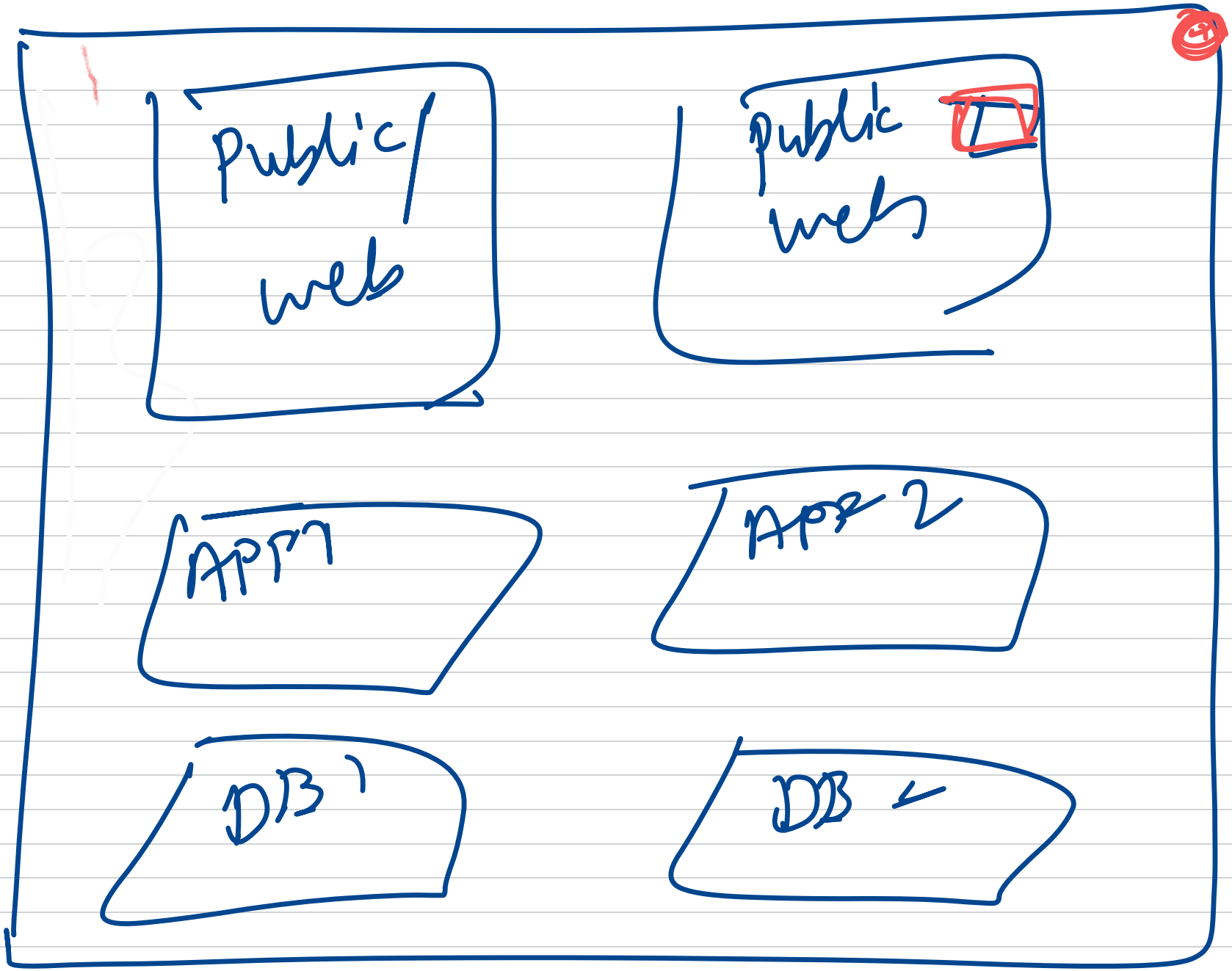
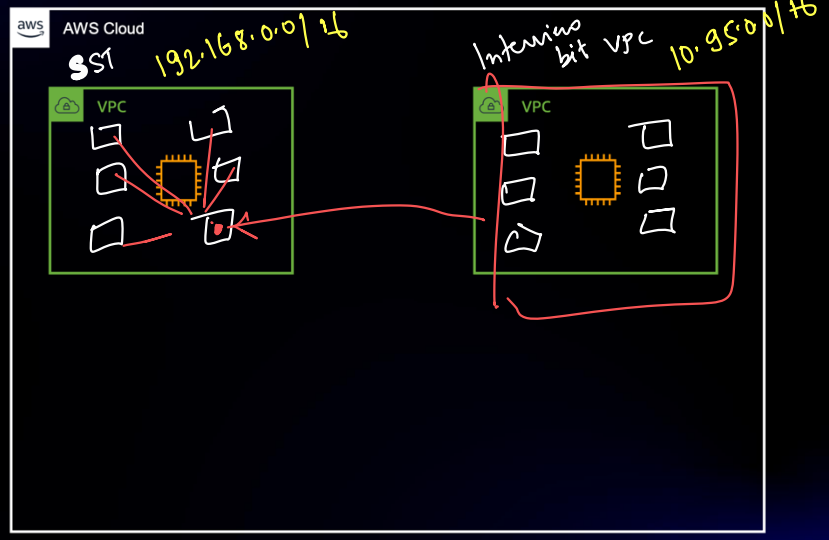
Agenda

