DIGITAL TALENT SCHOLARSHIP 2020

digitalent.kominfo.go.id

digitalent.kominfo.go.id

SA Networking

Agenda

- VPC Subnet Routing
- VPC Peering
- VPC Transit Gateway
- VPC End Point

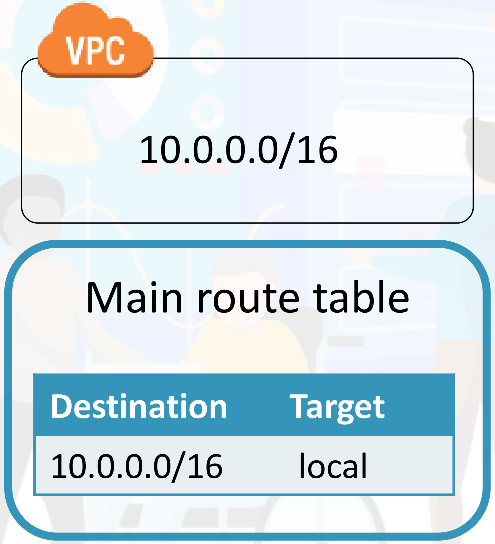
How do you control your VPC traffic?

Route tables, security groups, network ACLs, and Internet gateways

Route Tables: Directing Traffic Between VPC Resources

Route tables:

- Determine where network traffic is routed
- Main (default) and custom route tables
- All route tables include a local route entry
  - Local route covers the entire VPC
  - The local route entry cannot be deleted
- Only one route table per subnet



Destination	Target
10.0.0.0/16	local

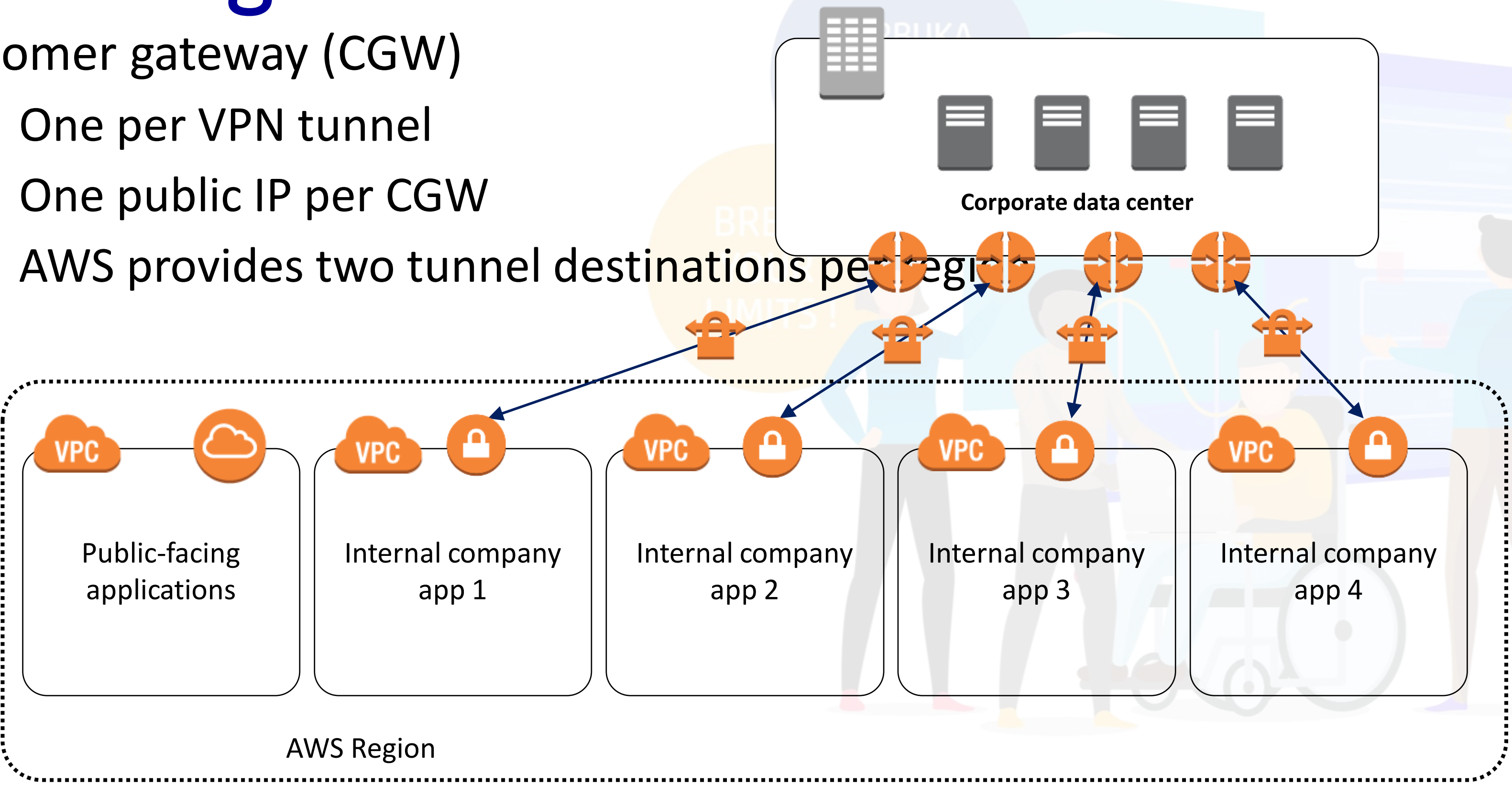
Best practice: Use custom route tables for each subnet.

