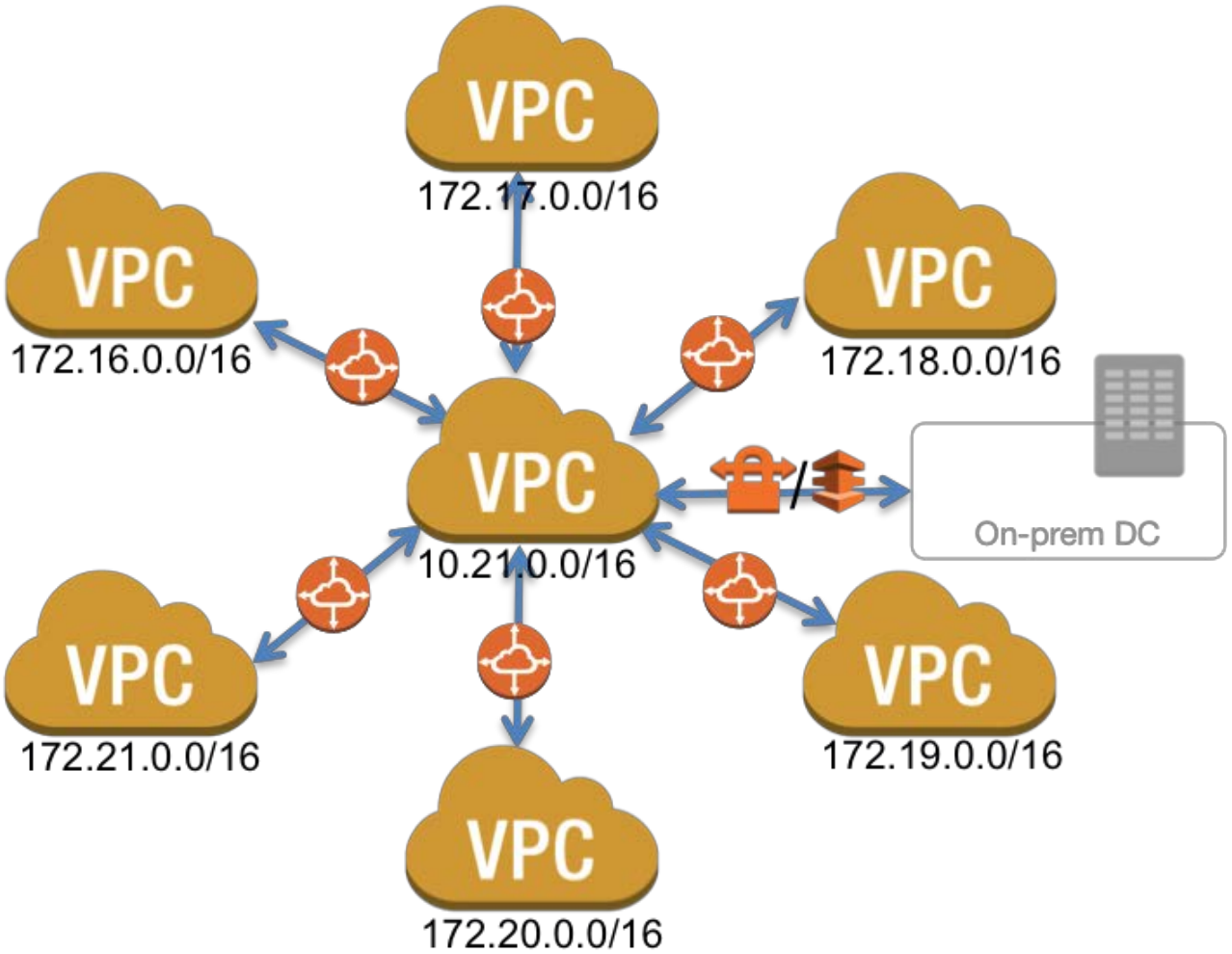
# Tips - VPC

- Se pueden lanzar las instancias en la subred que uno escoja.
- Se pueden asignar EIP automáticamente a las instancias.
- Todas las subredes por en la VPC por defecto tienen una tabla de enrutamiento a internet.
- Si se elimina la VPC por defecto se debe poner un ticket a AWS.
- Al crear una VPC debemos definir nuestro rango de direccionamiento IP.
- Por defecto se crea una ACL y una tabla de enrutamiento.
- ACL pueden estar a través de multiples subredes.
- Un grupo de seguridad puede ser asociado a una o más instancias.