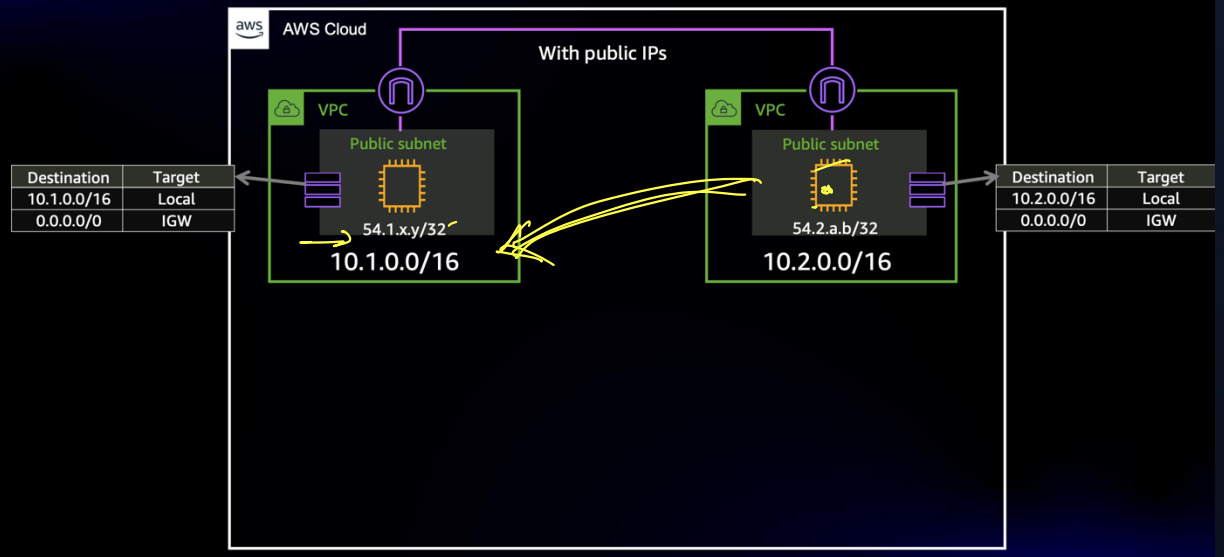
Quick Recap VPC


public/
web
public
web
APP1
APP 2
DB 1
DB 2

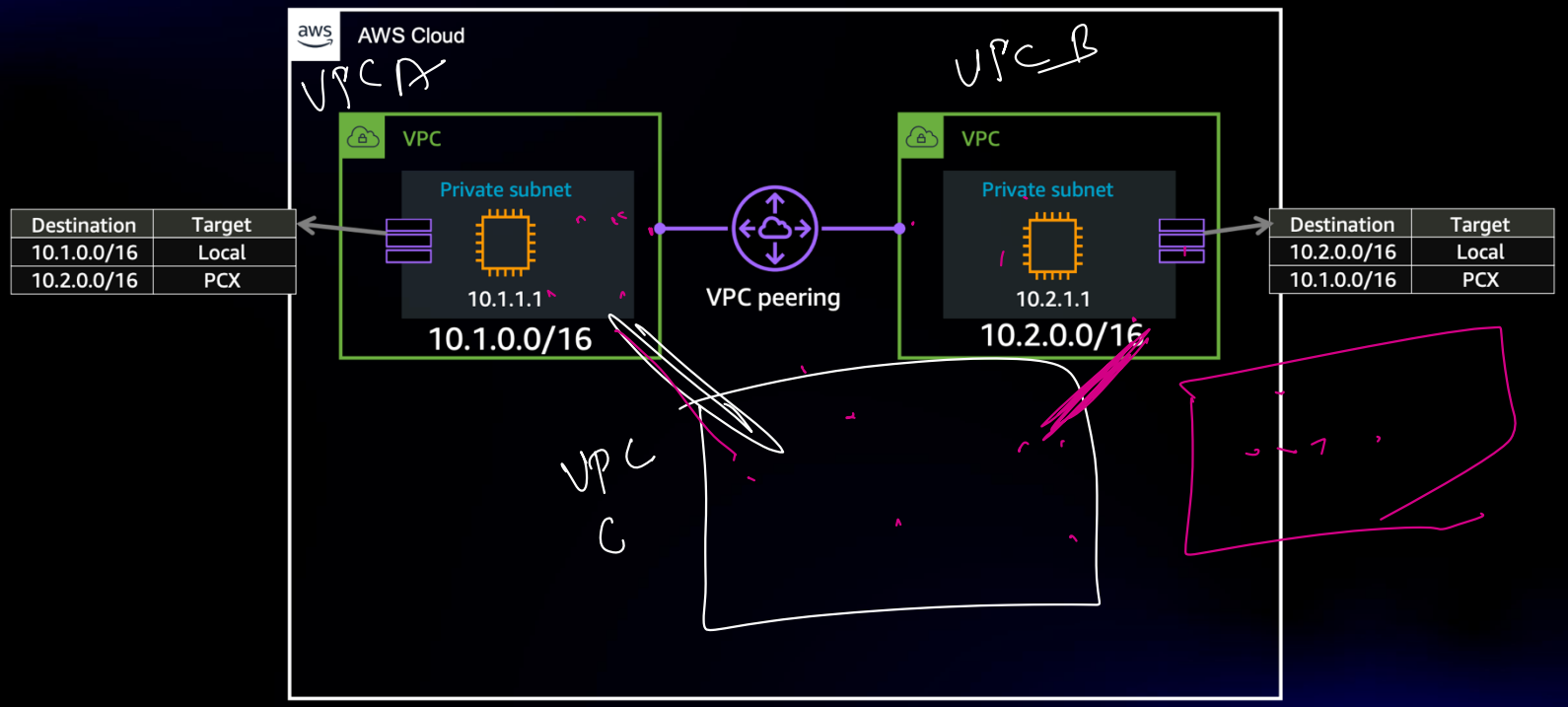
VPC-to-VPC connectivity options



VPC-to-VPC connectivity – Internet



VPC-to-VPC connectivity – VPC peering



Full mesh: How many Amazon VPC peering connections do I need to achieve full mesh?