Can you connect multiple VPCs to each other?

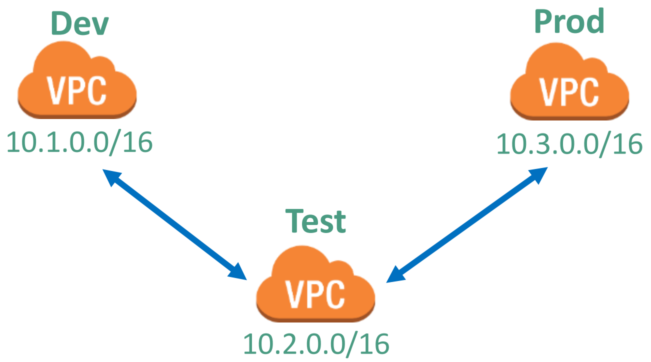
Is This the Most Efficient Way of Connecting VPCs?

Customer gateway (CGW)

- One per VPN tunnel
- One public IP per CGW
- AWS provides two tunnel destinations per region



Connecting VPCs – VPC Peering

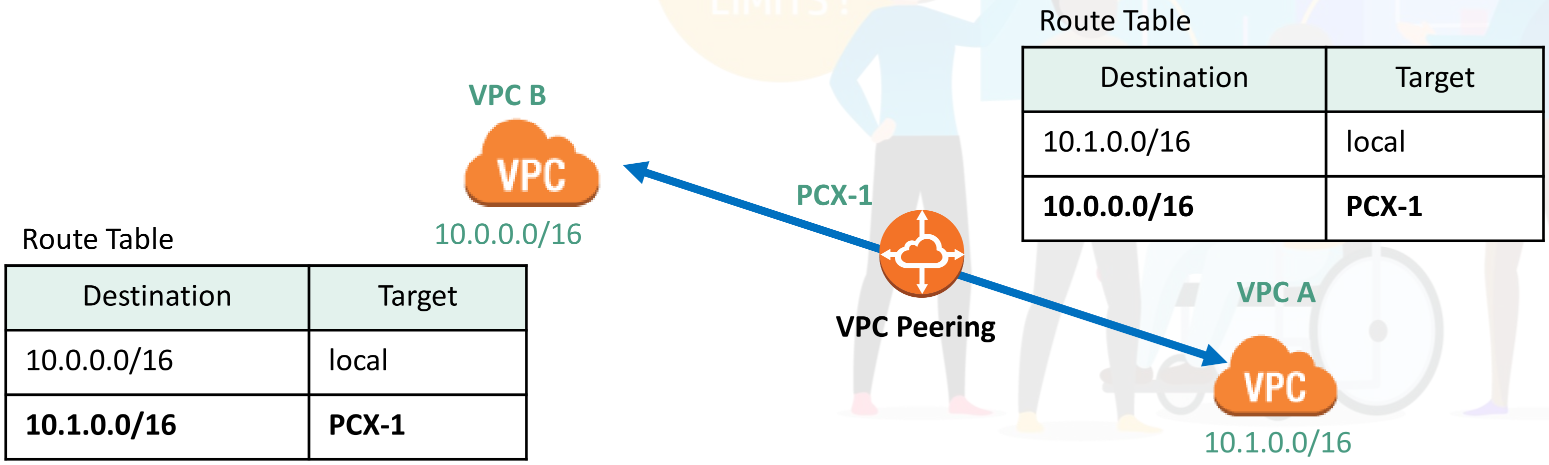


Instances can communicate across a peering connection as if they were in the same network.

- Use private IP addresses
- Intra and inter-region support
- IP spaces cannot overlap
- Only one peering resource between any two VPCs
- Transitive peering relationships are not supported
