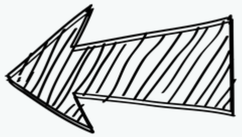
Cloud Computing - AWS

ACADEMIA CONSULTEC

Presentado por **Alejandro Chacón**
www.consultec-ti.com

Agenda

- Intro
- Almacenamiento S3
- Networking 
- Cómputo y Almacenamiento
- Integración y Monitoreo
- Bases de Datos
- Seguridad
- Despliegues y Gestión de Infraestructura

ACADEMIA CONSULTEC

AWS VPC

Redes en la Nube

- Intro
- labs: https://www.awseducate.com
- Direccionamiento IP
- Subredes
- Internet GW / NAT Gateway
- NACL y Grupos de Seguridad
- VPC Flows Logs
- VPC Peering
- VPC Endpoints / Private Link
- VPN & Direct Connect
- Transit Gateway

ACADEMIA CONSULTEC

Virtual Private Cloud
Introduccion

- Las Redes en AWS es algo que debemos conocer en profundidad para entender un poco las bases de sus servicios y es necesario para salvar alguna certificación en la nube.

- En esta sección tocaremos algunos de estos temas:
    - VPC, subredes, puertas de enlace de Internet y puertas de enlace NAT
    - Grupos de seguridad, ACL de red (NACL), VPC Flows Logs
    - VPC Peerings y VPC Endpoints
    - VPN de sitio a sitio y conexión directa (Direct Connect)
    - Transit Gateway

- También daremos un paseo por la "VPC predeterminada" en la consola de AWS

ACADEMIA CONSULTEC

Virtual Private Cloud

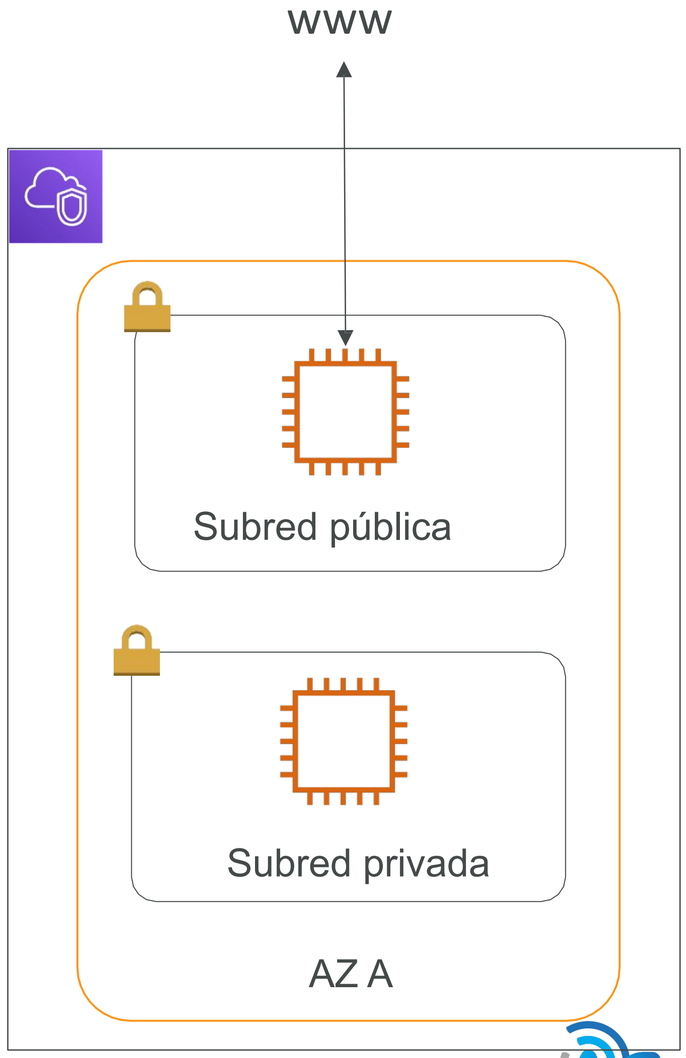
Direccionamiento IP

- IPv4: Protocolo de Internet versión 4 (4,3 mil millones de direcciones)
  - IPv4 pública: se puede utilizar en Internet
  - La instancia EC2 obtiene una nueva dirección IP pública cada vez que se detiene y luego se inicia (predeterminado)
  - IPv4 privada: se puede utilizar en redes privadas (LAN), como redes internas de AWS (p. ej., 192.168.1.1)
  - El IPv4 privada está arreglado para las instancias EC2 incluso si las inicia/detiene
- IP elástica:
  - le permite adjuntar una dirección IPv4 pública fija a la instancia EC2
  - Nota: tiene un costo continuo si no se adjunta a la instancia EC2 o si la instancia EC2 se detiene
- IPv6: Protocolo de Internet versión 6 (3,4 × 10!" Direcciones)
  - Cada dirección IP es pública (sin rango privado)
  - Ejemplo: 2001:db8:3333:4444:cccc:dddd:eeee:ffff