$$\frac{n(n-1)}{2}$$

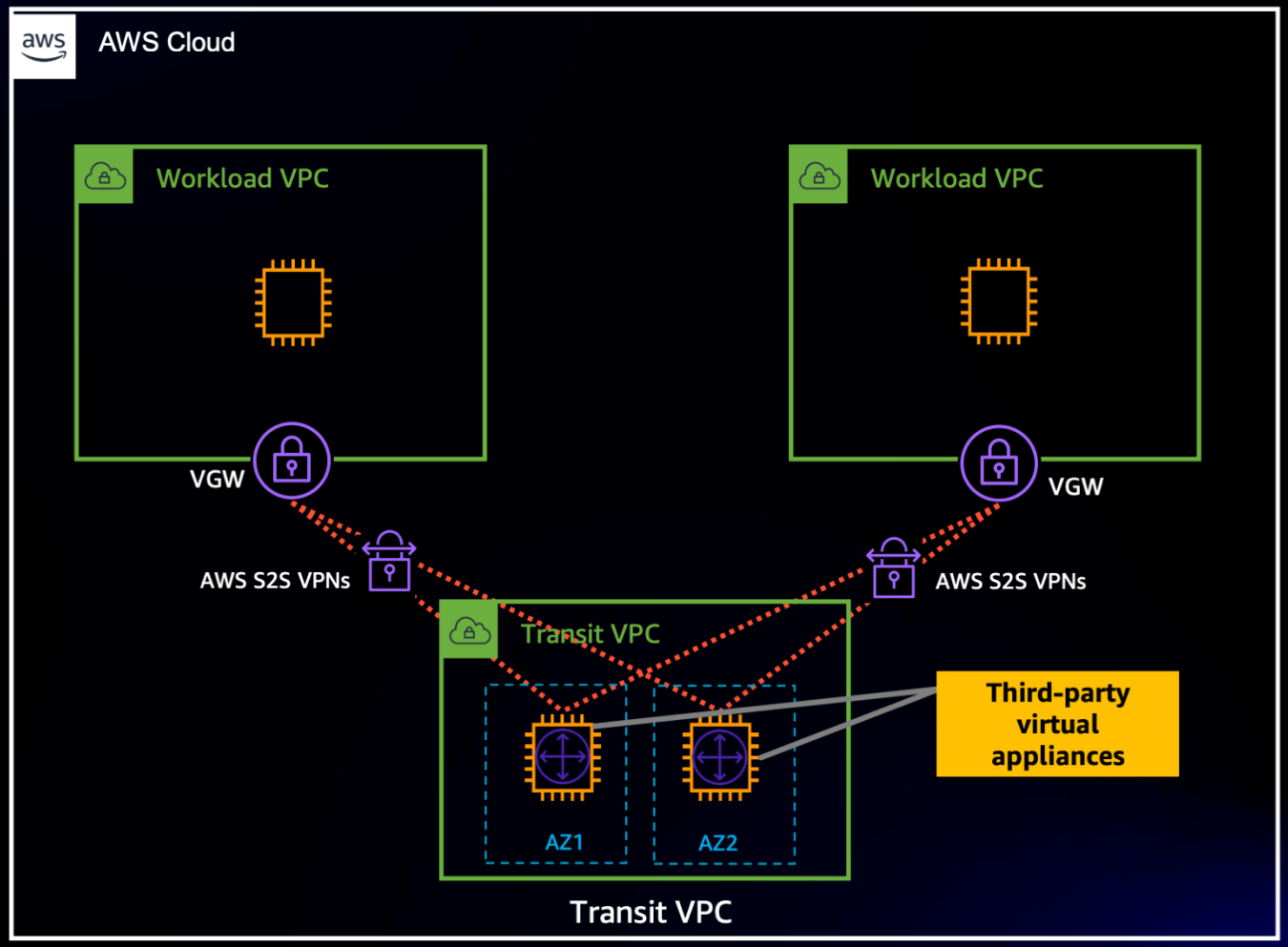
VPCs x 10

Full mesh: How many Amazon VPC peering connections do I need to achieve full mesh?

