

Redes, entrega de contenido y protección web.

Diseña una red privada, conéctala de forma segura y protege el tráfico de tu tráfico de tu aplicación.

Amazon VPC · Route 53 · CloudFront · AWS WAF

Lo que vamos a cubrir, y cuánto tiempo le dedicamos.

01	Antes de empezar Fundamentos de redes: direcciones IP, CIDR, NAT y puertos	10 min
02	Tema 1 · Amazon VPC y conectividad Subredes, ruteo, NAT, Security Groups, NACLs, VPN, Direct Connect, Peering y Transit Gateway	45 min
—	Descanso Estirarse, café y preguntas	10 min
03	Tema 2 · DNS, CDN y seguridad web Route 53, CloudFront y AWS WAF	35 min
04	Cierre y preguntas Resumen, tarea (los dos laboratorios) y Q&A	15 min

Hoy vamos a diseñar, conectar y proteger.



01 · DISEÑAR

Una red privada en AWS AWS

Crear una VPC con subredes públicas y privadas, tablas de ruteo y reglas de seguridad.



02 · CONECTAR

Al exterior, de forma segura

Dar salida a internet y unirla a tu oficina u oficina u otras redes con VPN, Direct Connect, Peering y Transit Gateway.



03 · PROTEGER

El tráfico web de todo el el mundo

Resolver nombres con Route 53, acelerar la entrega con CloudFront y filtrar ataques con AWS WAF.

ANTES DE EMPEZAR

00

Lo básico de las redes.

Cinco ideas que vamos a usar todo el día. No se supone ningún conocimiento previo.
previo.

Una red es un grupo de dispositivos que pueden hablarse.

DISPOSITIVOS

Computadoras, celulares y servidores: todo lo que envía o recibe datos.

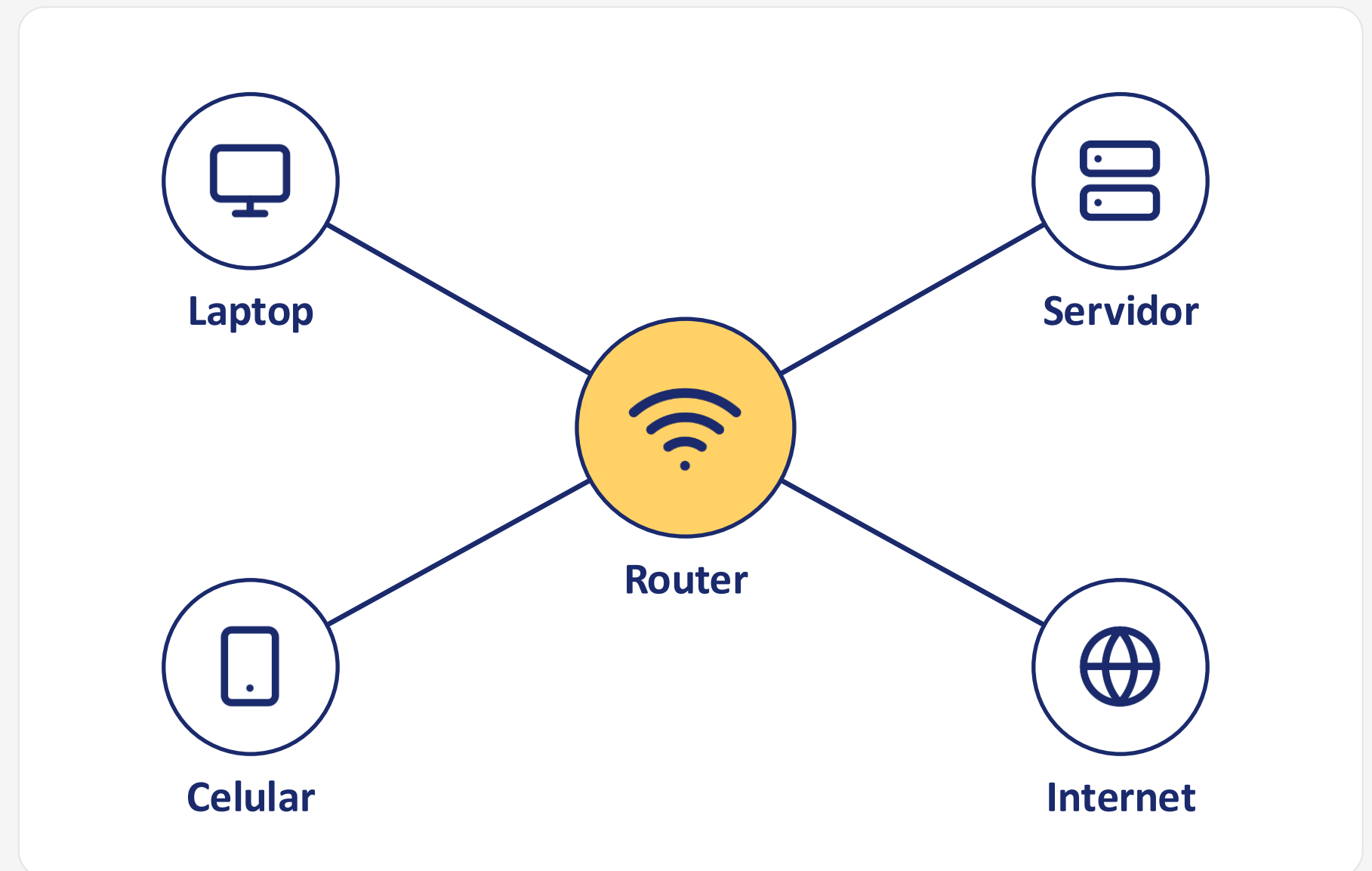
CONEXIONES

Cables, wifi o fibra óptica que los unen entre sí.

REGLAS

Los protocolos: acuerdos que definen cómo se entienden (por ejemplo, HTTP).

La nube no cambia esto: AWS te da la red ya construida, como software.



Cada dispositivo necesita una dirección: la dirección IP. dirección IP.

10.0.1.25

Cuatro números entre 0 y 255 (IPv4)

Como la dirección de tu casa: sin ella, el correo no llega.

RANGOS PRIVADOS RESERVADOS: 10.0.0.0/8 · 172.16.0.0/12 · 192.168.0.0/16

IP PÚBLICA

Visible desde todo internet

Cualquiera en el mundo puede intentar llegar a ella.

203.0.113.10

IP PRIVADA

Solo existe dentro de una red

Desde afuera nadie puede llegar a ella directamente.

10.0.1.25

Un rango de direcciones se escribe con CIDR.

10.0.0.0/16



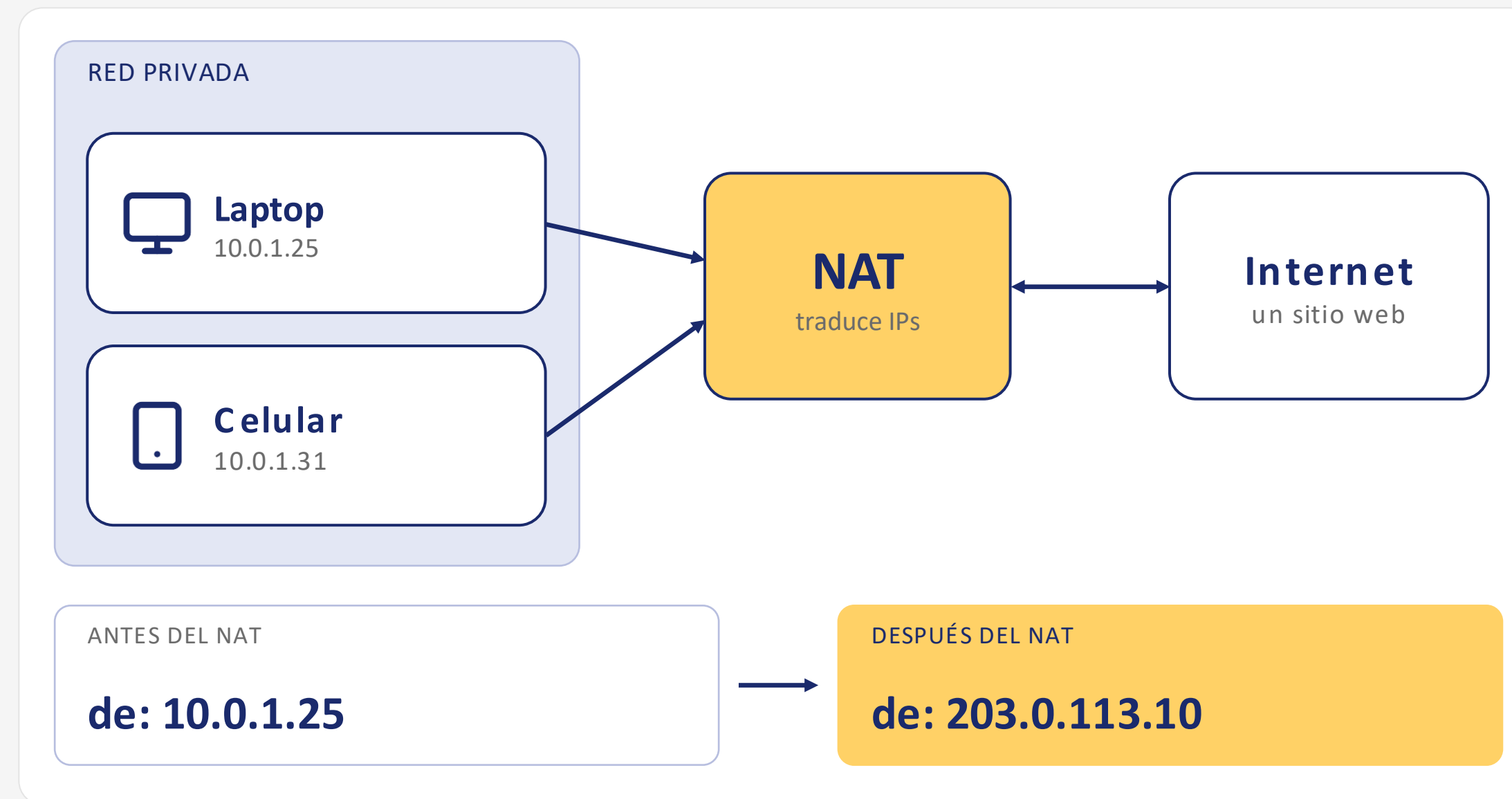
$2^{16} = 65,536$ direcciones

Más grande el número después de la diagonal, más pequeña la red.