# VPC Peering

- Permite realizar la conexión entre 2 VPC.
- Las instancias se comportan como si estuvieran en la misma red.
- No existen las VPC transitivas.
- 1 Subred es equivalente a una sola zona de disponibilidad.
- Los grupos de seguridad son Stateful.
- Las listas de Acceso de Red (ACL) son Stateless.

# VPC Peering


VPC
172.17.0.0/16
VPC
172.16.0.0/16
VPC
172.18.0.0/16
VPC
10.21.0.0/16
On-prem DC
VPC
172.21.0.0/16
VPC
172.19.0.0/16
VPC
172.20.0.0/16

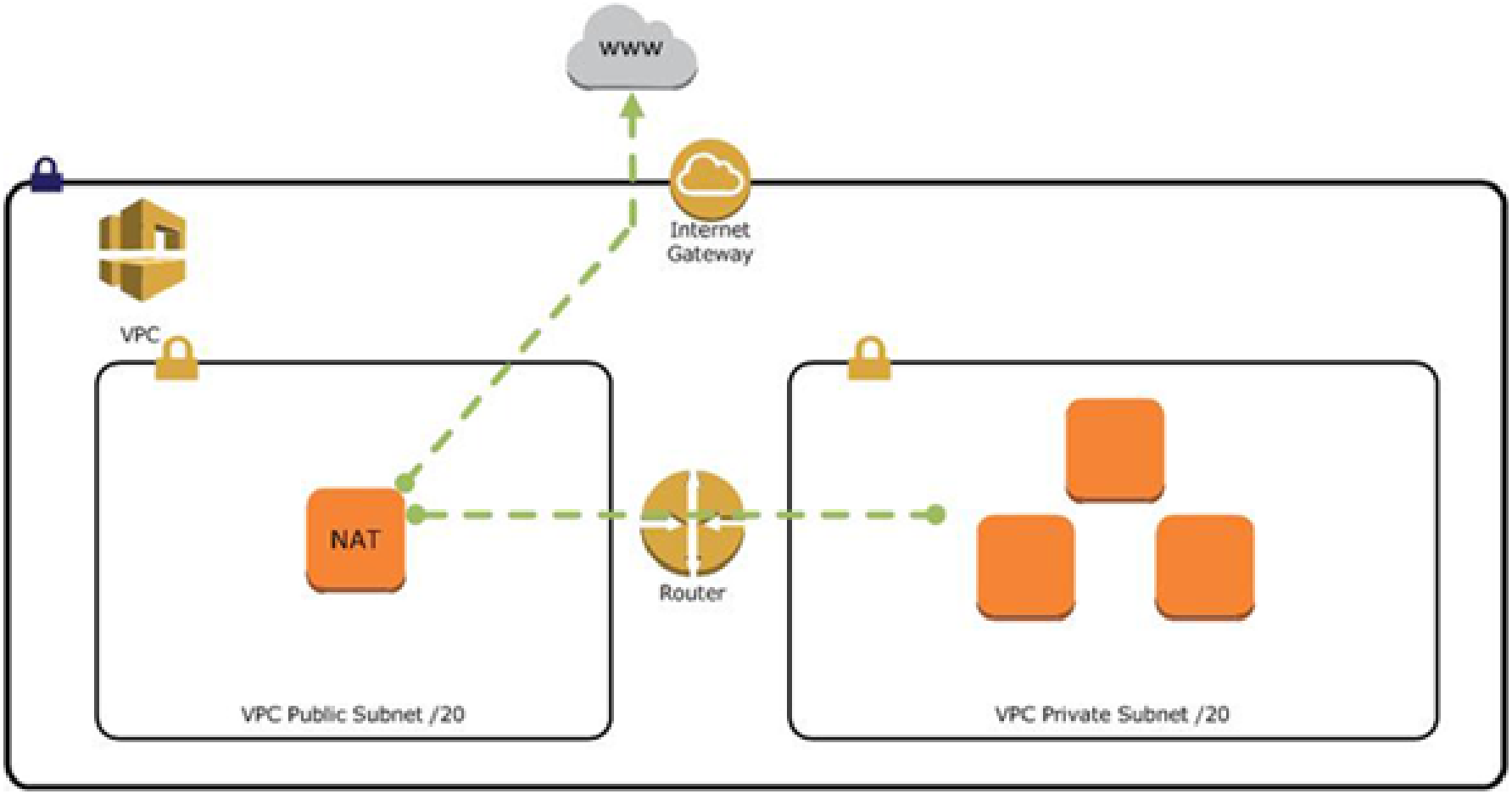
# Grupos de Seguridad vs ACL

| Security Group | Network ACL |
|---|---|
| Operates at the instance level (first layer of defense) | Operates at the subnet level (second layer of defense) |
| Supports allow rules only | Supports allow rules and deny rules |
| Is stateful: Return traffic is automatically allowed, regardless of any rules | Is stateless: Return traffic must be explicitly allowed by rules |
| We evaluate all rules before deciding whether to allow traffic | We process rules in number order when deciding whether to allow traffic |
| Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on | Automatically applies to all instances in the subnets it's associated with (backup layer of defense, so you don't have to rely on someone specifying the security group) |

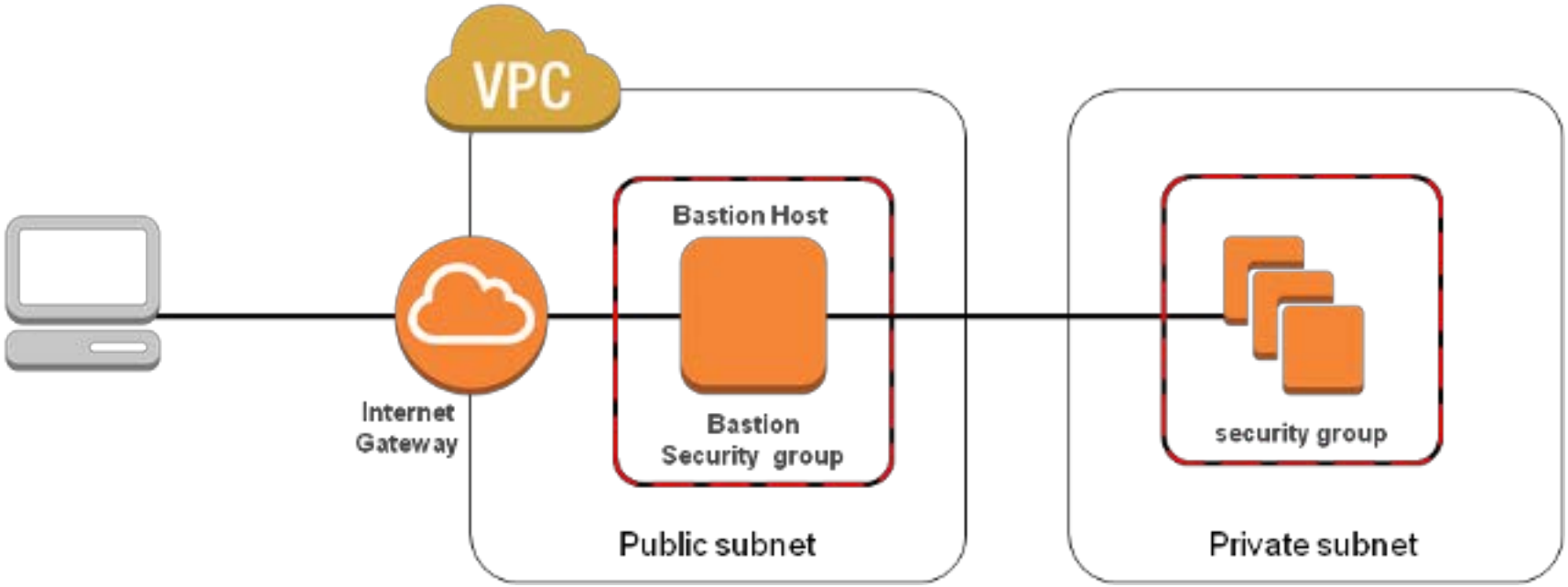
# Nat Gateway vs Nat Instance

| Attribute | NAT gateway | NAT instance |
|---|---|---|
| Availability | Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture. | Use a script to manage failover between instances. |
| Bandwidth | Supports bursts of up to 10Gbps. | Depends on the bandwidth of the instance type. |
| Maintenance | Managed by AWS.You do not need to perform any maintenance. | Managed by you, for example, by installing software updates or operating system patches on the instance. |
| Performance | Software is optimized for handling NAT traffic. | A generic Amazon Linux AMI that's configured to perform NAT. |
| Cost | Charged depending on the number of NAT gateways you use, duration of usage, and amount of data that you send through the NAT gateways. | Charged depending on the number of NAT instances that you use, duration of usage, and instance type and size. |
| Type and size | Uniform offering; you don't need to decide on the type or size. | Choose a suitable instance type and size, according to your predicted workload. |
| Public IP addresses | Choose the Elastic IP address to associate with a NAT gateway at creation. | Use an Elastic IP address or a public IP address with a NAT instance. You can change the public IP address at any time by associating a new Elastic IP address with the instance. |