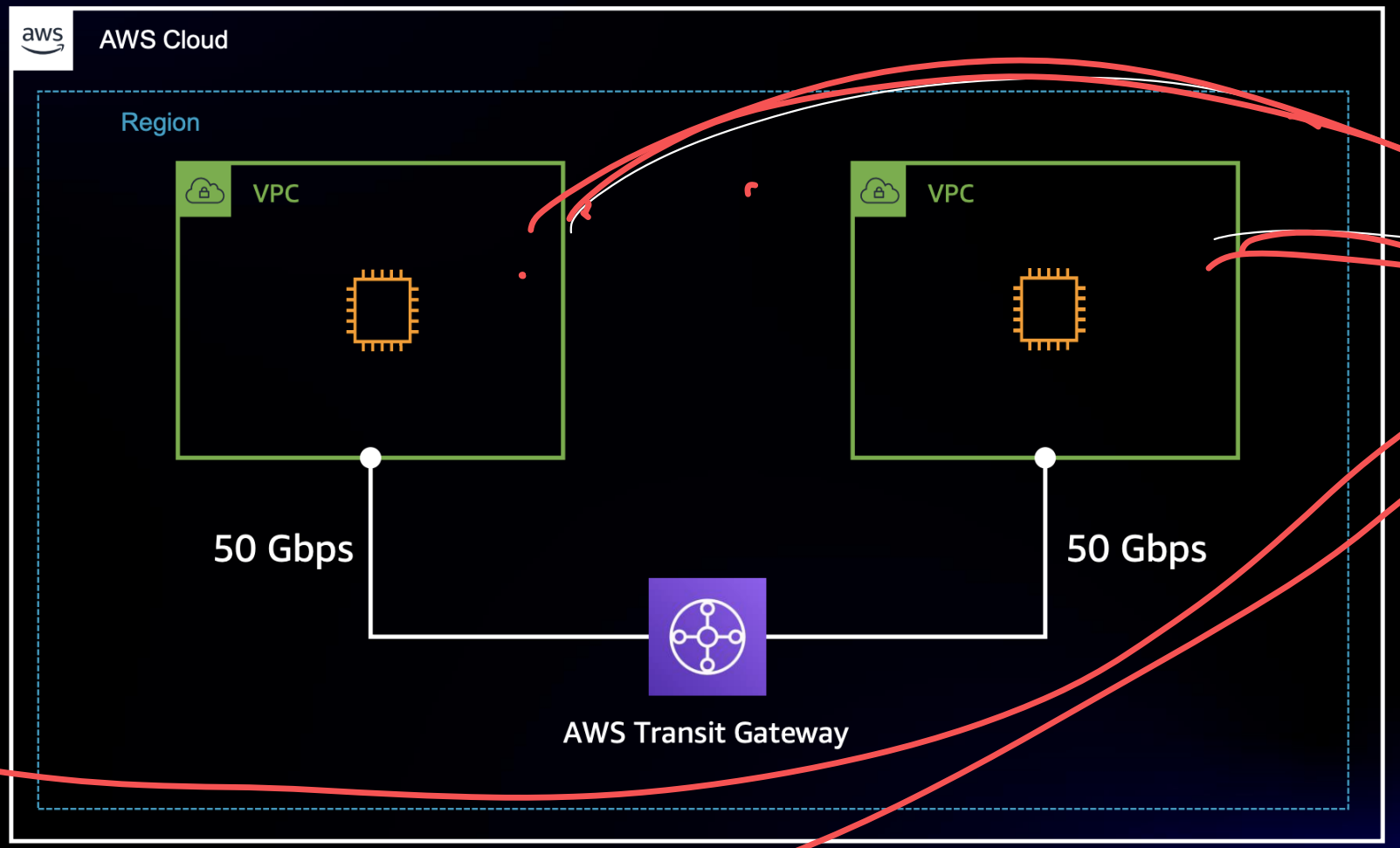
45

VPCs x 10

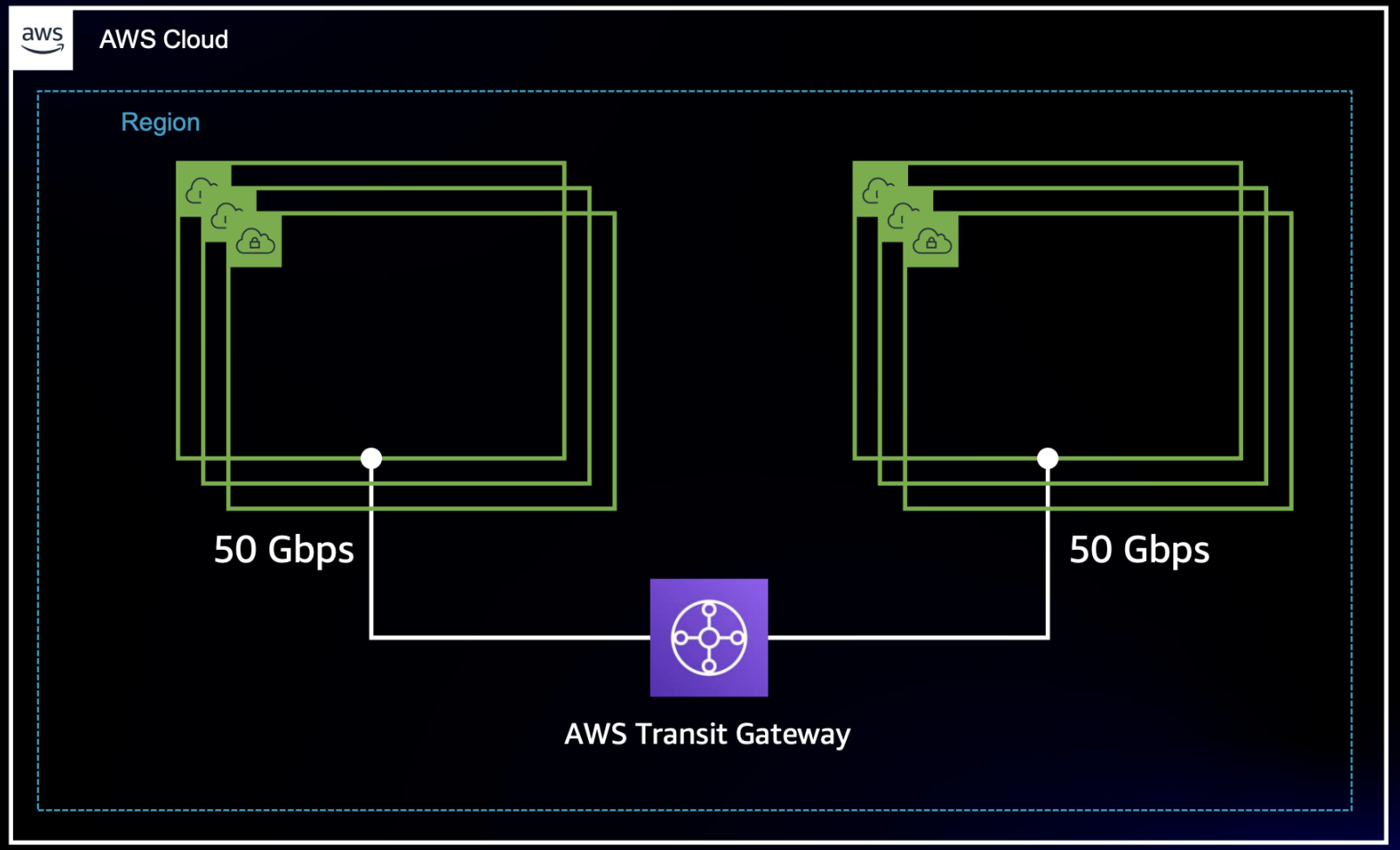
VPC-to-VPC connectivity – Transit VPC



VPC-to-VPC connectivity – AWS Transit Gateway

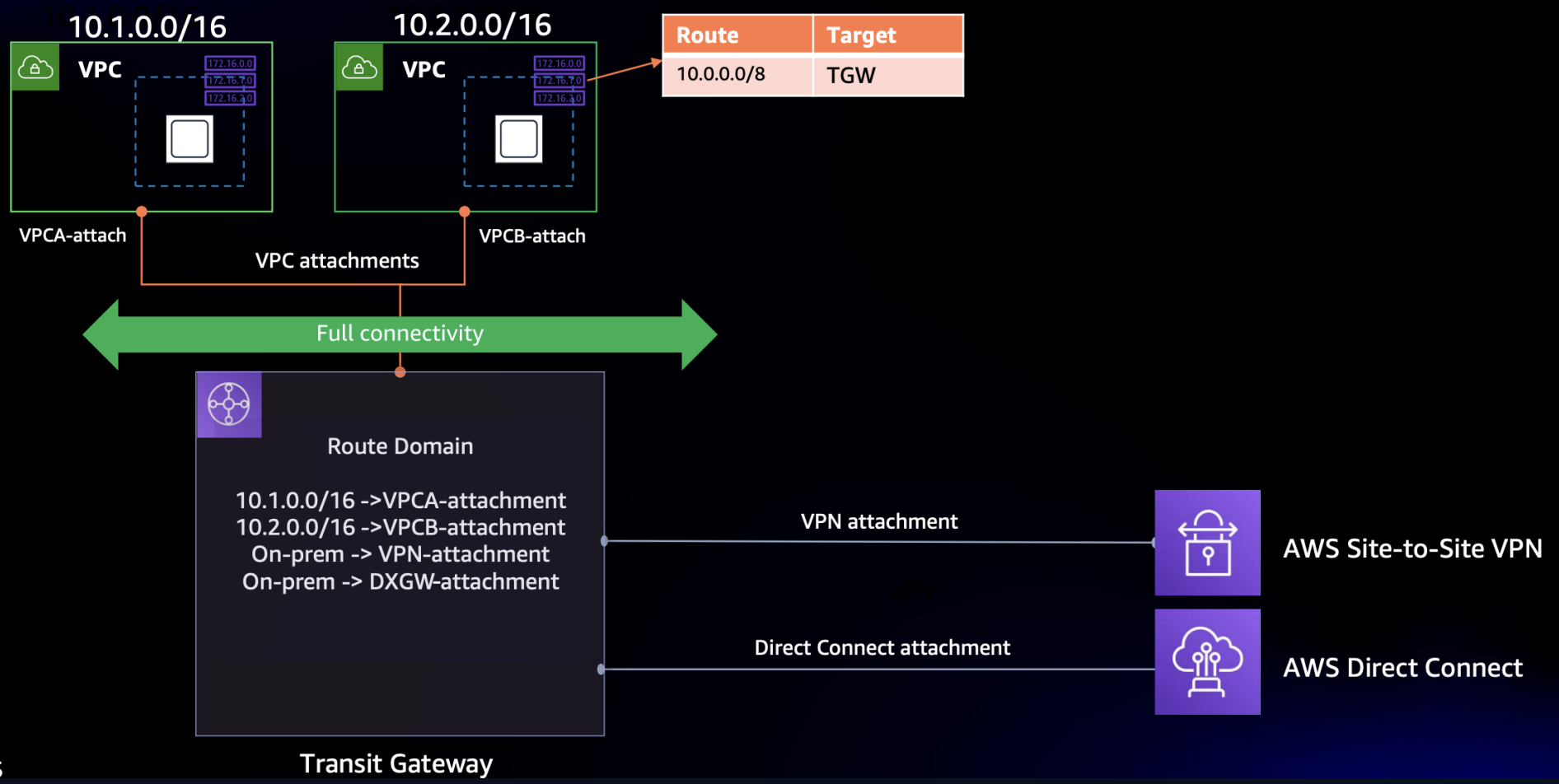


VPC-to-VPC connectivity – AWS Transit Gateway

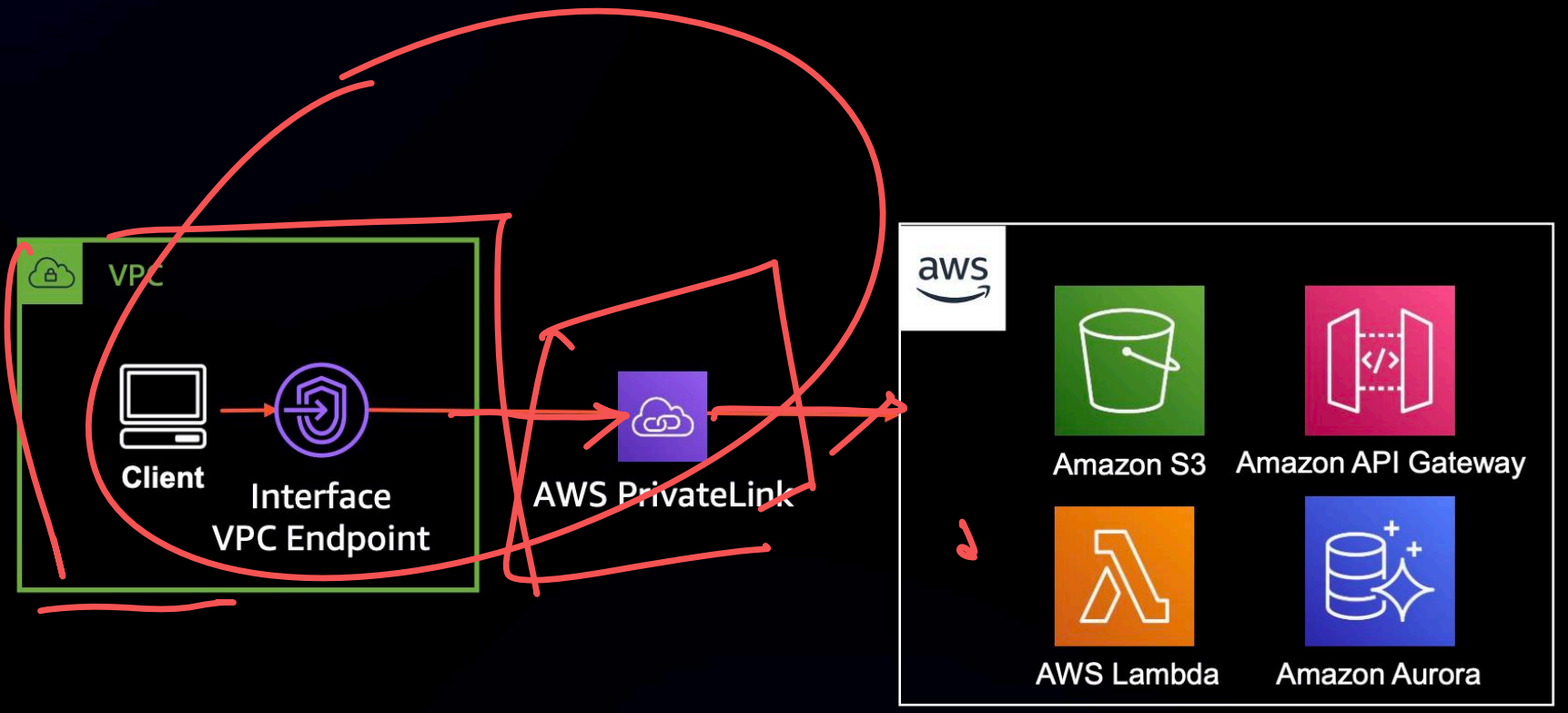


VPCs
x5000

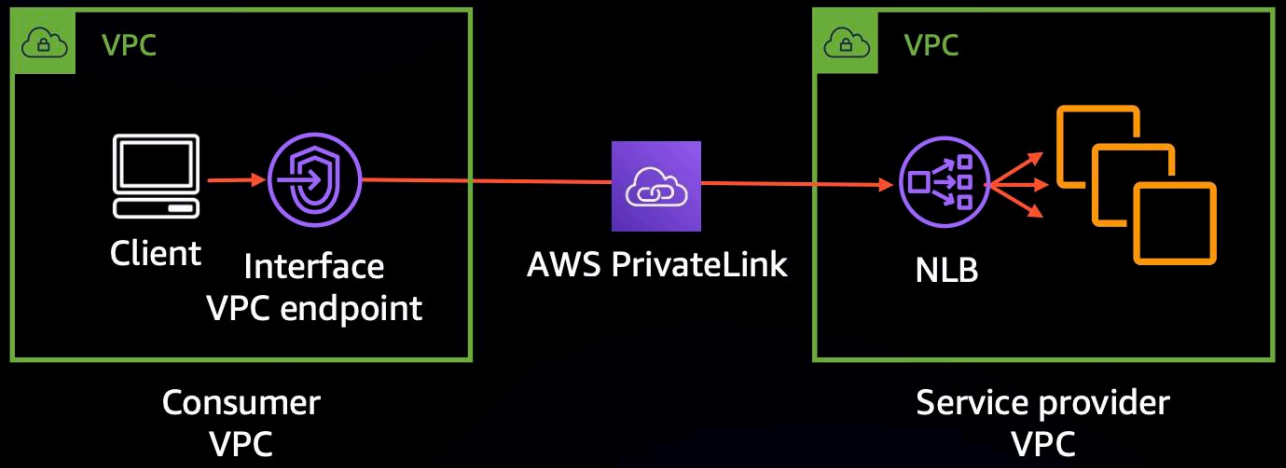
Transit Gateway – Flat network



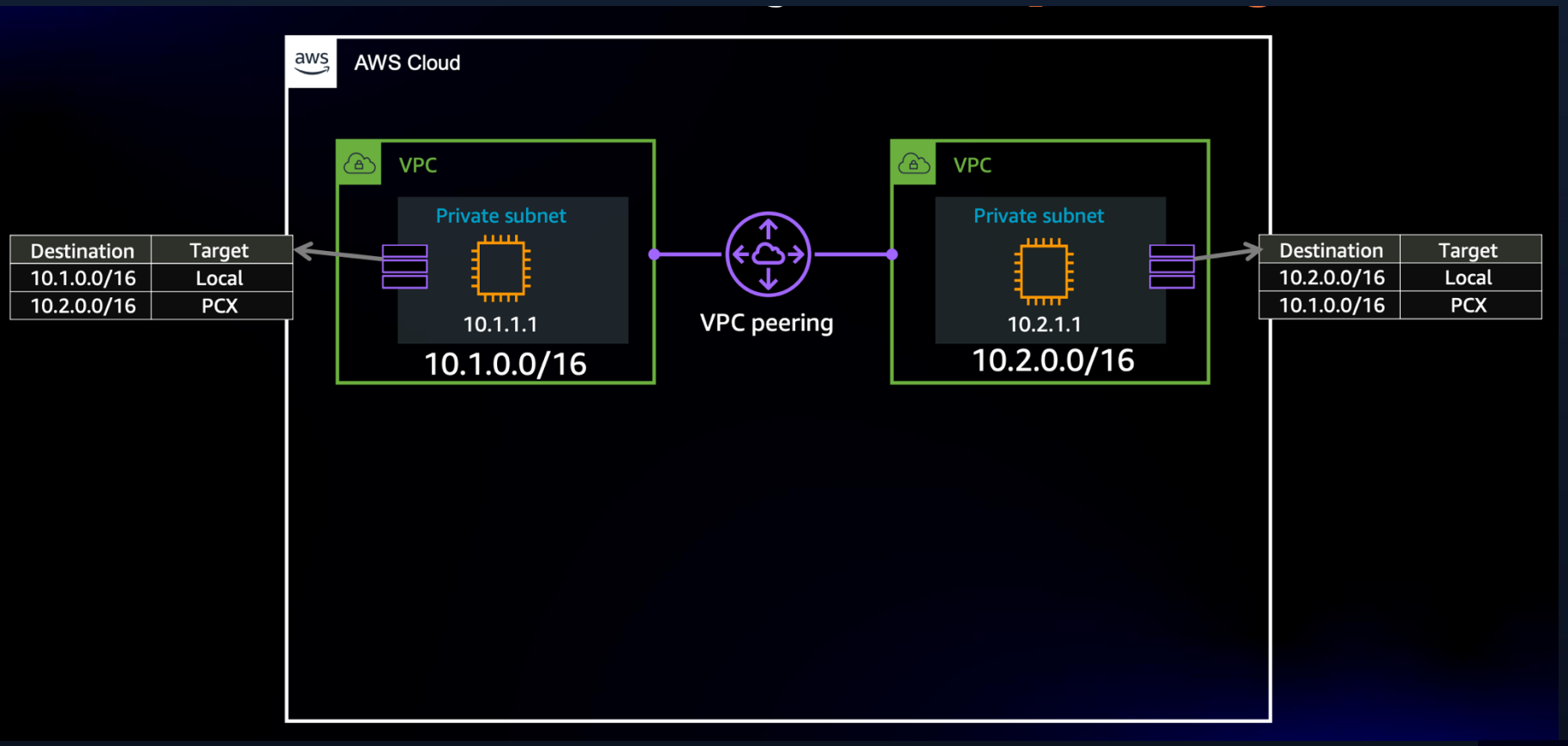
AWS PrivateLink



AWS PrivateLink



VPC Connectivity Options (Peering)