Virtual Private Cloud

Subredes

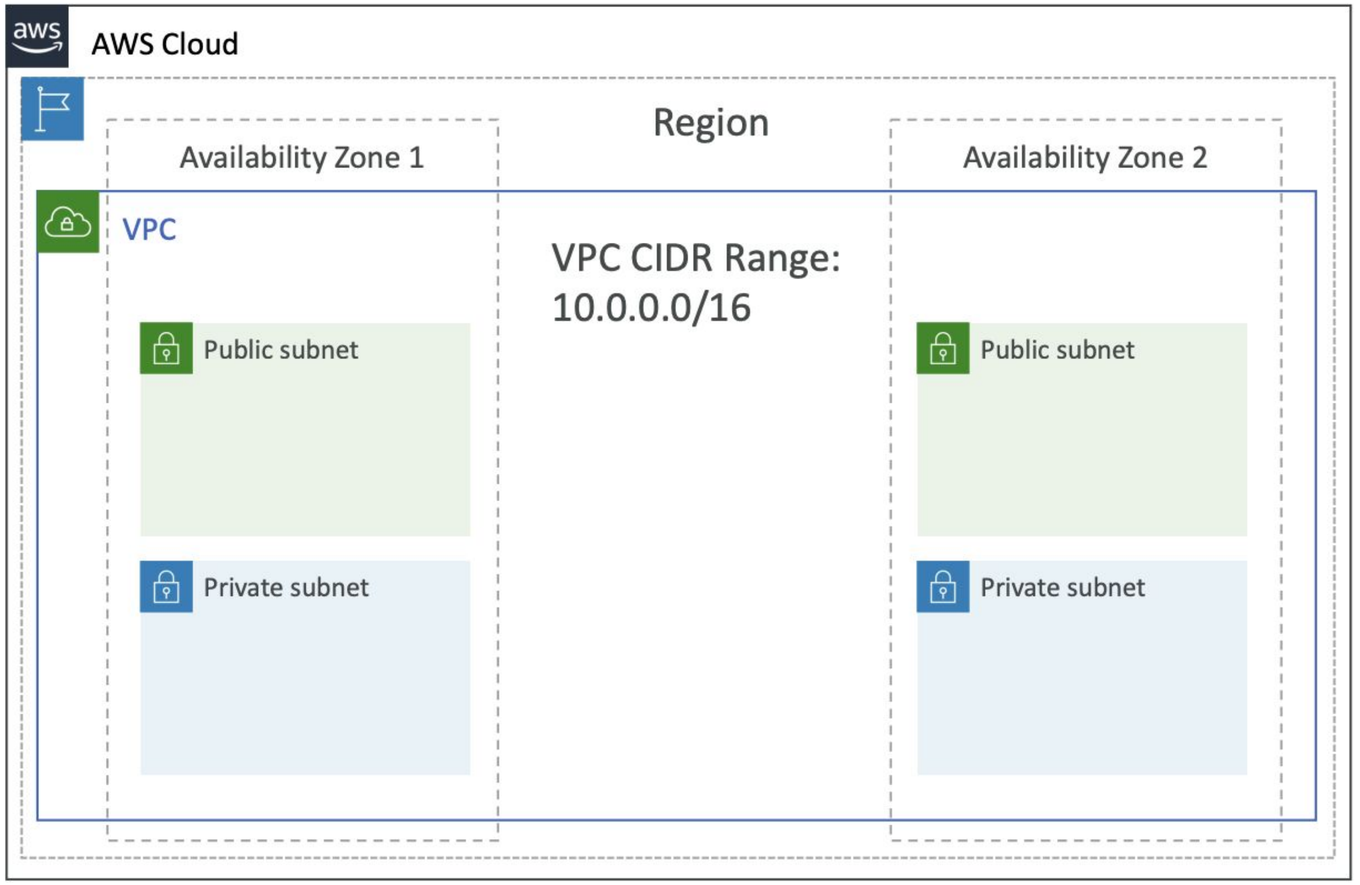
- VPC: privada
- red para desplegar sus recursos (recurso regional)
- Las subredes nos permiten particionar la red dentro de su VPC (recurso de zona de disponibilidad)
- Una subred pública es una subred a la que se puede acceder desde Internet.
- Una subred privada es una subred a la que no se puede acceder desde Internet.
- Para definir el acceso a Internet y entre subredes, usamos tablas de rutas.