# NAT Instance



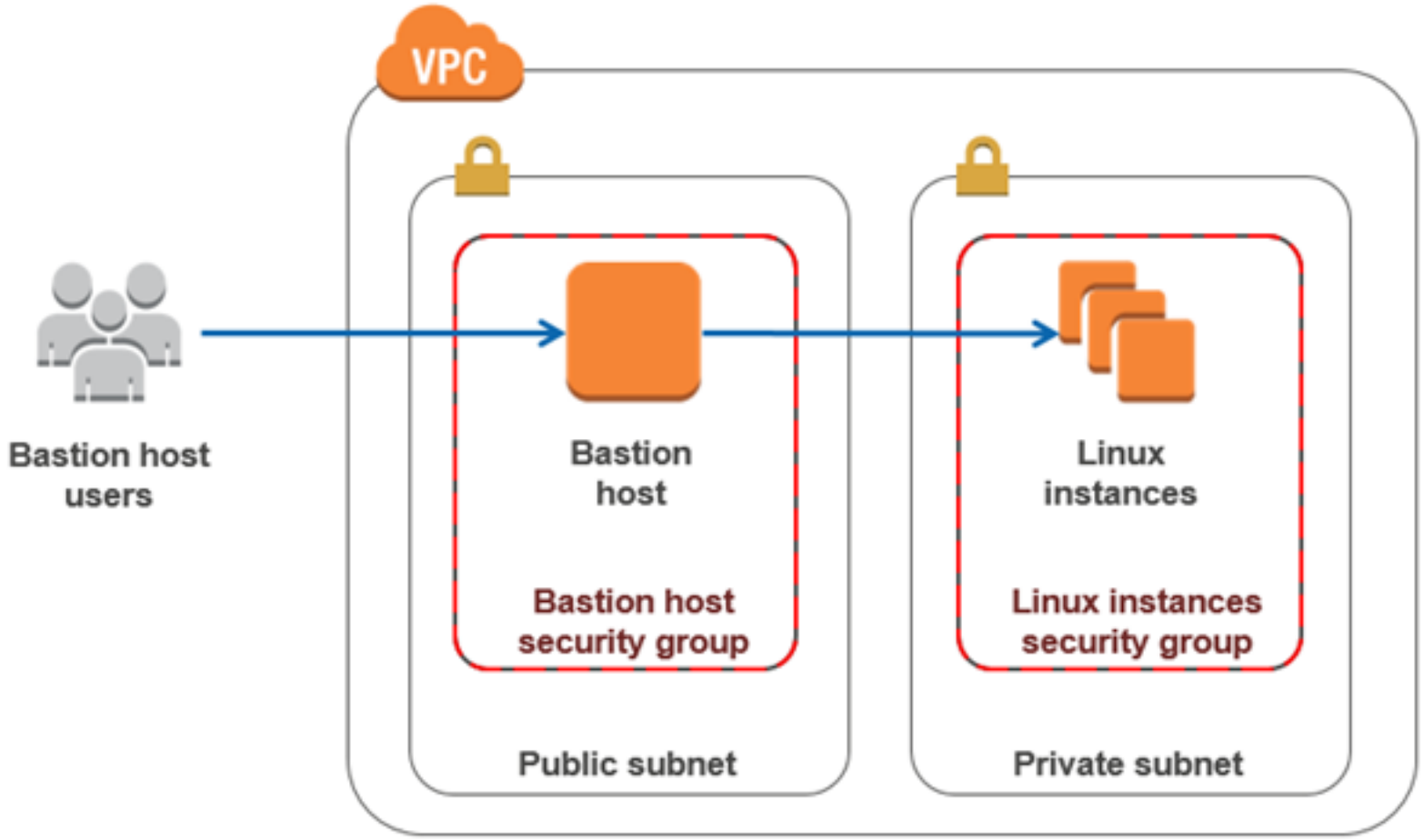
# NAT Gateway


VPC
Bastion Host
Internet
Gateway
Bastion
Security group
security group
Public subnet
Private subnet