CIDR	DIRECCIONES	USO TÍPICO
/16	65,536	VPC completa
/20	4,096	Subred grande
/24	256	Subred típica
/28	16	Subred mínima

En AWS, una VPC puede ir de /16 a /28.

NAT: cómo una red privada comparte una sola IP pública.



- 1 Tus dispositivos usan IP privadas, que que no existen en internet.
- 2 Al salir, el NAT cambia la IP privada privada por su IP pública.
- 3 La respuesta vuelve al NAT y llega a llega a quien preguntó. Nadie de afuera puede iniciar la conversación. conversación.

Es lo que hace el router de tu casa: muchos muchos dispositivos, una sola IP pública. pública.

La IP encuentra el dispositivo. El puerto encuentra el servicio.

EL SERVIDOR

203.0.113.10

IP: la dirección del edificio

:443

Puerto: el número de oficina

HTTPS

PUERTO	PROTOCOLO	PARA QUÉ SIRVE
80	HTTP	Páginas web sin cifrar
443	HTTPS	Páginas web cifradas
22	SSH	Administrar servidores Linux
3389	RDP	Escritorio remoto de Windows
53	DNS	Traducir nombres a direcciones IP
5432	PostgreSQL	Conectarse a una base de datos

01

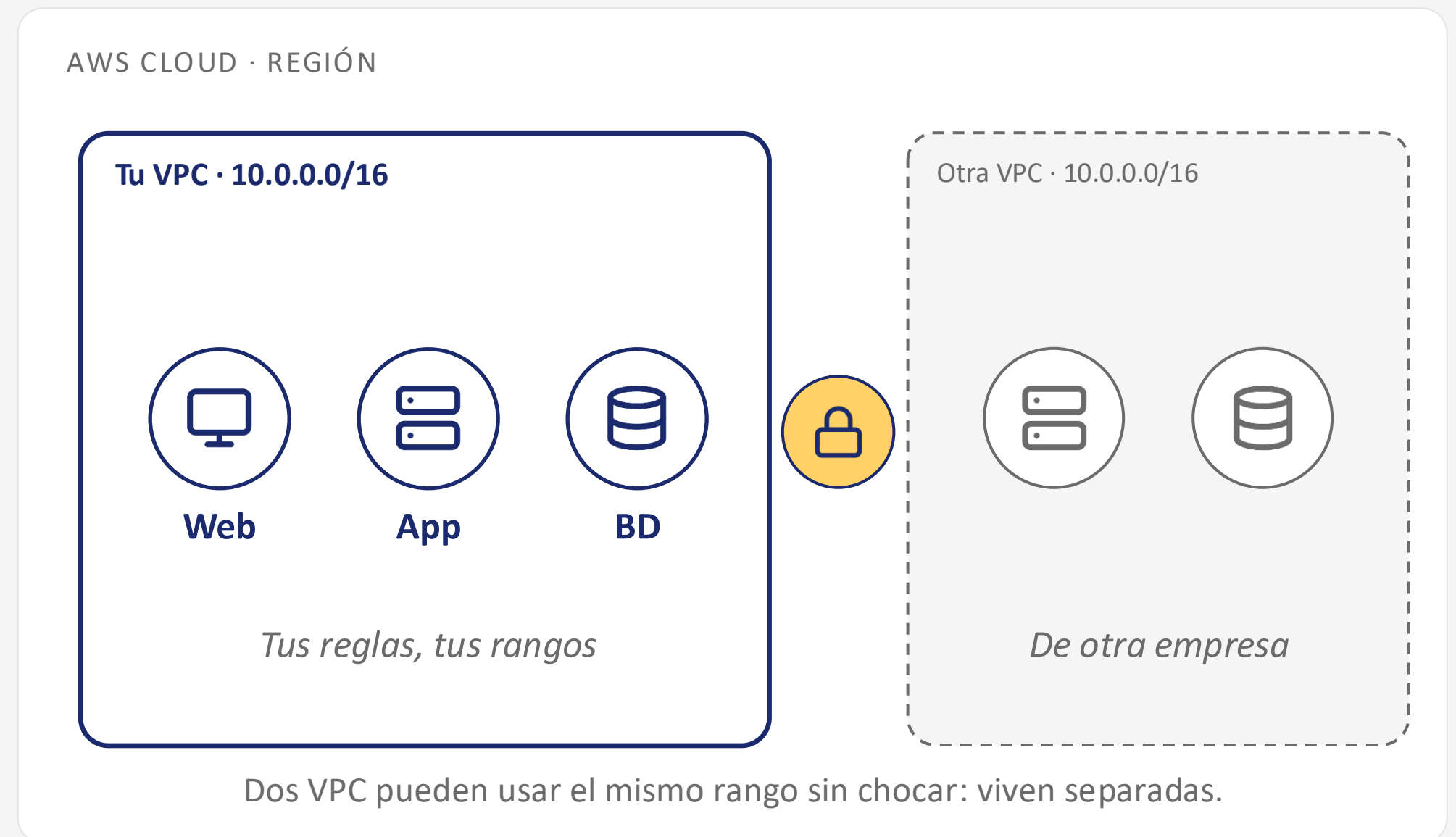
Redes virtuales: Amazon VPC y conectividad. conectividad.

Creación de una red privada y aislada dentro de la nube de AWS, y sus opciones de conexión de conexión con el exterior u otras redes.

Una VPC es tu propia red privada dentro de AWS.

VPC = VIRTUAL PRIVATE CLOUD

-  Tú eliges el rango de direcciones IP.
IP.
-  Tú decides qué se comunica con qué.
qué.
-  Está aislada de las demás VPC por defecto.



Nuestra analogía de hoy: un edificio de oficinas.



VPC

El edificio completo, con su perímetro



Tabla de ruteo

Los letreros que indican a dónde ir



Subred pública

El lobby: tiene puerta a la calle



NAT Gateway

Recepción: llama por ti, no deja pasar a nadie



Subred privada

Las oficinas internas, sin puerta a la calle



NACL

El guardia de cada piso



Internet Gateway

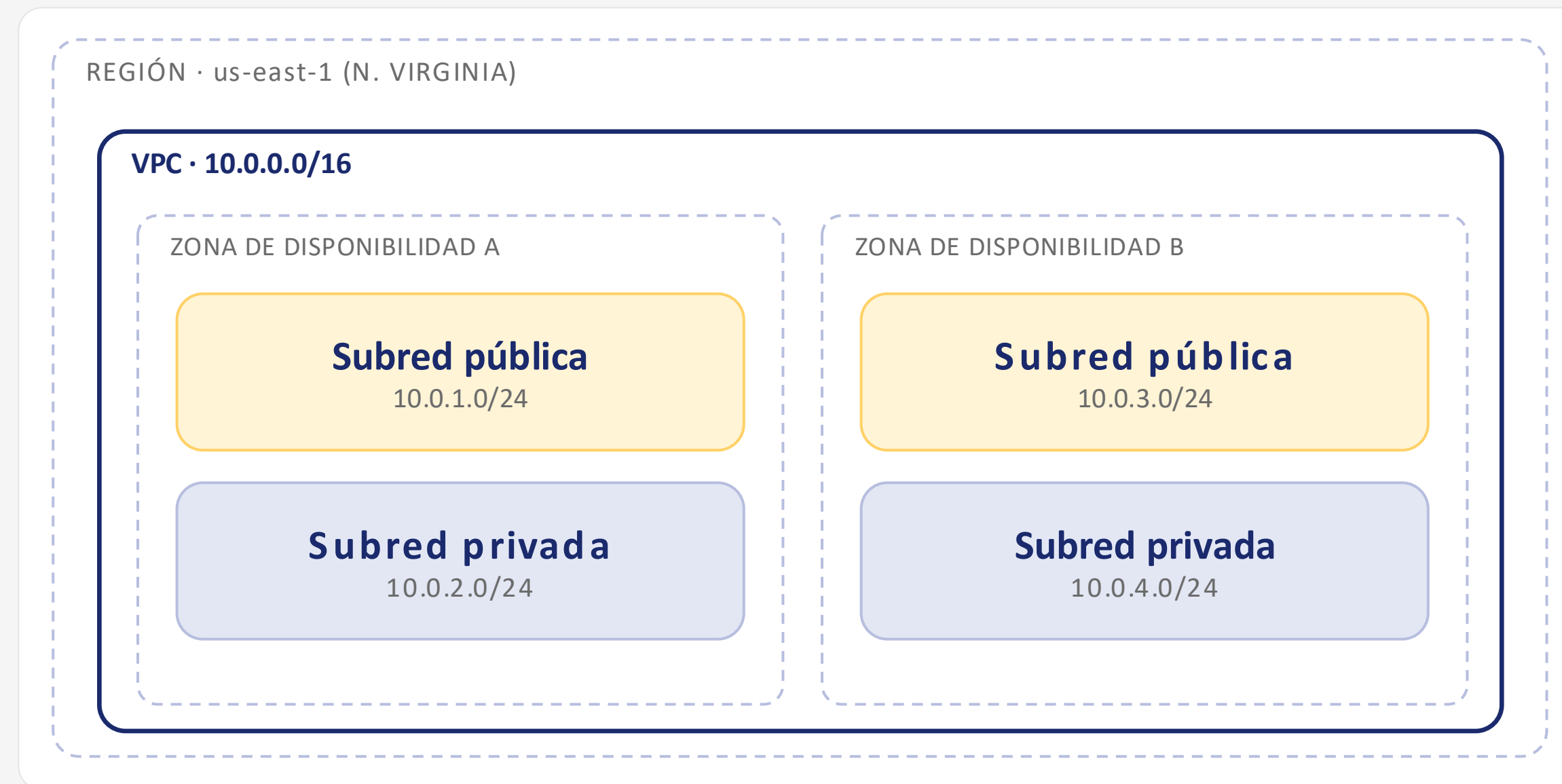
La puerta principal del edificio



Security Group

La cerradura de cada oficina

La VPC abarca una Región. Cada subred, una Zona de Disponibilidad.