ACADEMIA CONSULTEC

Virtual Private Cloud

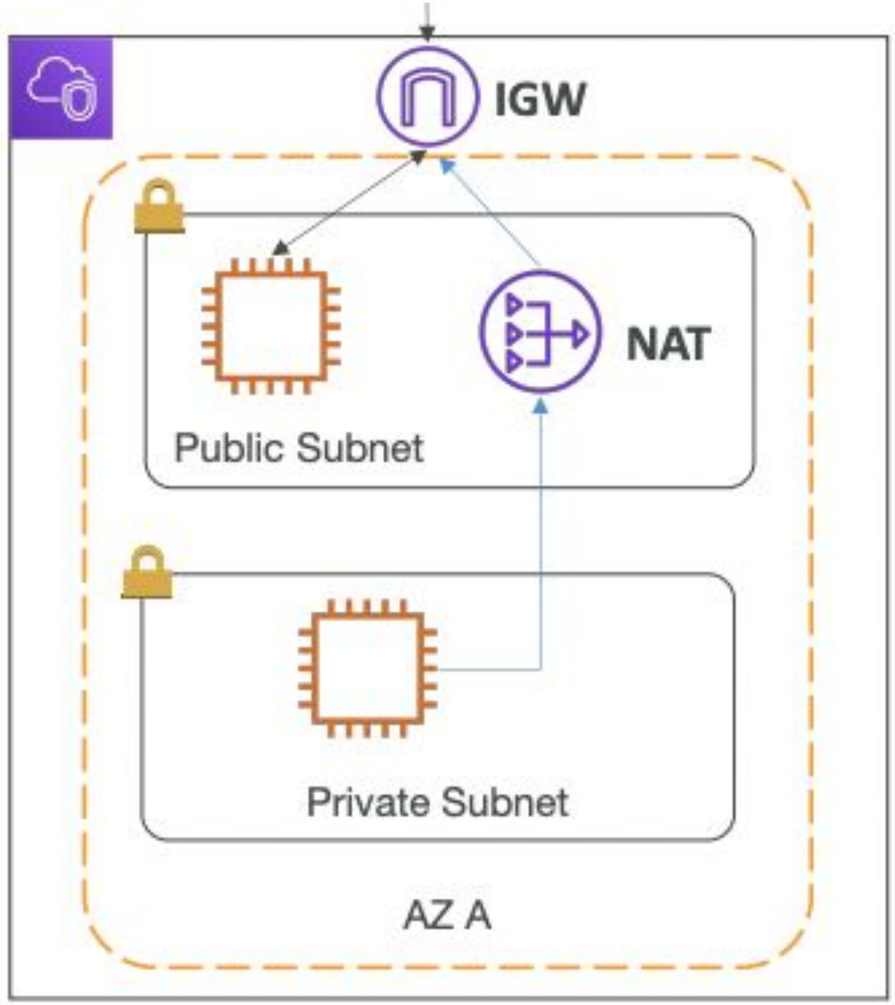
Diagrama VPC



ACADEMIA CONSULTEC

Virtual Private Cloud
IGW & NAT Gateways

- Internet Gateways ayuda a nuestras instancias de VPC a conectarse a Internet
- Las subredes públicas tienen una ruta a la puerta de enlace de Internet.
- Las puertas de enlace NAT (administradas por AWS) y las instancias NAT (autoadministradas) permiten que sus instancias en sus subredes privadas accedan a Internet sin dejar de ser privadas