# Bastion Host

- Un Bastion Host es usado para acceder de forma segura a las instancias EC2 que se encuentran en subredes privadas, también son conocidos como Jump Box.
- Por recomendación de buenas prácticas se deben tener en al menos 2 zonas diferentes de disponibilidad.
- Se pueden configurar en instancias micro o nano.
- Solo se encargan de proveer un puente seguro entre una red pública y una red privada.
- Usualmente son usados para permitir las conexiones SSH (puerto 22) y RDP (Puerto 3389).

# Bastion Host



# Ejemplos de Arquitecturas

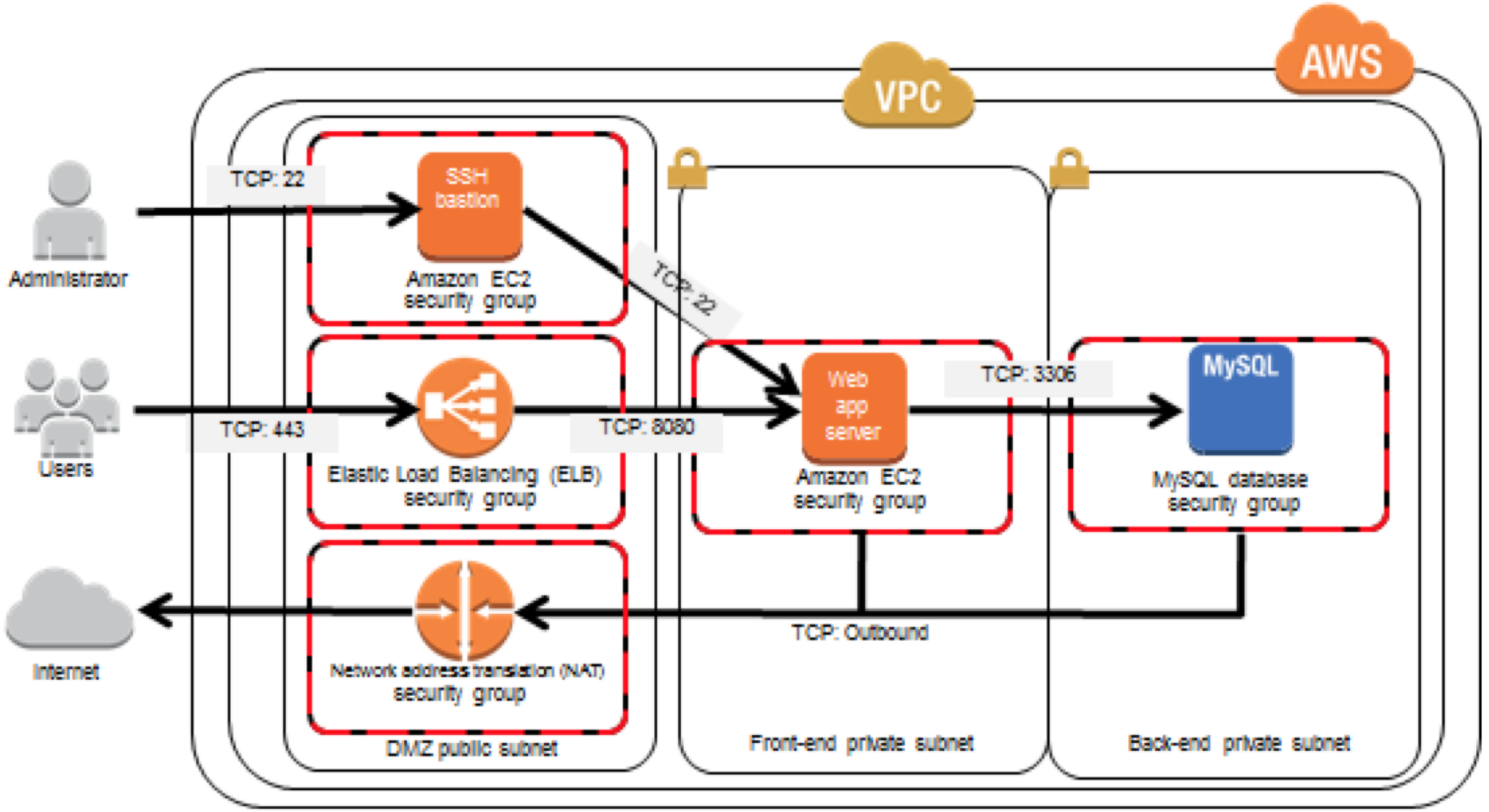
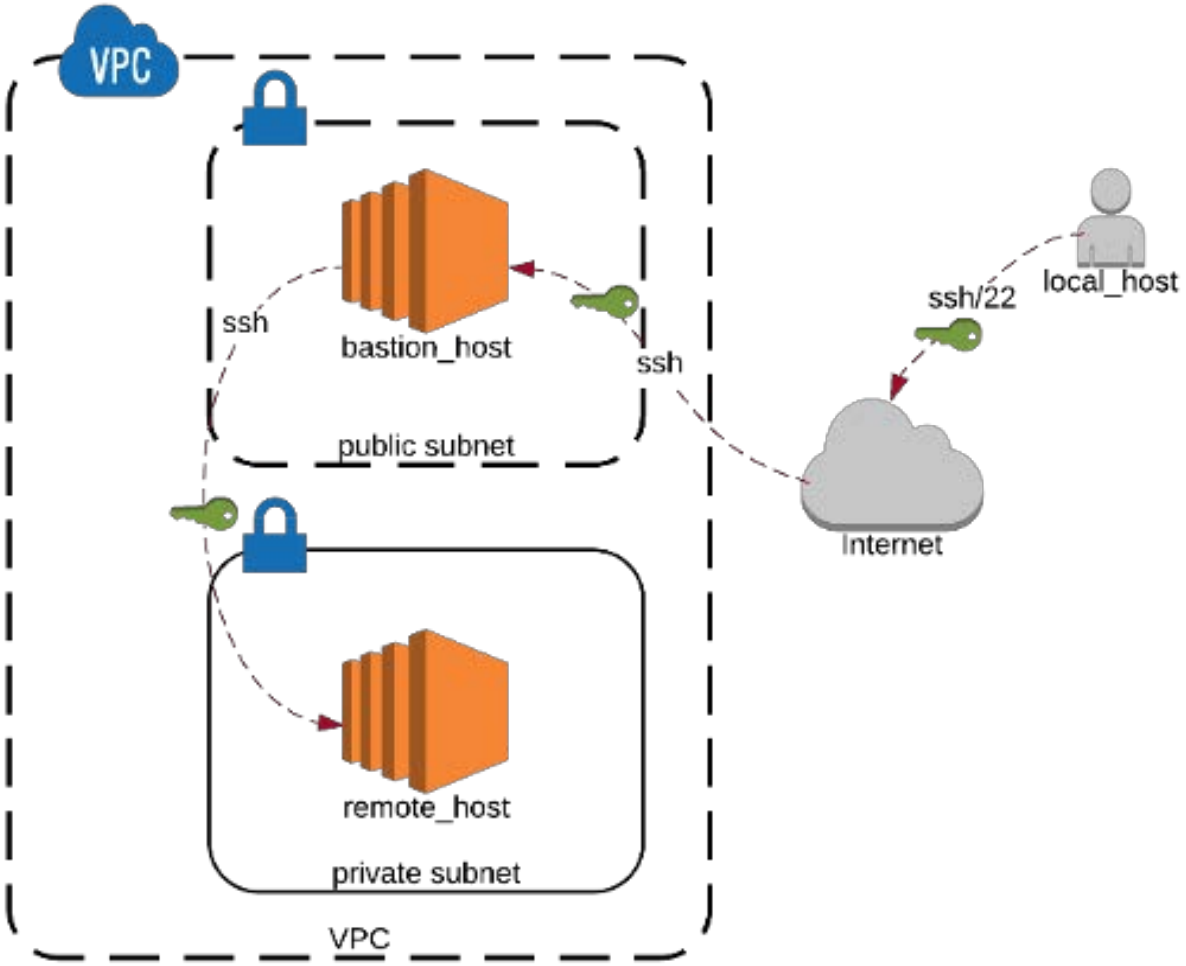
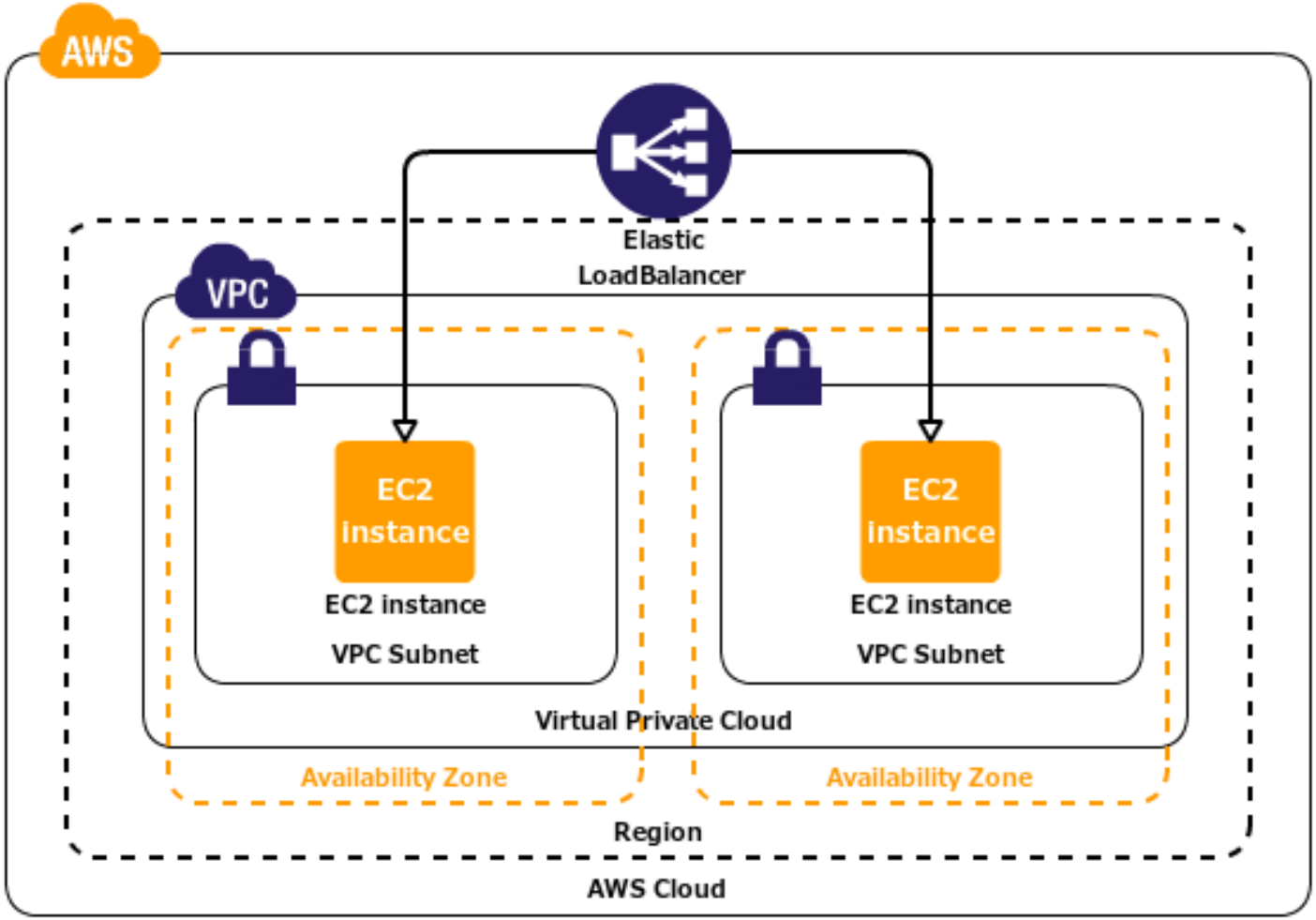



*Figure 2. Reference architecture with Amazon VPC configuration*

# Ejemplos de Arquitecturas



# Ejemplos de Arquitecturas



# Resumen de la Sesión

- Una VPC provee el servicio de conectividad a todos los componentes de una arquitectura AWS.
- Se pueden tener diferentes VPC por cuenta y trabajar entre ellas.
- Las VPC no pueden ser transitivas.
- A nivel de seguridad tenemos 2 escenarios: 1 los security groups a nivel de instancia y las ACL a nivel de subred.
- Un bastión host es usado como una medida de seguridad para nuestras instancias en subredes privadas.