¿Por qué dos zonas?

Cada zona es uno o más centros de datos independientes. Si una falla, falla, la otra sigue funcionando.

EJEMPLO LOCAL

AWS tiene una Región en México: México (Centro), mx-central-1.

Subredes: cada parte de la red con su propósito.



SUBRED PÚBLICA

**Para lo que debe ser visible desde internet.
internet.**

- ✓ Servidores web y balanceadores de carga
- ✓ NAT Gateway
- ✓ Tiene una ruta hacia el Internet Gateway

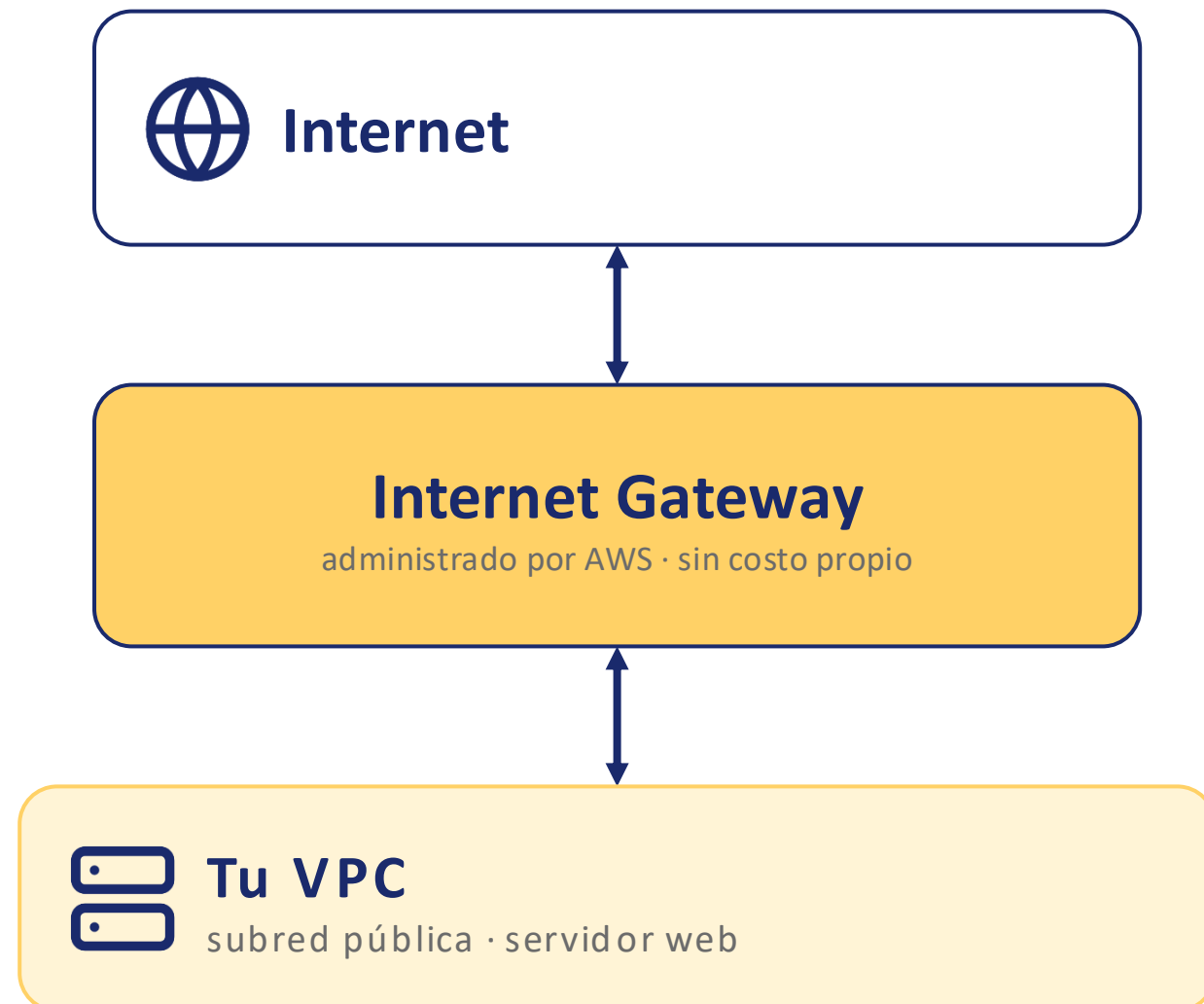


SUBRED PRIVADA

Para lo que debe quedar protegido.

- ✓ Bases de datos
- ✓ Servidores de aplicación
- ✓ No tiene ruta directa hacia ni desde internet

El Internet Gateway es la puerta de tu VPC hacia internet.



Servidor público: cuatro requisitos

- 1 Un Internet Gateway asociado a la VPC.
- 2 Una ruta 0.0.0.0/0 → IGW en la tabla de ruteo de su de su subred.
- 3 Una IP pública (o una Elastic IP) en el servidor.
- 4 Reglas de NACL y Security Group que permitan el el tráfico.

La tabla de ruteo es el GPS de tu red.

TABLA DE RUTEO · SUBRED PÚBLICA	
DESTINO	SALIDA
10.0.0.0/16	local
0.0.0.0/0	igw-0a1b2c3d

TABLA DE RUTEO · SUBRED PRIVADA	
DESTINO	SALIDA
10.0.0.0/16	local
—	sin ruta a internet

LOCAL

Siempre existe: todo lo que está dentro de dentro de la VPC puede hablarse.

0.0.0.0/0

Significa «cualquier otro destino». Es la la ruta hacia internet.

LA MÁS ESPECÍFICA GANA

Si varias rutas coinciden, se usa la más más específica.

LA IDEA CLAVE

**Lo que hace pública a una subred no es
no es su nombre. Es su **tabla de ruteo.**
ruteo.**

Pública significa que hay una ruta hacia un Internet Gateway. Privada, que no la hay.
no la hay. Eso es todo.

El NAT Gateway deja salir a lo privado sin dejar entrar a entrar a nadie.



DÓNDE VIVE

En una subred pública, con una Elastic IP.
Elastic IP.

CÓMO SE USA

La tabla de ruteo privada apunta 0.0.0.0/0
0.0.0.0/0 → NAT Gateway.

OJO CON EL COSTO

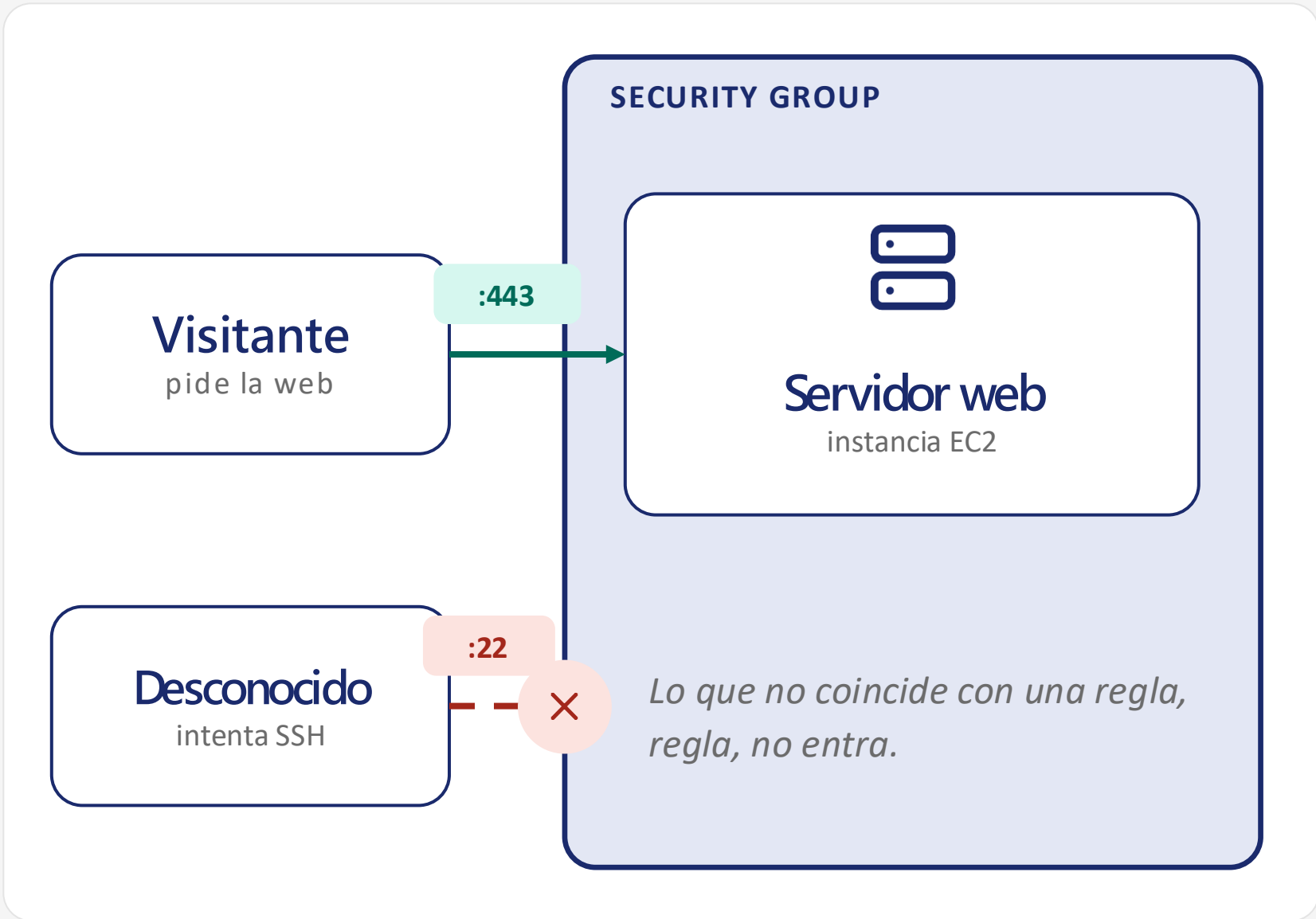
Cobra por hora y por GB procesado.
Bórralo al terminar tus labs.