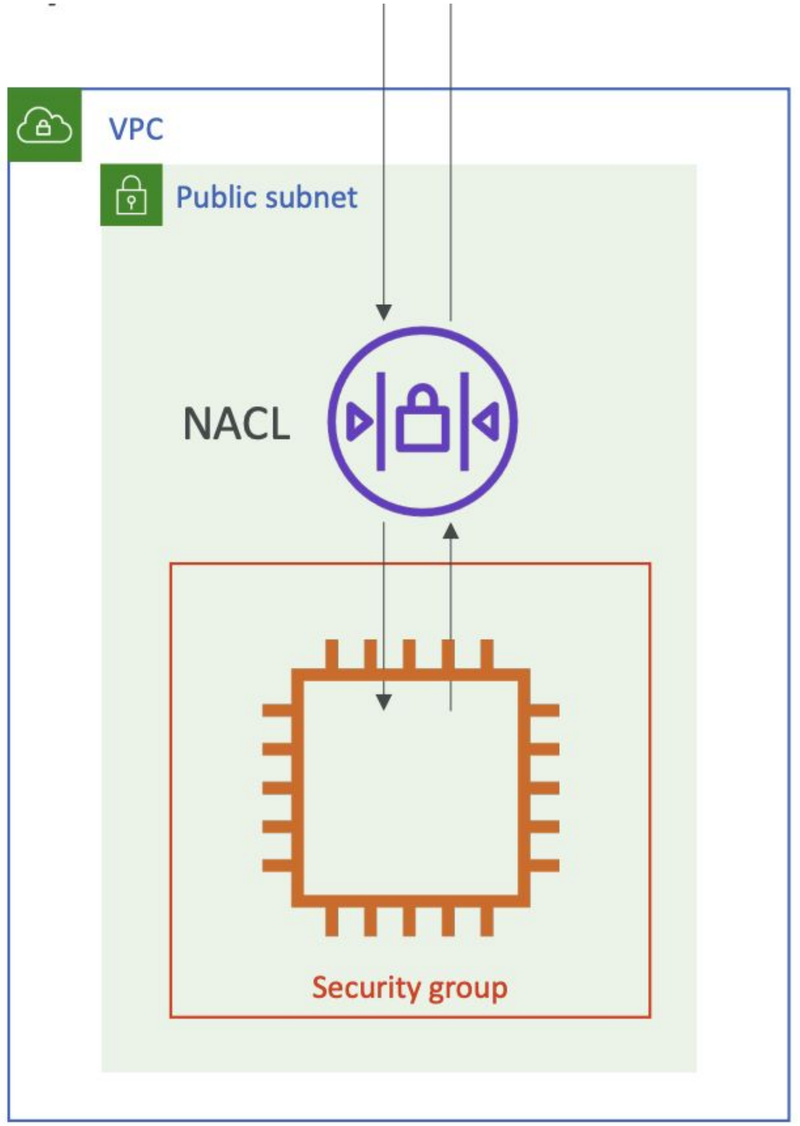


ACADEMIA CONSULTEC

Virtual Private Cloud
NACL & Grupos de Seguridad

- NACL (ACL de red)
  - Un cortafuegos que controla el tráfico desde y hacia la subred
  - Puede tener reglas PERMITIR y DENEGAR
  - Están conectados a nivel de subred
- Grupos de seguridad
  - Un cortafuegos que controla el tráfico hacia y desde una instancia ENI/EC2
  - Solo puede tener reglas PERMITIR
  - Las reglas incluyen direcciones IP y otros grupos de seguridad

Las reglas solo incluyen direcciones IP



ACADEMIA CONSULTEC

Virtual Private Cloud

Comparativa entre NACL & SGs

Security Group	Network ACL
Operates at the instance level	Operates at the subnet level
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 (therefore, you don't have to rely on users to specify the security group)

Virtual Private Cloud

VPC Flows Logs

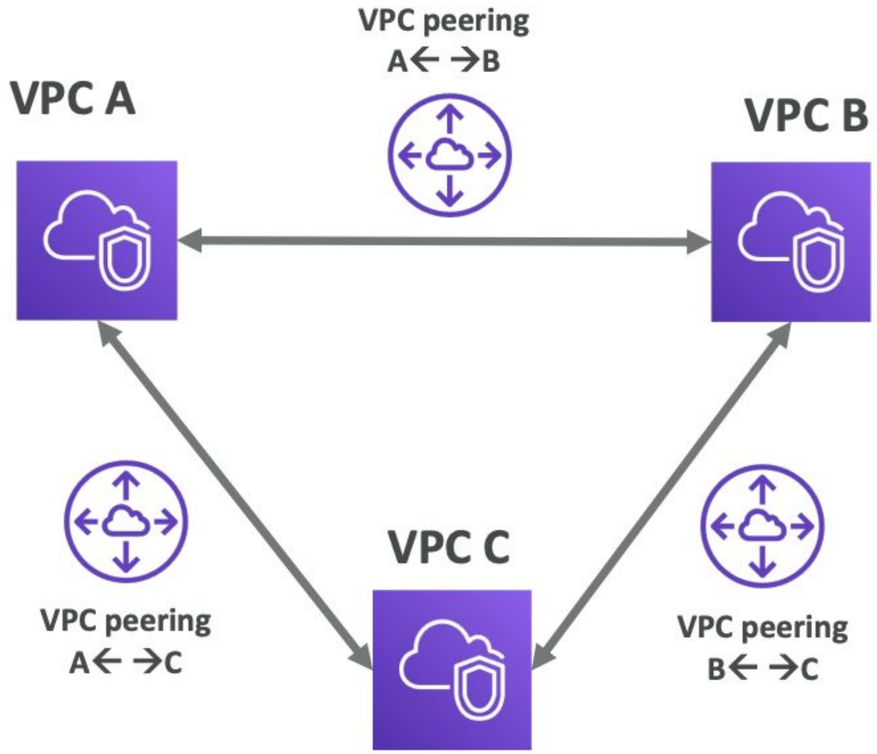
- Captura información sobre el tráfico IP que ingresa a sus interfaces:
  - Registros de flujo de VPC
  - Registros de flujo de subred
  - Registros de flujo de la interfaz de red elástica

- Ayuda a monitorear y solucionar problemas de conectividad. Ejemplo:
  - Subredes a internet
  - Subredes en subredes
  - Internet a subredes
- También captura información de red de las interfaces administradas por AWS: Elastic Load Balancers, ElastiCache, RDS, Aurora, etc.
- Los Logs de flujo de VPC pueden ir a S3/CloudWatch Logs