- Can be established between different AWS accounts

How Does VPC Peering Work?

- No Internet gateway or virtual gateway required.
- No single point of failure.
- No bandwidth bottlenecks.
- Traffic always stays on the global AWS backbone.



Route Table

Destination	Target
10.1.0.0/16	local
10.0.0.0/16	**PCX-1**

Route Table

Destination	Target
10.0.0.0/16	local
10.1.0.0/16	**PCX-1**

Peering Multiple VPCs

General Best Practices

When connecting multiple VPCs, there are some universal network-design principles to consider:

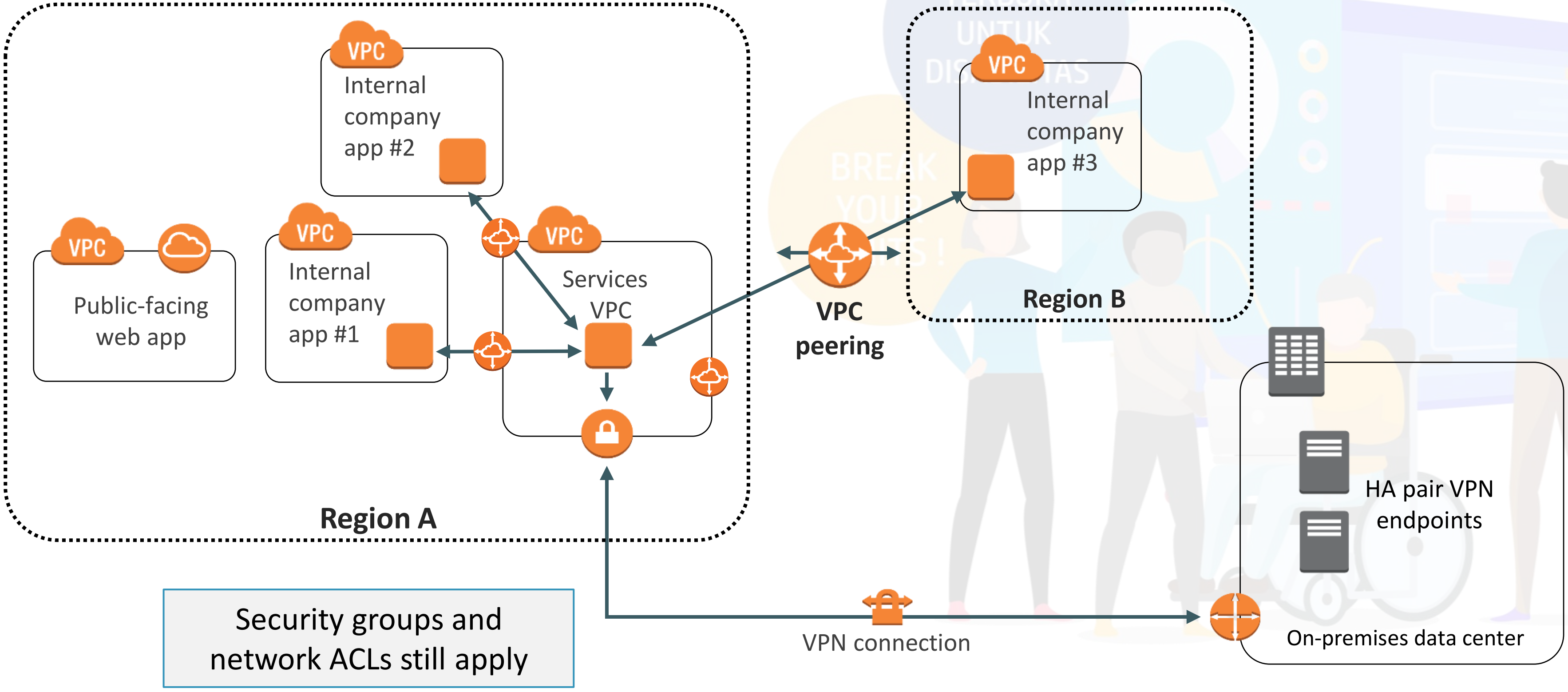
Destination	Target
10.1.0.0/16	local
10.2.0.0/16	**PCX-1**