Internet Gateway y NAT Gateway no compiten: trabajan juntos.

	INTERNET GATEWAY	NAT GATEWAY
Para qué sirve	Puerta de entrada y salida entre la VPC e internet	Deja salir a lo privado sin dejar entrar a nadie
Quién lo usa	Servidores públicos, con IP pública	Servidores privados, sin IP pública
Dónde vive	Se asocia a la VPC	En una subred pública, con una Elastic IP
Ruta en la tabla	0.0.0.0/0 → igw-...	0.0.0.0/0 → nat-...
Costo	Sin costo propio	Por hora y por GB procesado
Depende de	Nada más	Del Internet Gateway: sin él, no llega a internet

El NAT Gateway no reemplaza al Internet Gateway: para llegar a internet, lo usa.

Security Group: la cerradura de cada servidor.



REGLAS DE ENTRADA · EJEMPLO

TIPO	PUERTO	ORIGEN
HTTPS	443	0.0.0.0/0
SSH	22	203.0.113.25/32
SOLO PERMITE	No hay reglas de denegar: lo que no está permitido, se bloquea.	
CON MEMORIA	Si la petición entró, la respuesta sale sola. No hace falta regla de salida.	
POR DEFECTO	Uno nuevo bloquea toda la entrada y permite permite toda la salida.	

Dos capas de seguridad: una en la subred, otra en el servidor.

	NACL · EL GUARDIA DEL PISO	SECURITY GROUP · LA CERRADURA DE LA OFICINA
Dónde actúa	En la subred: todo lo que entra o sale	En cada servidor (su interfaz de red)
Memoria	Stateless: revisa la ida y la vuelta por separado	Stateful: si la petición entró, la respuesta sale sola sola
Tipos de regla	Permitir y denegar	Solo permitir
Cómo evalúa	En orden numérico; gana la primera que coincide	Evalúa todas las reglas a la vez
Por defecto	La NACL predeterminada permite todo	Un Security Group nuevo bloquea todo lo entrante entrante

Las NACL no tienen memoria: hay que permitir la ida y la ida y la vuelta.

REGLAS DE ENTRADA · NACL DE EJEMPLO

REGLA	TIPO	PUERTOS	ORIGEN	ACCIÓN
90	Todo	Todo	203.0.113.0/24	DENEGAR
100	HTTPS	443	0.0.0.0/0	PERMITIR
110	HTTP	80	0.0.0.0/0	PERMITIR
120	TCP	1024–65535	0.0.0.0/0	PERMITIR
*	Todo	Todo	0.0.0.0/0	DENEGAR

1 · EL ORDEN

Se evalúan de menor a mayor. La primera primera que coincide gana.

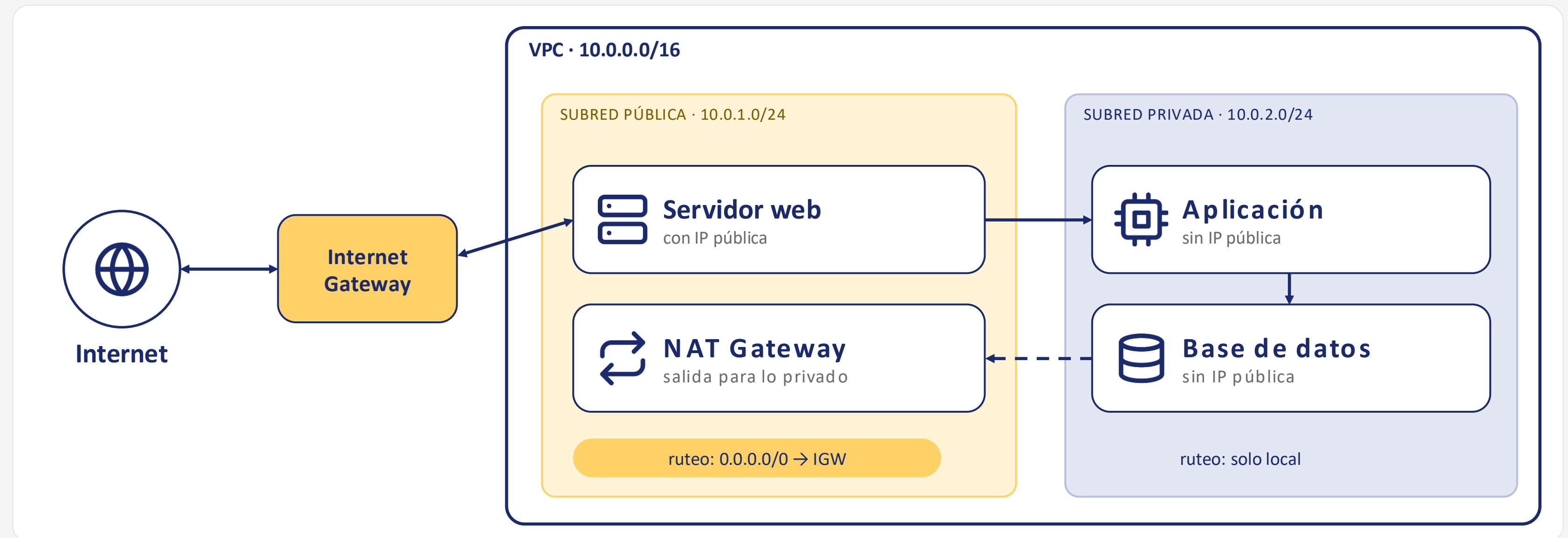
2 · SIN MEMORIA

Las respuestas también necesitan permiso: permiso: por eso abrimos 1024–65535 65535 (puertos temporales).

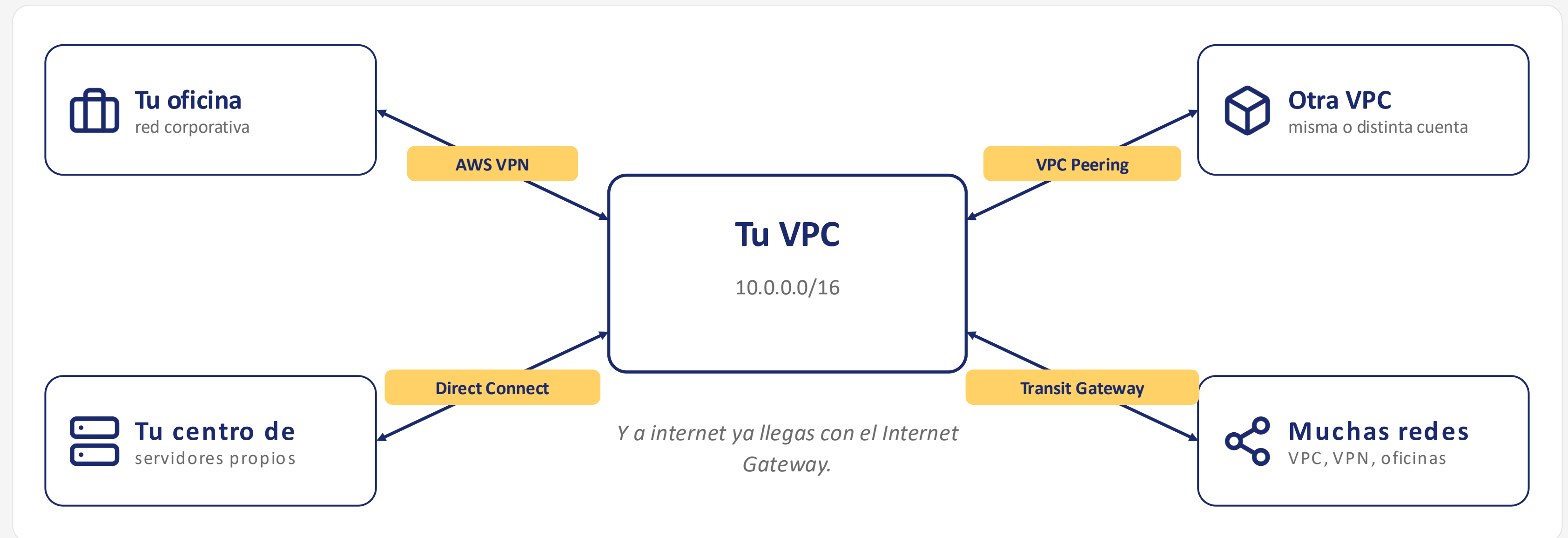
3 · LA REGLA *

Cierra la puerta a todo lo que no se permitió arriba.