ACADEMIA CONSULTEC

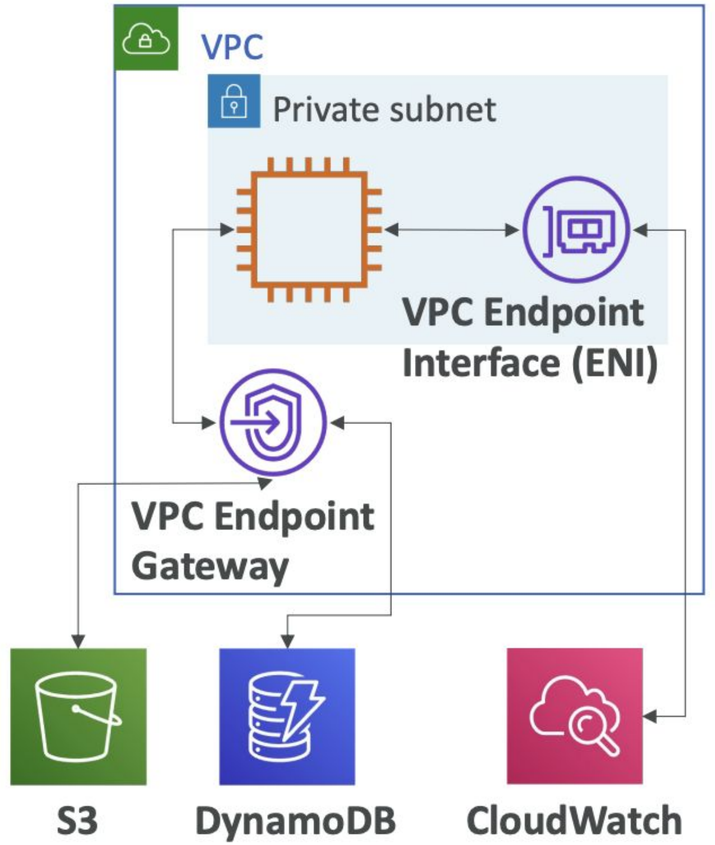
Virtual Private Cloud
VPC Peering

- Conecta dos VPC, de forma privada utilizando la red de AWS
- se comporta como si estuvieran en la misma red
- No debe tener CIDR superpuesto (rango de direcciones IP)*
- La interconexión de VPC no es transitiva (debe establecerse para cada VPC que necesite comunicarse entre sí)



Virtual Private Cloud
VPC Endpoints

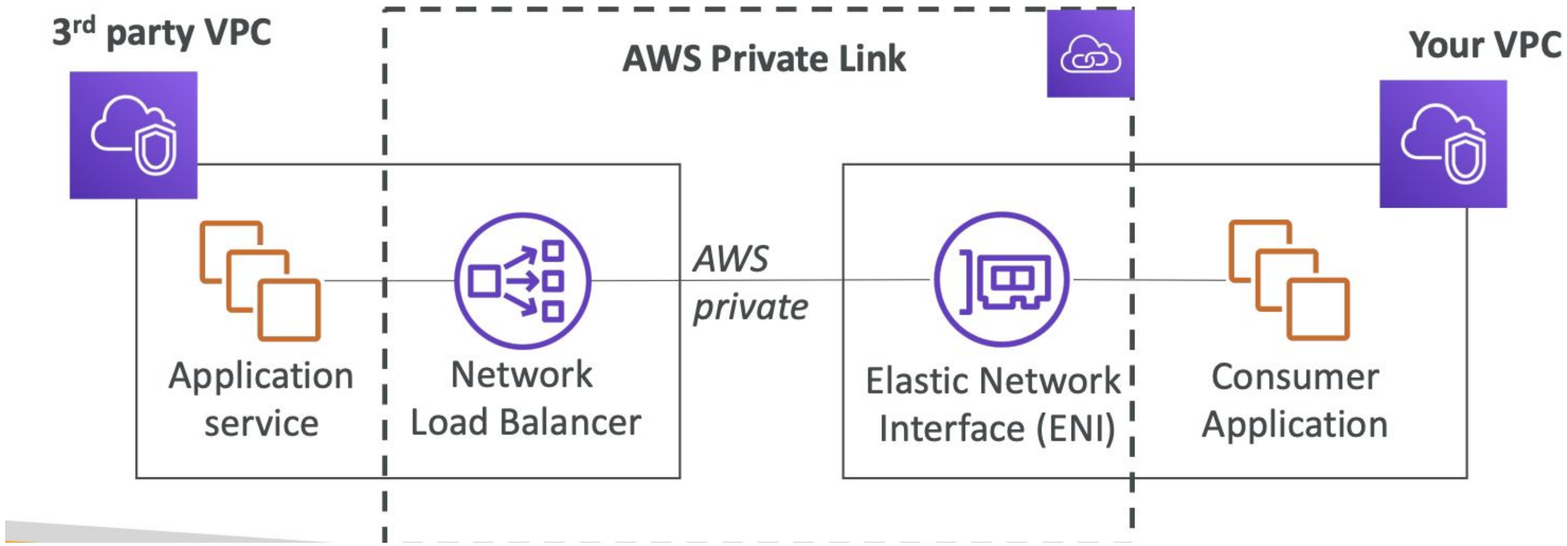
- Los puntos de enlace le permiten conectarse a los servicios de AWS mediante una red privada en lugar de la red www pública
- Esto le brinda mayor seguridad y menor latencia para acceder a los servicios de AWS
- VPC Endpoint GW: S3 y DynamoDB
- VPC Endpoint Interface: el resto



ACADEMIA CONSULTEC

Virtual Private Cloud
Private Link (VPC Endpoint Service)