No overlapping CIDR blocks

Only connect essential VPCs

Make sure your solution can scale

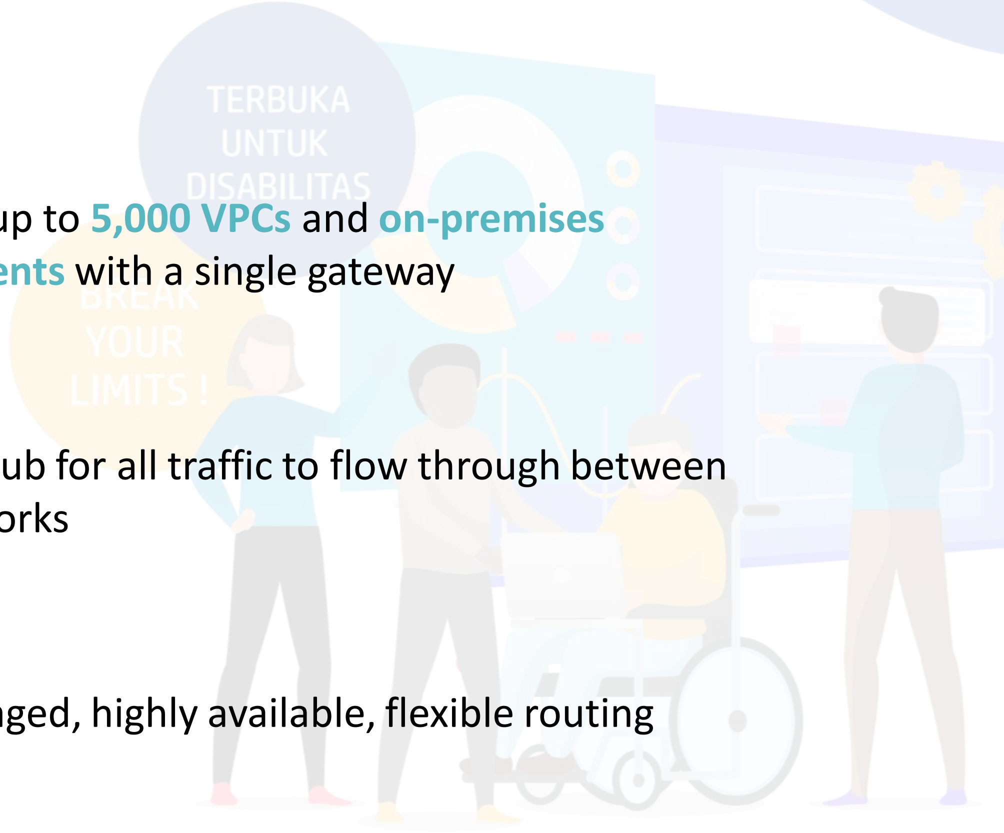
Example: VPC Peering for Shared Services