Todo junto: una VPC con una subred pública y una privada.

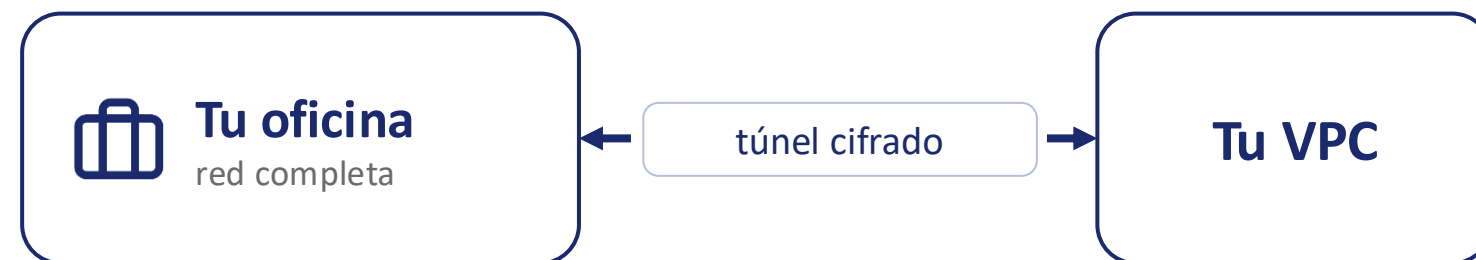


Cinco formas de conectar tu VPC con el mundo.



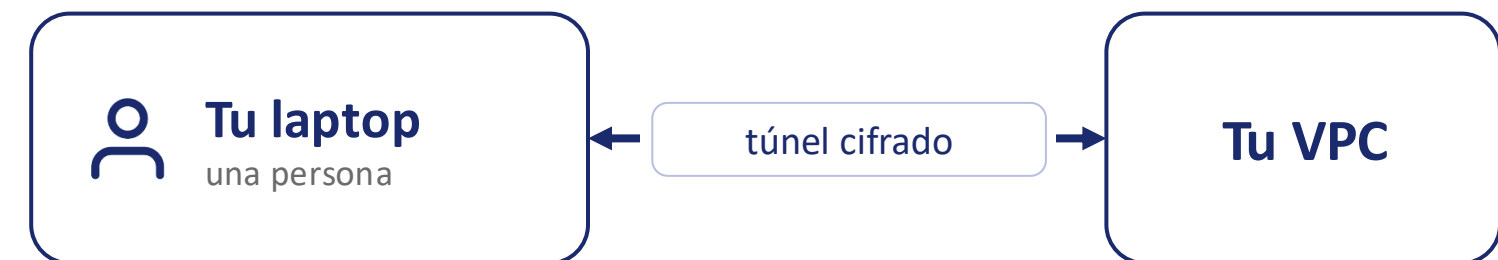
AWS VPN: un túnel cifrado por internet.

SITE-TO-SITE VPN



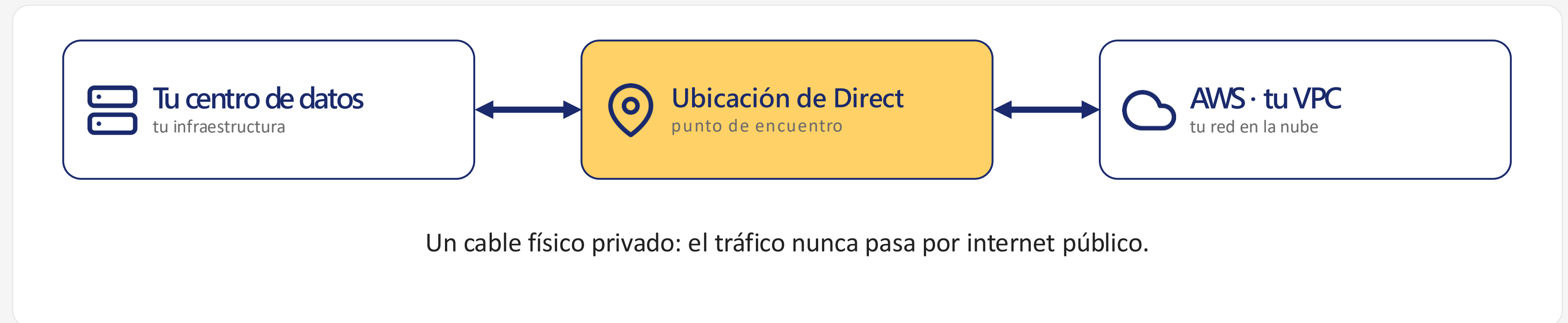
- ✓ Conecta una red completa, como tu oficina, con tu VPC.
- ✓ El tráfico viaja cifrado por internet.
- ✓ Cada conexión trae 2 túneles, para tener redundancia.

CLIENT VPN



- ✓ Conecta a una persona, desde su laptop, con tu VPC.
- ✓ Se usa con un cliente compatible con OpenVPN.
- ✓ Ideal para trabajo remoto.

Direct Connect: un cable dedicado hacia AWS.



PRIVADA

El tráfico no viaja por el internet público.
público.

ESTABLE

Velocidad y latencia más predecibles que
que con una VPN. Conexiones dedicadas de
dedicadas de 1, 10 y 100 Gbps.

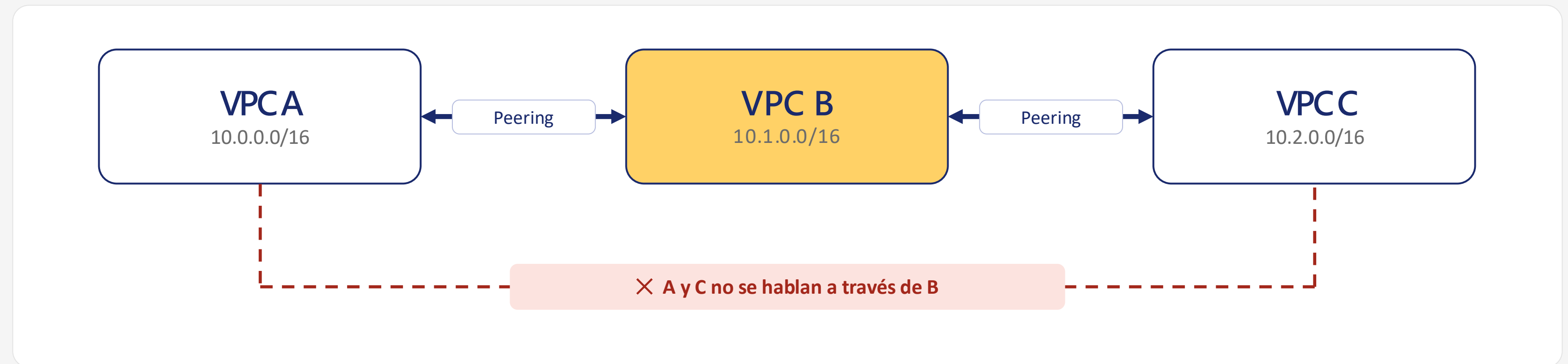
CON PLAZO

Hay que instalar un enlace físico: puede
puede tardar semanas y cuesta más.

VPN o Direct Connect: rapidez contra estabilidad.

	AWS VPN	DIRECT CONNECT
Camino	Por internet, cifrado	Enlace privado, sin internet público
Velocidad	Hasta 1.25 Gbps por túnel	Conexiones de 1, 10 o 100 Gbps
Latencia	Variable: depende de internet	Constante y predecible
Cifrado	Sí, incluido (IPsec)	No por defecto: se puede añadir una VPN encima
Plazo	Minutos	Semanas
Costo	Bajo	Mayor: puerto más datos transferidos
Ideal para	Empezar rápido o como respaldo	Mucho tráfico o latencia crítica

VPC Peering une dos VPC, pero no es transitivo.



UNO A UNO

Cada par de VPC necesita su propio peering.