- La forma más segura y escalable de exponer un servicio a miles de VPC
- No requiere interconexión de VPC, gateway de Internet, NAT, tablas de rutas...
- Requiere un balanceador de carga de red (Service VPC) y ENI (Customer VPC)



ACADEMIA CONSULTEC

Virtual Private Cloud

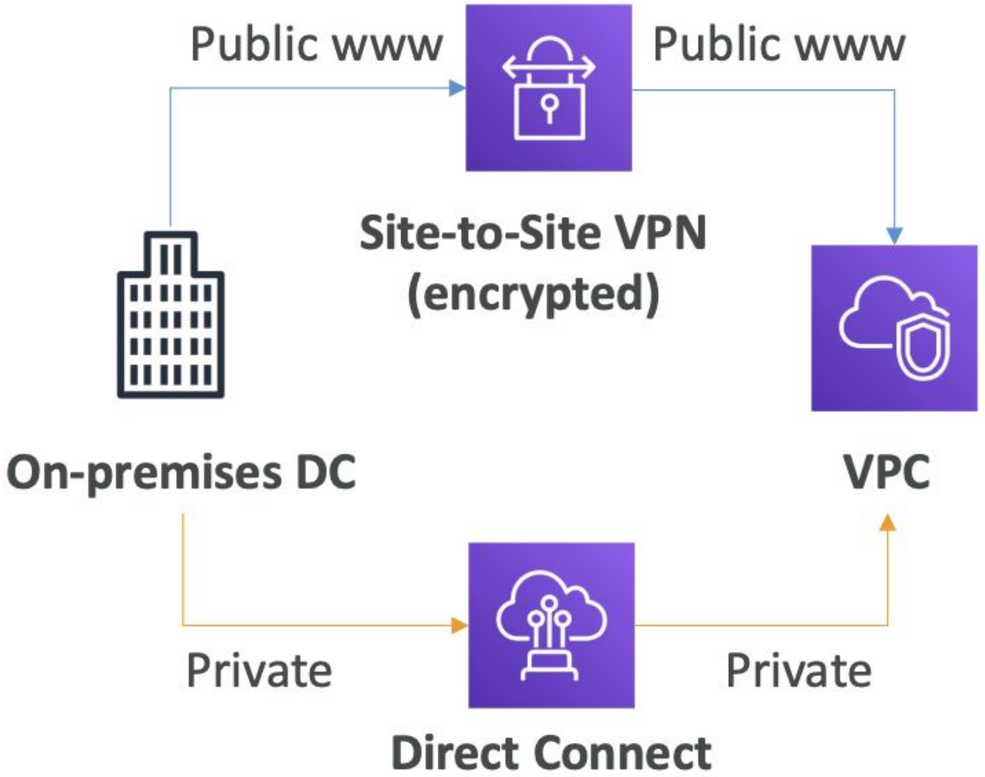
VPN Site to Site & Direct Connect

Site to Site VPN

- Conecta una VPN local a AWS
- La conexión se cifra automáticamente.
- Va a través de la Internet pública

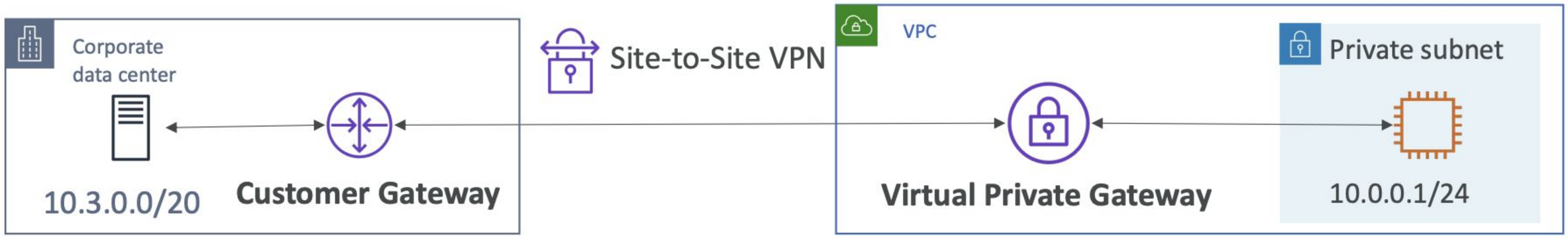
Direct Connect (DX)

- Establezca una conexión física entre las instalaciones y AWS
- La conexión es privada, segura y rápida.
- Pasa por una red privada
- Toma al menos un mes para establecer