Full mesh: How many Amazon VPC peering connections do I need to achieve full mesh?

$$\frac{n(n-1)}{2}$$

VPCs x 10

VPC Connectivity Options (Peering)

Connecting VPCs and On-Premises Networks

AWS offers multiple options to connect your VPC to other networks.

VPC Peering | AWS VPN | Direct Connect | Transit Gateway

VPC Peering

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.

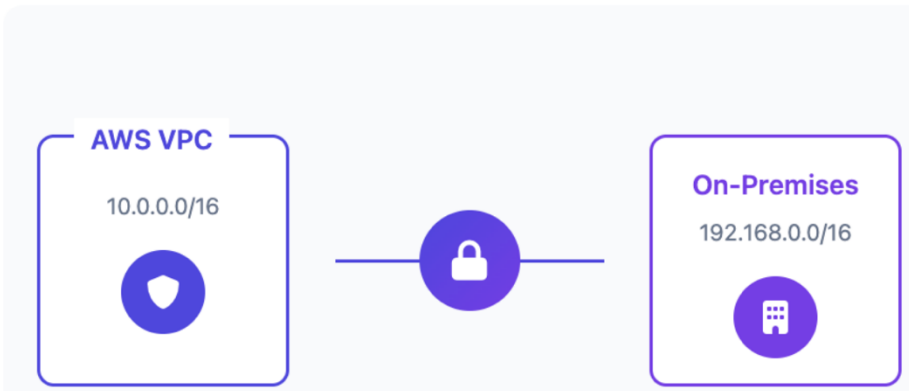
- Direct network route between two VPCs
- No gateway or VPN connection required
- No single point of failure or bandwidth bottleneck
- Traffic stays on the AWS global network

VPC Connectivity Options (VPN)

Connecting VPCs and On-Premises Networks

AWS offers multiple options to connect your VPC to other networks.

VPC Peering | **AWS VPN** | Direct Connect | Transit Gateway



AWS VPN

AWS Virtual Private Network (VPN) solutions establish secure connections between your on-premises networks, remote offices, client devices, and the AWS global network.