NO TRANSITIVO

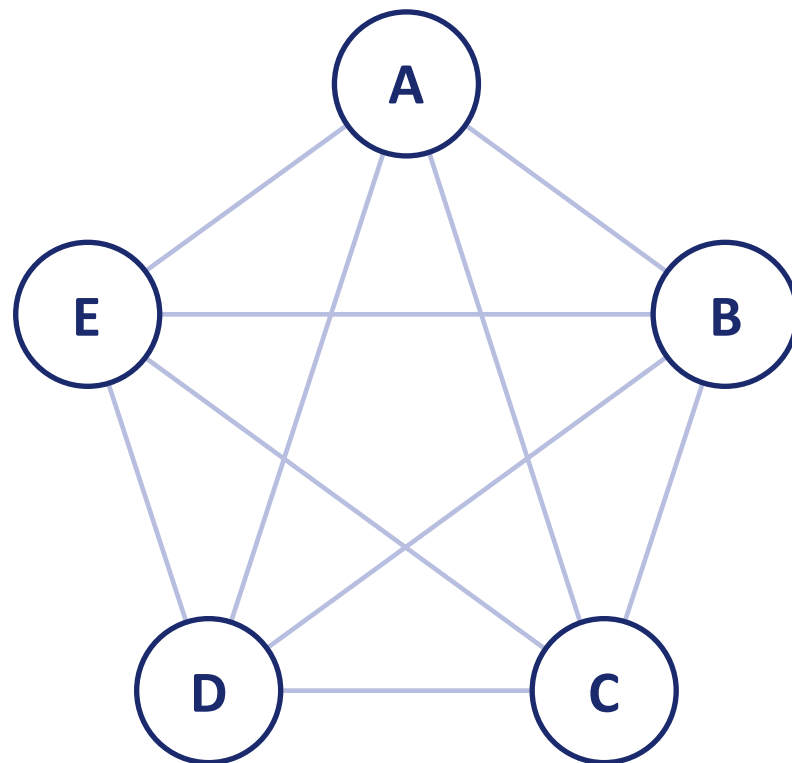
Que A hable con B y B con C no significa que A hable con C.

SIN TRASLAPES

Los rangos CIDR de las dos VPC no pueden coincidir.

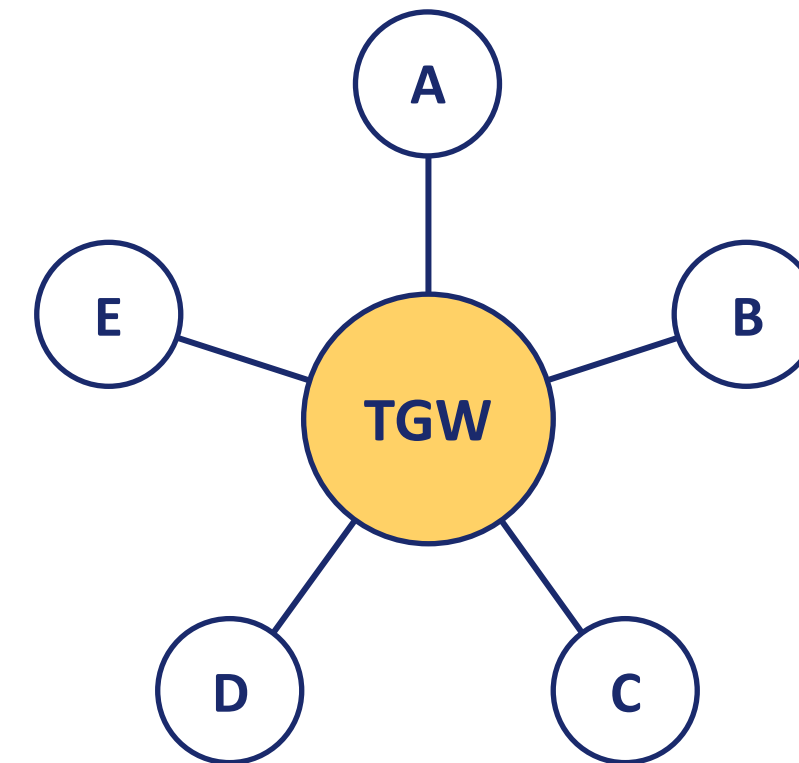
Transit Gateway es un centro de conexiones para muchas redes.

SIN TRANSIT GATEWAY



5 VPC = 10 conexiones. Con 10 VPC serían 45.

CON TRANSIT GATEWAY



Cada red se conecta una sola vez. También acepta VPN y Direct Connect.

¿Cuál uso? Depende de lo que quieras conectar.

Internet Gateway

Quiero que mis servidores públicos sean visibles desde internet.

AWS VPN

Quiero conectar mi oficina o a mis usuarios, rápido y sin instalar cables.

Direct Connect

Necesito un enlace privado, estable y de mucha capacidad.

VPC Peering

Quiero unir dos VPC de forma sencilla y directa.

Transit Gateway

Tengo muchas VPC y redes que conectar entre sí.

Lo que nos llevamos del Tema 1.

01

Una VPC es tu red privada en AWS; cada subred vive en una sola Zona de Disponibilidad. Disponibilidad.

02

Una subred es pública si tiene ruta a un Internet Gateway; el NAT Gateway deja salir a lo salir a lo privado.

03

La NACL protege la subred y no tiene memoria; el Security Group protege el servidor y sí la tiene.

04

Para conectar: VPN (rápido), Direct Connect (estable), Peering (dos VPC) y Transit Gateway Transit Gateway (muchas).

Tu tarea: construye una VPC y comprueba quién sale a internet.

- 1 En la consola abre VPC y elige «Crear VPC» → «VPC y más» (VPC and more).
- 2 Configura 1 zona de disponibilidad, 1 subred pública y 1 subred privada; privada; sin NAT Gateway.
- 3 Revisa el diagrama de recursos: VPC, subredes, Internet Gateway y tablas y tablas de ruteo.
- 4 Lanza una instancia EC2 en cada subred (con IP pública solo en la pública). la pública).
- 5 Conéctate a cada una y ejecuta: `curl https://checkip.amazonaws.com`
- 6 Compara: ¿cuál responde y cuál se queda esperando? Explica por qué.

AL TERMINAR DEBERÍAS VER

La pública responde con su IP pública.

La privada se queda esperando: no tiene ruta a un Internet Gateway.

TIP Y COSTOS

Para entrar a la privada usa EC2 Instance Connect Endpoint (no necesita IP pública). Al terminar, elimina las instancias y la VPC para no generar costos.

DESCANSO

10 min

Regresamos con el Tema 2.

Para pensar mientras tanto: si tu sitio vive en Virginia, ¿por qué se ve más lento desde Tokio?



02

DNS, CDN y seguridad web.

Optimización del tráfico mundial de la aplicación y defensa ante ataques maliciosos comunes.

Tres problemas, tres servicios.



01 · NOMBRES

**Nadie quiere aprenderse
54.239.28.85.**

Route 53

Convierte nombres como tuapp.com en direcciones IP.



02 · VELOCIDAD

**Cada 1,000 km suman unos 10
ms de ida y vuelta.**

CloudFront

Guarda copias de tu contenido cerca de tus usuarios.



03 · SEGURIDAD

**Cualquiera en internet puede
intentar atacarte.**

AWS WAF

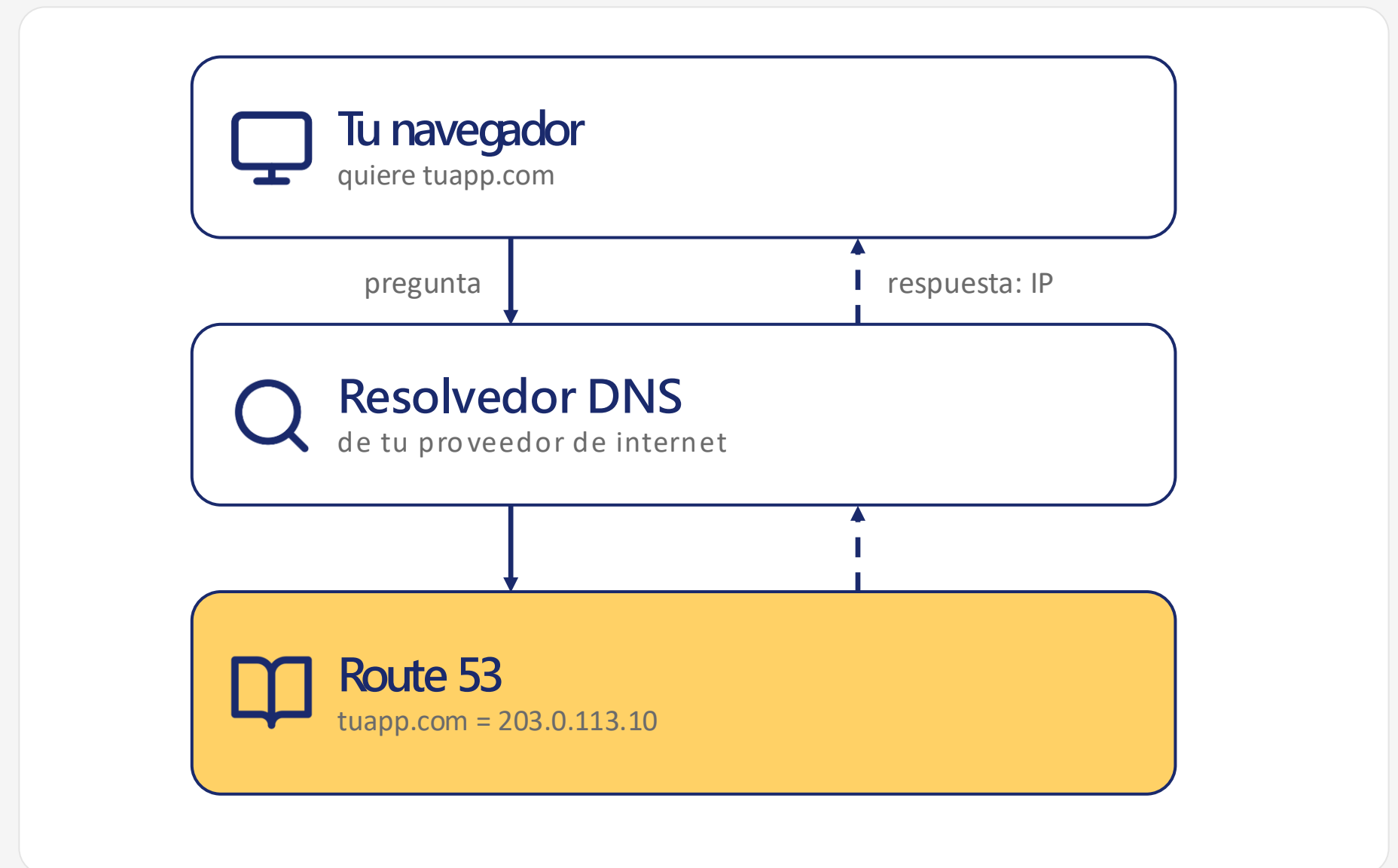
Filtra las peticiones maliciosas antes de que lleguen.