Virtual Private Cloud
VPN Site to Site

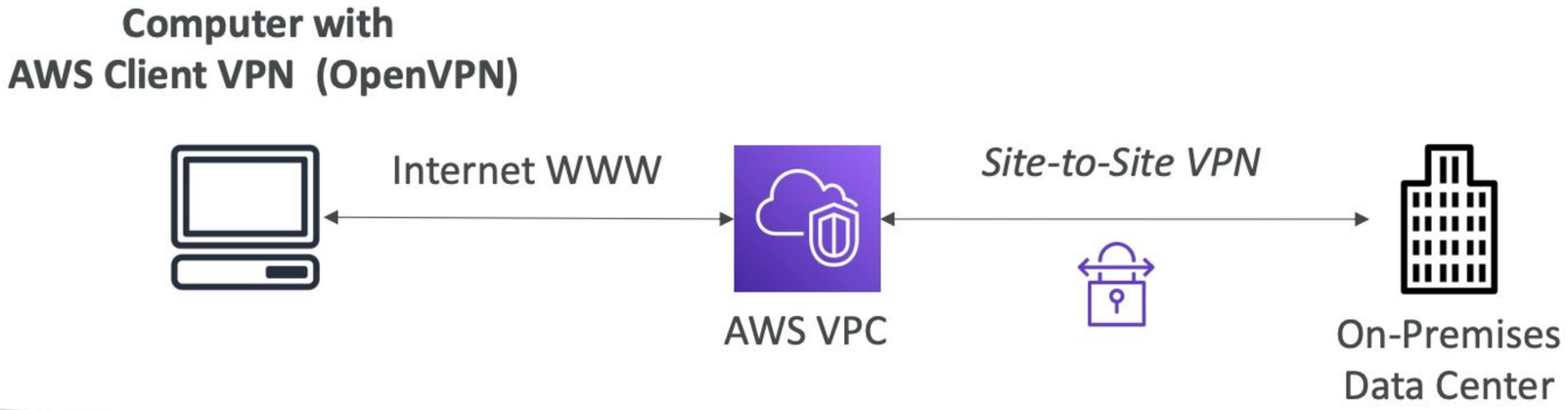
- On-Premises: debemos usar una puerta de enlace de cliente (CGW)
- AWS: debemos usar una puerta de enlace privada virtual (VGW)



ACADEMIA CONSULTEC

Virtual Private Cloud
Client VPN

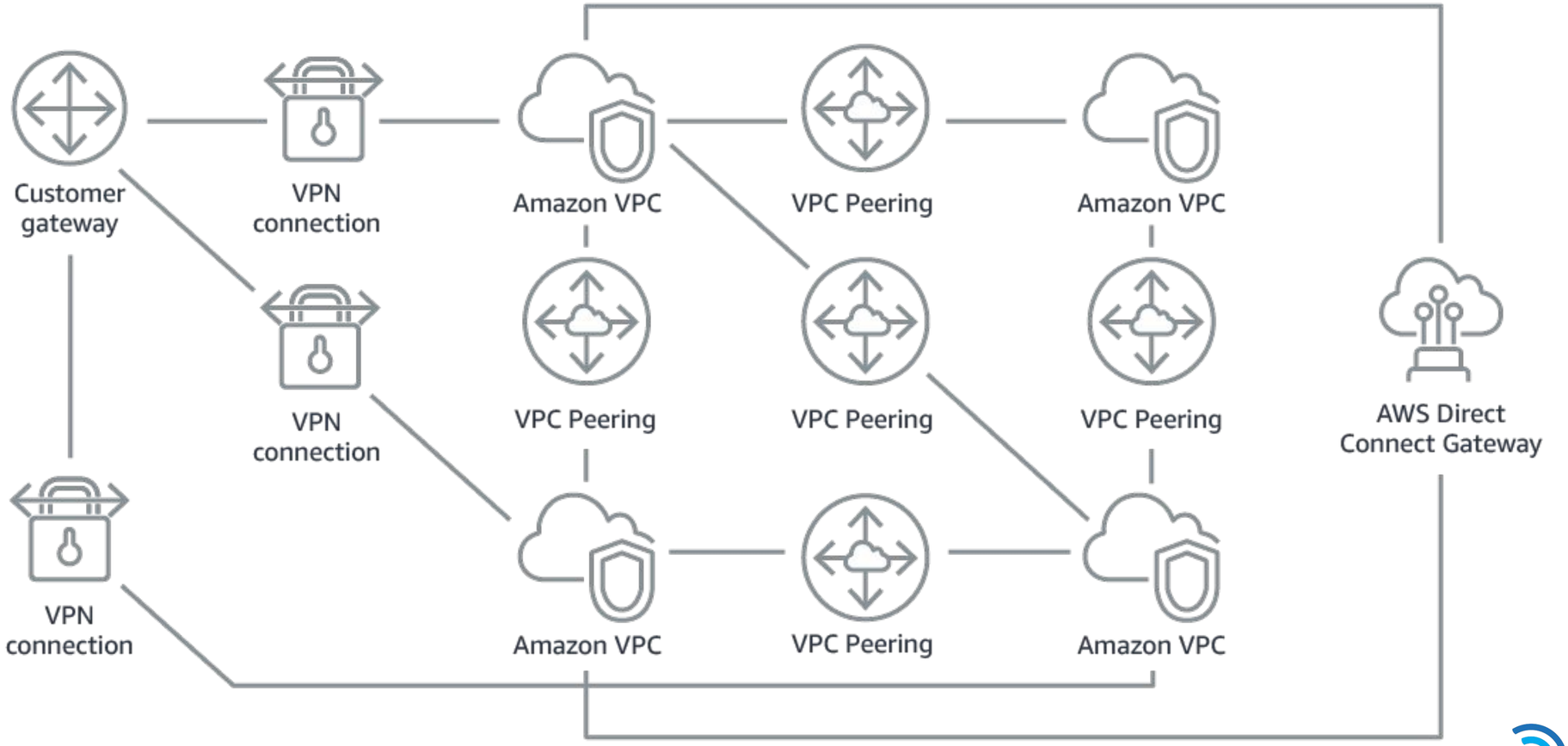
- Conéctese desde su computadora usando OpenVPN a su red privada en AWS y en las instalaciones
- Permite conectarse a sus instancias EC2 a través de una IP privada (como si estuviera en la red privada de VPC)
- Pasa por Internet pública