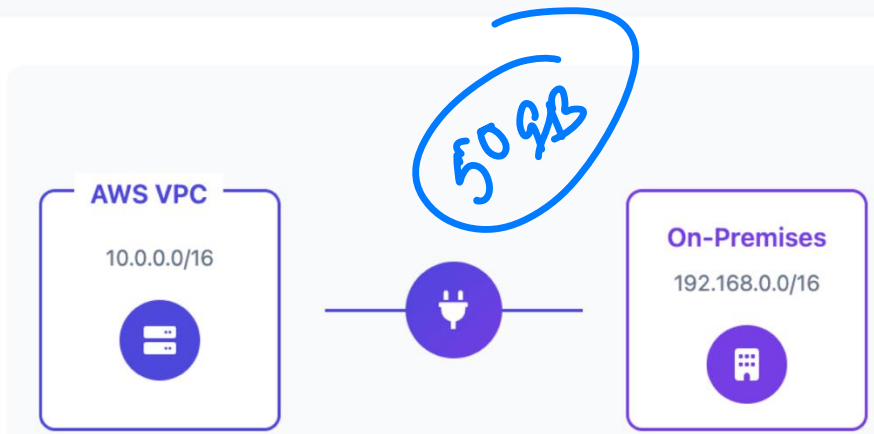
- Site-to-Site VPN connects on-premises to AWS
- Client VPN connects remote users to AWS
- Encrypted connection over the internet
- Supports IPsec protocol

VPC Connectivity Options (Direct Connect)

Connecting VPCs and On-Premises Networks

AWS offers multiple options to connect your VPC to other networks.

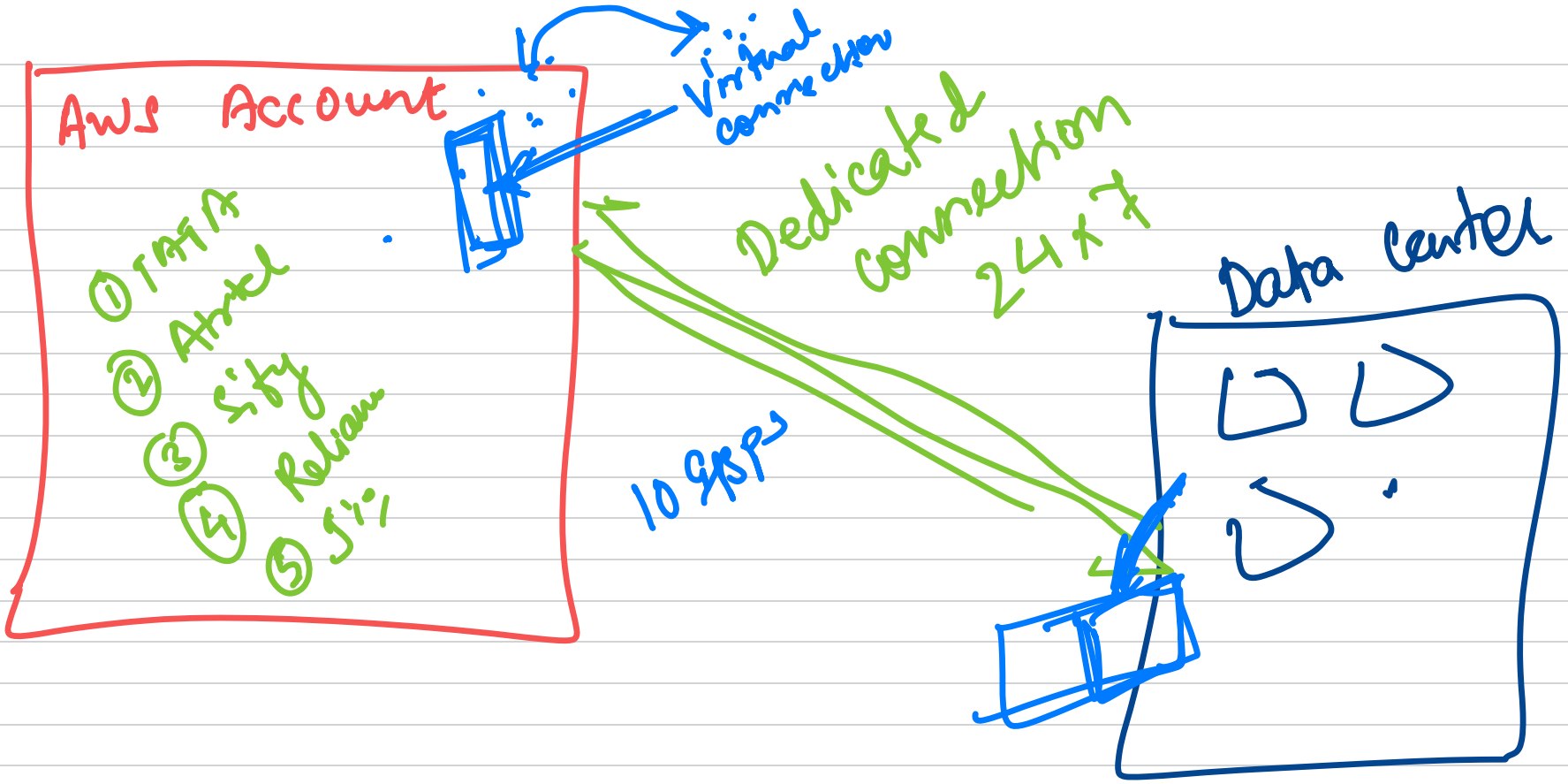
VPC Peering | AWS VPN | **Direct Connect** | Transit Gateway



AWS Direct Connect

AWS Direct Connect is a cloud service that establishes a dedicated network connection from your premises to AWS, providing consistent network performance and reducing bandwidth costs.