¿Qué pasa cuando escribes una dirección web?

1	Escribes tuapp.com en el navegador.	
2	El navegador pregunta: ¿cuál es la dirección IP de tuapp.com?	DNS · Route 53
3	Tu petición llega al punto de entrada más cercano.	CloudFront
4	Se revisa que la petición no sea maliciosa.	AWS WAF
5	Recibes la página, desde una copia guardada o desde el origen.	CloudFront · origen

El DNS es la agenda telefónica de internet.

- 1 Tu navegador pregunta: ¿cuál es la IP de tuapp.com?
- 2 Un resolvedor DNS (el de tu proveedor) busca la respuesta.
- 3 Pregunta hasta llegar al servidor que administra tu dominio: Route 53.
- 4 Regresa la IP, por ejemplo 203.0.113.10, y el navegador se conecta.



Route 53: el DNS de AWS, altamente disponible.



Registrar dominios

Compra y administra tu dominio, por ejemplo tuapp.com.



Resolver nombres

Responde «¿cuál es la IP?» con servidores repartidos por el



Enrutar el tráfico

Decide a dónde mandar a cada usuario y revisa la salud de tus servidores.

DISPONIBILIDAD

100%

SLA de disponibilidad del DNS de Route 53.

El nombre viene del puerto 53, el que usa el DNS.
DNS.

Los registros DNS son las entradas de la agenda.

TIPO	QUÉ HACE	EJEMPLO
A	Apunta un nombre a una dirección IPv4.	tuapp.com → 203.0.113.10
AAAA	Lo mismo, pero para direcciones IPv6.	tuapp.com → 2001:db8::1
CNAME	Apunta un nombre a otro nombre.	www.tuapp.com → tuapp.com
MX	Indica a dónde llega el correo del dominio.	tuapp.com → mail.tuapp.com
Alias	Solo en Route 53: apunta a un recurso de AWS, incluso en el dominio raíz.	tuapp.com → d111.cloudfront.net

Route 53 decide a dónde mandar a cada usuario.



Simple

Simple

Un nombre, un destino. Lo básico.



Ponderada

Weighted

Reparte por porcentajes: 90% a la versión versión actual, 10% a la nueva.



Por latencia

Latency

Manda al usuario a la Región que le responde más rápido.



De respaldo

Failover

Si el servidor principal falla, responde con con el de respaldo.



Geolocalización

Geolocation

Responde según el país del usuario: idioma o contenido local.

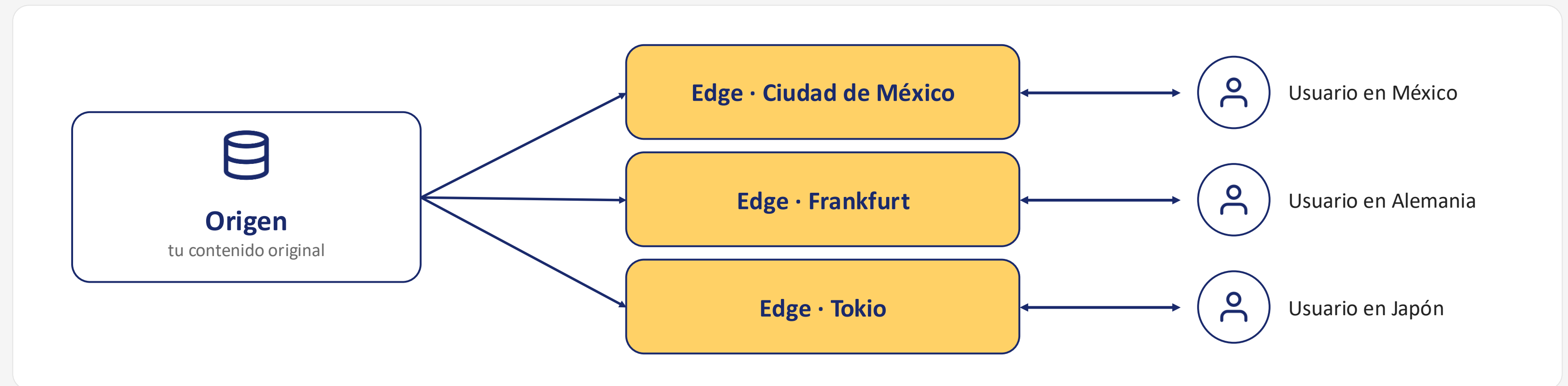


Multivalor

Multivalue

Devuelve varias IP sanas a la vez, con revisión de salud.

CloudFront acerca tu contenido a tus usuarios.



ORIGEN

Donde vive tu contenido original: un bucket de S3, un balanceador balanceador o tu servidor.

EDGE LOCATION

Centro de datos de AWS cerca de los usuarios, donde se guardan guardan copias temporales.

Una red global pensada para estar cerca de ti.

750+

puntos de presencia (edge
(edge locations))

100+

ciudades

50+

países

Fuente: página de características de Amazon CloudFront. Las cifras crecen con el tiempo.

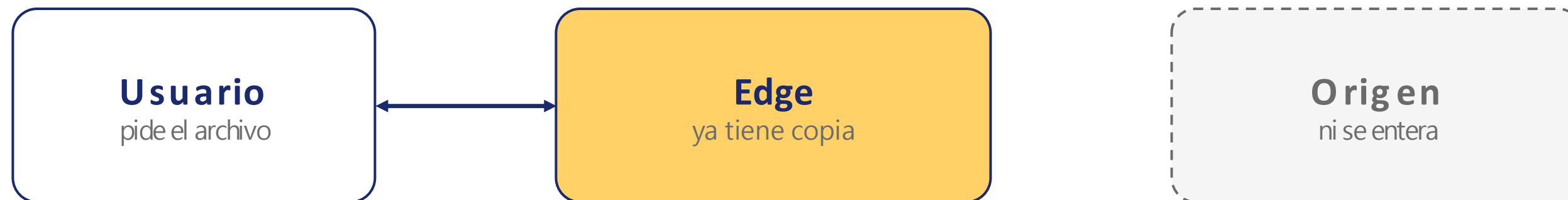
La primera vez viaja lejos. Las siguientes, no.

CACHE MISS · PRIMERA PETICIÓN



Más lento: el viaje llega hasta el origen.

CACHE HIT · SIGUIENTES PETICIONES



Rápido: responde el edge, edge, sin molestar al origen.

Las piezas de CloudFront que usarás en el laboratorio.



Origen

Origin

De dónde toma el contenido: S3, un balanceador o un servidor.



Distribución

Distribution

Tu configuración de CloudFront. Recibe una URL cloudfront.net.



Comportamientos

Behaviors

Reglas por ruta: qué se guarda en caché y caché y qué métodos se permiten.



Caché y TTL

Time to live

El TTL es cuánto vive una copia antes de volver a pedirla al origen.



HTTPS

Certificado

HTTPS con un certificado gratuito de AWS Certificate Manager.



OAC

Origin Access Control

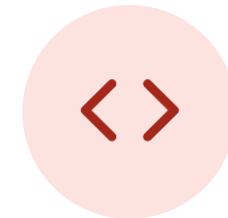
Mantiene privado el bucket de S3: solo CloudFront puede leerlo.

Las amenazas web más comunes.



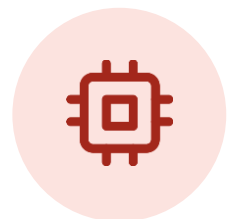
Inyección SQL

Alguien escribe comandos de base de datos en un formulario para robar o borrar datos.



Cross-site scripting (XSS)

Se cuela código malicioso en una página para que se ejecute en el navegador de otros usuarios.