ACADEMIA CONSULTEC

Virtual Private Cloud

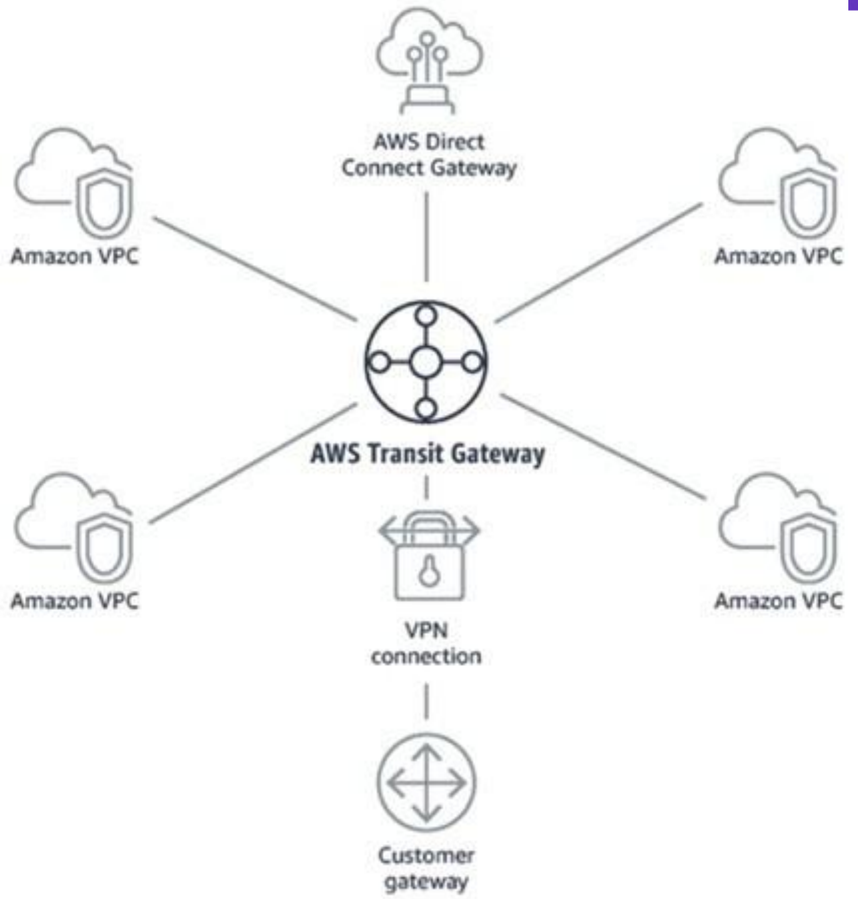
Topologías Complejas



ACADEMIA CONSULTEC

Virtual Private Cloud
Transit Gateway

- Para tener intercambio de tráfico transitivo entre miles de VPC y conexión de hub-and-spoke (estrella) en las instalaciones
- Una única puerta de enlace para proporcionar esta funcionalidad
- Funciona con Direct Connect



ACADEMIA CONSULTEC

Virtual Private Cloud

Resumen de Tema

- VPC: nube privada virtual
- Subredes: vinculadas a una AZ, partición de red de la VPC
- Internet Gateway: en el nivel de VPC, proporciona acceso a Internet
- NAT Gateway/Instancias: brinda acceso a Internet a subredes privadas
- NACL: reglas de subred sin estado para entrada y salida
- Grupos de seguridad: con estado, operan a nivel de instancia EC2 o ENI
- VPC Peering: conecte dos VPC con rangos de IP no superpuestos, no transitivos

Virtual Private Cloud

Resumen de Tema

- VPC Endpoints: proporcione acceso privado a los servicios de AWS dentro de la VPC
- PrivateLink: conexión privada a un servicio en una VPC de terceros
- VPC Flows Logs: registros de tráfico de red
- VPN de sitio a sitio: VPN a través de Internet pública entre DC local y AWS
- Client VPN: conexión OpenVPN desde su computadora a su VPC
- Direct Connect DX conexión privada directa a AWS
- Transit Gateway: conecte miles de VPC y redes locales juntas

ACADEMIA CONSULTEC

Contacto

achacon@consultec-ti.com

info@consultec-ti.com

@consulteclatam

@consultec-ti

consultec-ti.com

Gracias

¡Nos vemos pronto!