- Dedicated private connection
- Reduced network costs
- Consistent network performance
- Compatible with all AWS services

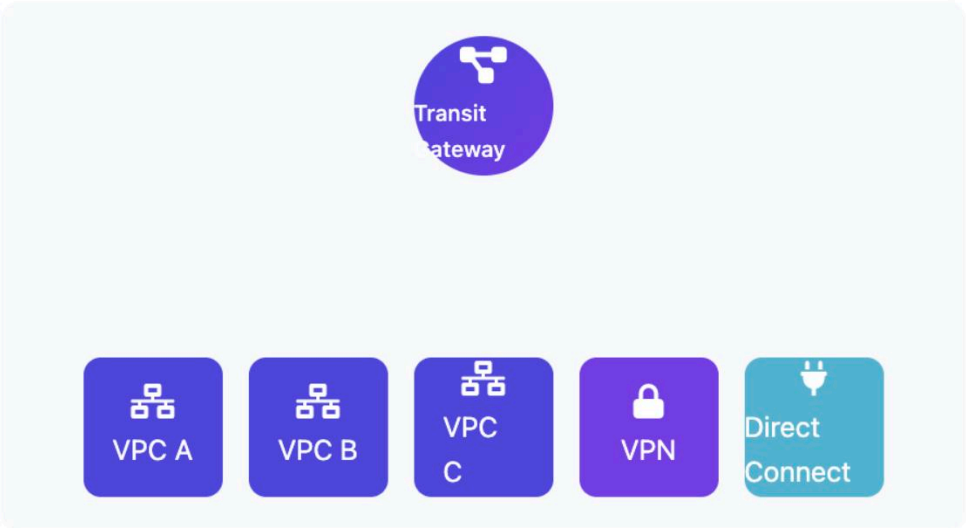

AWS Account
Virtual connection
Dedicated connection 24 x 7
Data center
10 Gbps

VPC Connectivity Options (Mixed Connect)

Connecting VPCs and On-Premises Networks

AWS offers multiple options to connect your VPC to other networks.

VPC Peering | AWS VPN | Direct Connect | **Transit Gateway**

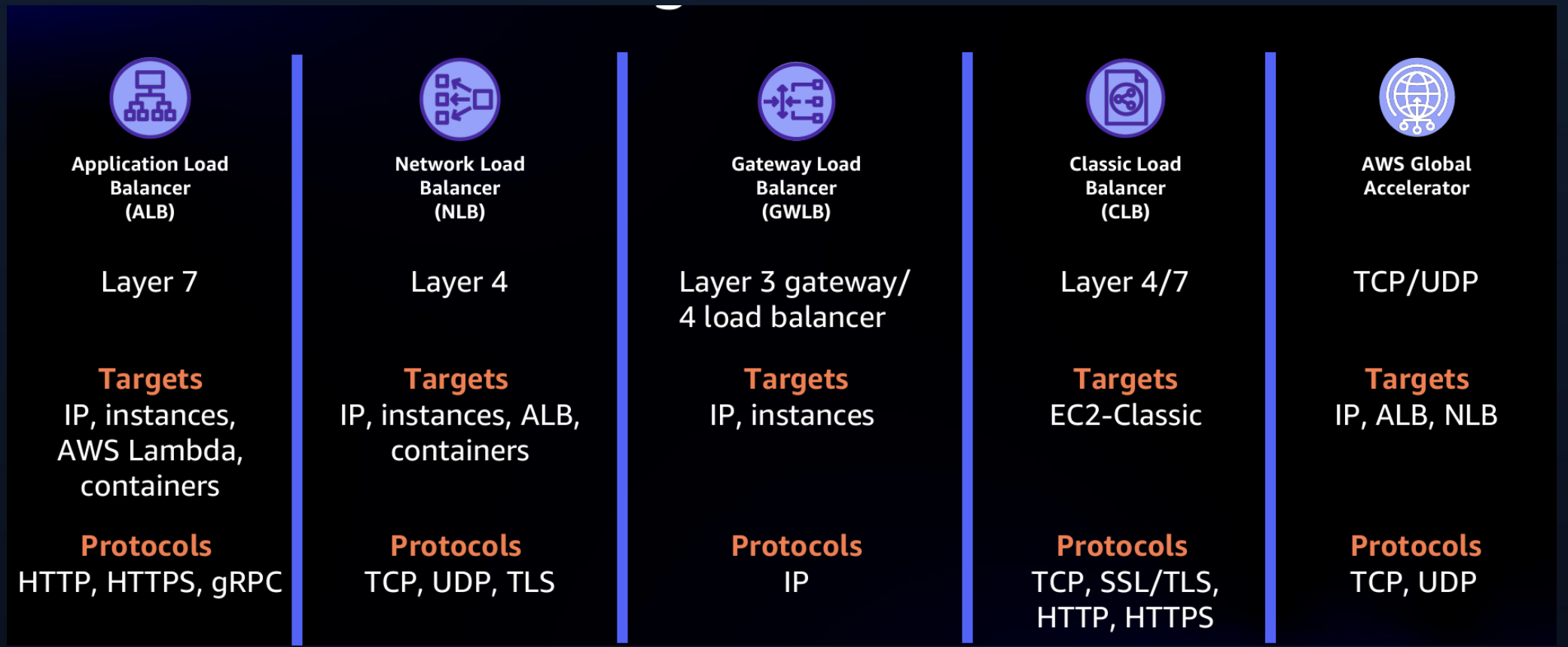


AWS Transit Gateway

AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway.

- Hub-and-spoke connectivity model
- Simplifies network architecture
- Centralized control and management
- Supports thousands of connections

Types of Load balancer



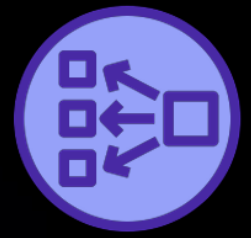
Which load balancing technology should we use?

Targets	Requires
Instances	Layer 7 routing
AWS Lambda	HTTP2/gRPC
Containers	Redirects, web sockets
IP	Fixed response
	Authentication
	Web application firewall, AWS Outposts/AWS Local Zones
	Cookie stickiness, HTTP Desync mitigation
	Best option for the AWS Load Balancer Controller for containers

Application Load Balancer

Which load balancing technology should we use?

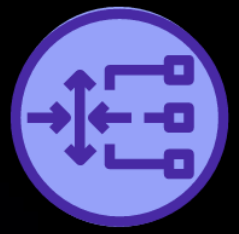
Targets	Requires
Instances	Low latency
ALB	Zonal isolation
Containers	Long-lived TCP connections
IP	Connection-based Layer 4 load balancing
	PrivateLink support
	Elastic IP support
	Hybrid architecture support
	AWS Fargate support direct to K8s pod



Network Load Balancer

Which load balancing technology should we use?

Targets	Requires
Instances	Bump in the wire
	Auto scaling for packet processing devices (firewall, IdP)
	Packet preservation for inspection
IP	PrivateLink GWLB endpoint
	Multi-port to same instance
	Route table entry



Gateway Load Balancer

Which load balancing technology should we use?

Targets	Requires
NLB	Accelerate latency-sensitive applications
ALB	Improve resiliency and availability on a global scale
IP	Simplified global traffic management
	Global set of anycast static IP addresses

AWS Global Accelerator