Bots y fuerza bruta

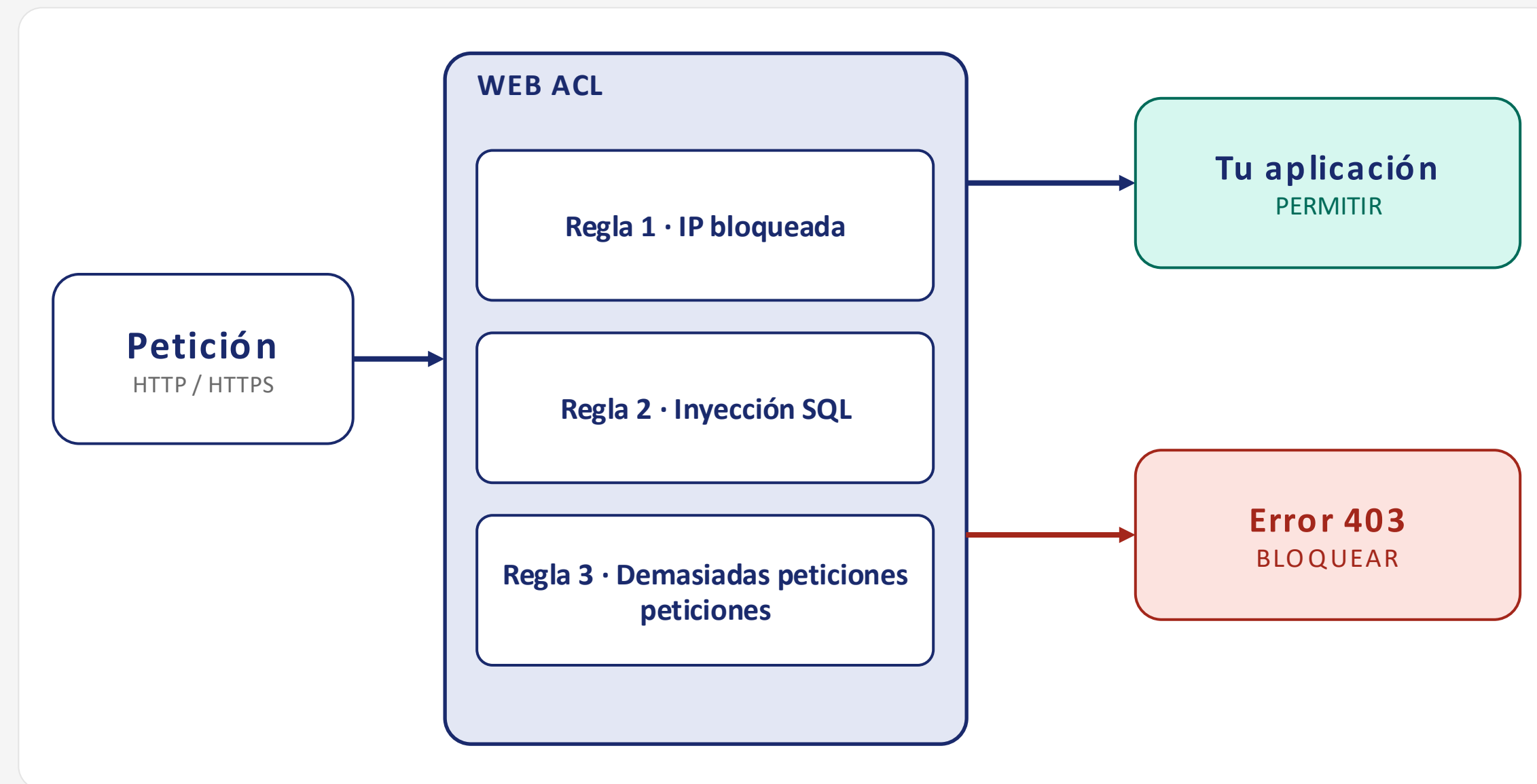
Programas que prueban miles de contraseñas o copian tu sitio de forma automática.



Inundación HTTP (DDoS)

Miles de peticiones falsas a la vez, para que tu sitio no pueda atender a nadie.

AWS WAF revisa cada petición web y decide si pasa. pasa.



SE ASOCIA A

CloudFront

Application Load Balancer

API Gateway

ACCIONES DE UNA REGLA

Allow

Block

Count

CAPTCHA

Count sirve para probar una regla sin bloquear a nadie.

Defensa en capas: cada una detiene algo distinto.



AWS WAF

Lee el contenido de la petición HTTP: inyección SQL, SQL, XSS, bots.

NACL

Filtra por IP y puerto en la subred; puede denegar denegar rangos.

SECURITY GROUP

Filtra por puerto en cada servidor; solo permite.

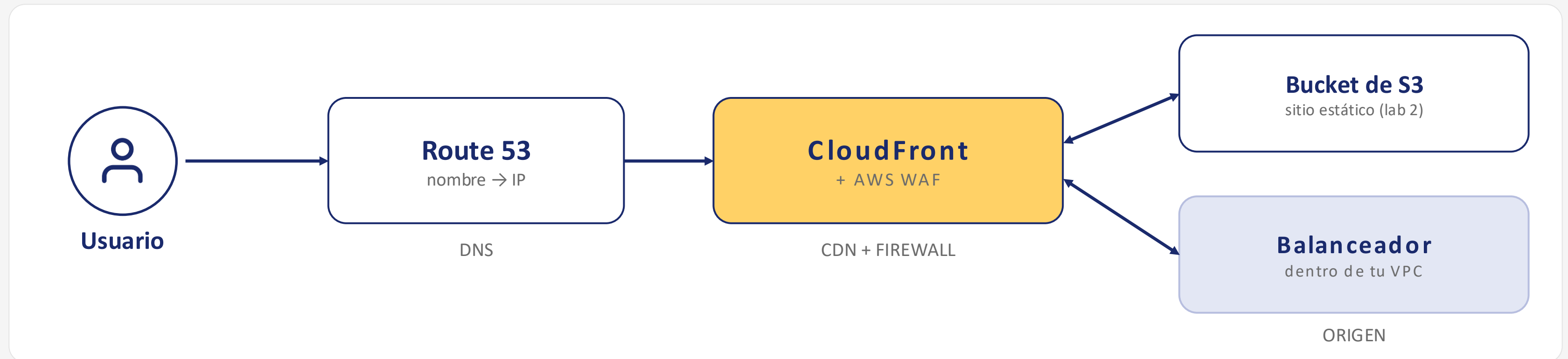
TU APLICACIÓN

Valida los datos que recibe y protege las contraseñas. contraseñas.

Qué tipos de reglas puedes usar en AWS WAF.

REGLA	QUÉ HACE	EJEMPLO
Conjunto de IP	Permite o bloquea direcciones o rangos de IP.	Bloquear 203.0.113.0/24
Basada en tasa	Limita cuántas peticiones puede hacer una misma IP.	Más de 1,000 en 5 minutos
Coincidencia de patrón	Busca texto en la URL, los encabezados o el cuerpo.	La URL contiene /admin
Geografía	Permite o bloquea según el país de origen.	Bloquear un país
Reglas administradas	Paquetes listos para usar, mantenidos por AWS.	Protección contra SQLi y XSS
AWS Shield Standard Incluido sin costo: protege contra los ataques DDoS de red más comunes.		

Todo junto: del nombre a tu aplicación.



1

Route 53 traduce tuapp.com a la dirección de CloudFront.

2

CloudFront y WAF revisan la petición y responden desde la caché si caché si pueden.

3

Solo si hace falta, llega al origen: S3 o S3 o un balancedador en tu VPC.

Lo que nos llevamos del Tema 2.

-
- 01 Route 53 traduce nombres en direcciones IP y decide a dónde mandar a cada usuario.
usuario.
 - 02 CloudFront guarda copias en edge locations cercanas: menos latencia y menos carga en el
carga en el origen.
 - 03 AWS WAF filtra las peticiones web con reglas: bloquea IP, patrones y ataques como SQLi y
XSS.
-

Tu tarea: publica un sitio con CloudFront y protégelo con WAF.

- 1 Sube un index.html sencillo al bucket de S3 de la Sesión 4. El bucket puede seguir privado.
- 2 En CloudFront crea una distribución con ese bucket como origen y activa origen y activa OAC.
- 3 Espera a que el estado sea «Deployed» y abre la URL de cloudfront.net.
- 4 En AWS WAF crea un web ACL (protection pack) en N. Virginia con una con una regla que bloquee un rango de IP.
- 5 Asócialo a tu distribución de CloudFront.
- 6 Compara: desde la IP bloqueada verás un error 403; desde otra red, el sitio carga.

AL TERMINAR DEBERÍAS VER

El sitio carga desde la URL de CloudFront, no desde S3.

Desde la IP bloqueada: error 403.

TIP Y COSTOS

Bloquea tu propia IP y prueba con los datos del celular para ver la diferencia. Al terminar, elimina la distribución y el web ACL; revisa los precios vigentes.

Cada servicio responde una pregunta.

T1 · VPC

¿Dónde vive mi red privada?

T1 · SUBRED + TABLA DE RUTEO

¿Quién tiene salida a internet?

T1 · NAT GATEWAY

¿Cómo sale lo privado sin quedar expuesto?

T1 · NACL + SECURITY GROUP

¿Qué tráfico dejo pasar?

T1 · VPN + DIRECT CONNECT

¿Cómo conecto mi oficina?

T1 · PEERING + TRANSIT GATEWAY

¿Cómo conecto mis VPC entre sí?

T2 · ROUTE 53

¿Cómo encuentran mi sitio?

T2 · CLOUDFRONT

¿Cómo llega rápido a todo el mundo?

T2 · AWS WAF

¿Cómo lo protejo de ataques?

Ponte a prueba: cinco preguntas.

-
- 01 ¿Qué convierte a una subred en pública?
 - 02 ¿Para qué sirve un NAT Gateway?
 - 03 ¿En qué se diferencian una NACL y un Security Group?
 - 04 ¿Qué ventaja le da CloudFront a un usuario que está lejos de tu servidor?
 - 05 ¿Qué puede hacer AWS WAF que un Security Group no puede?
-

Para seguir aprendiendo.

-
- | | |
|----|---|
| 01 | Documentación de Amazon VPC
docs.aws.amazon.com/vpc · guía del usuario y tutoriales |
| 02 | Documentación de Amazon Route 53
docs.aws.amazon.com/route53 · dominios, registros y políticas |
| 03 | Documentación de Amazon CloudFront
docs.aws.amazon.com/cloudfront · distribuciones, caché y OAC |
| 04 | Documentación de AWS WAF
docs.aws.amazon.com/waf · web ACL, reglas y acciones |
| 05 | AWS Skill Builder
skillbuilder.aws · cursos y rutas de aprendizaje |
-

CIERRE

Q&A

Gracias. Preguntas, dudas y comentarios.

Tarea: Laboratorio 1 (VPC con subred pública y privada) y Laboratorio 2 (sitio estático con CloudFront y WAF). Al terminar, borra los recursos.