Security groups and network ACLs still apply

Connecting VPCs - Transit Gateway

AWS Transit Gateway



Connects up to **5,000 VPCs** and **on-premises environments** with a single gateway

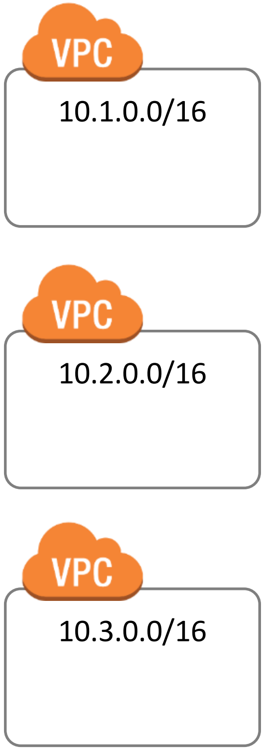
Acts as a hub for all traffic to flow through between your networks

Fully managed, highly available, flexible routing service

Transit Gateway in Action - Connected

Scenario: We want all three VPCs to be able to be fully connected.

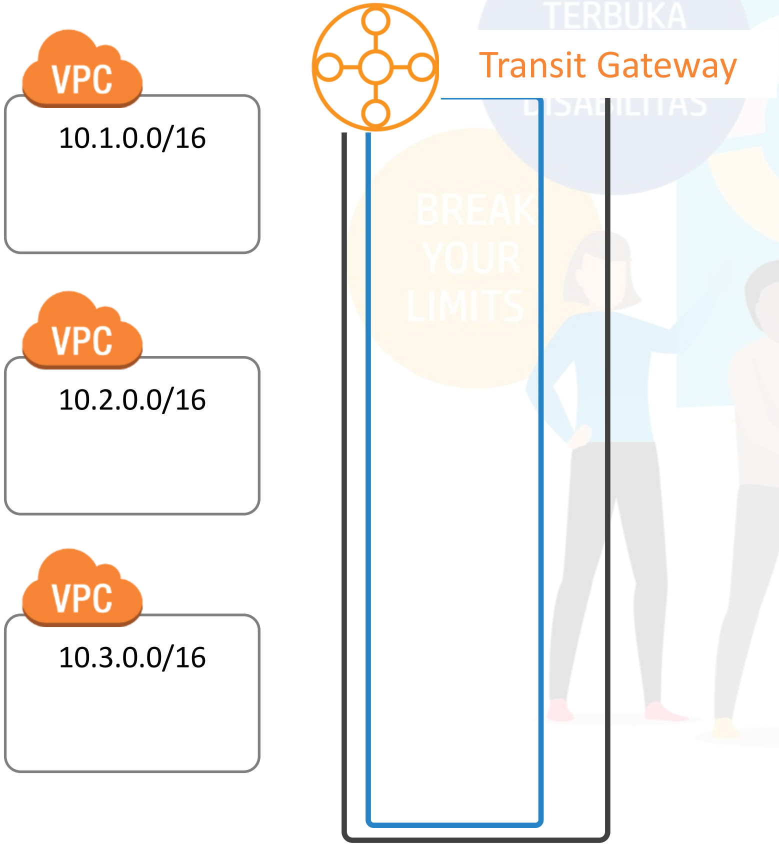
How do we do this using Transit Gateway?



Transit Gateway in Action - Connected

Scenario: We want all three VPCs to be able to be fully connected.

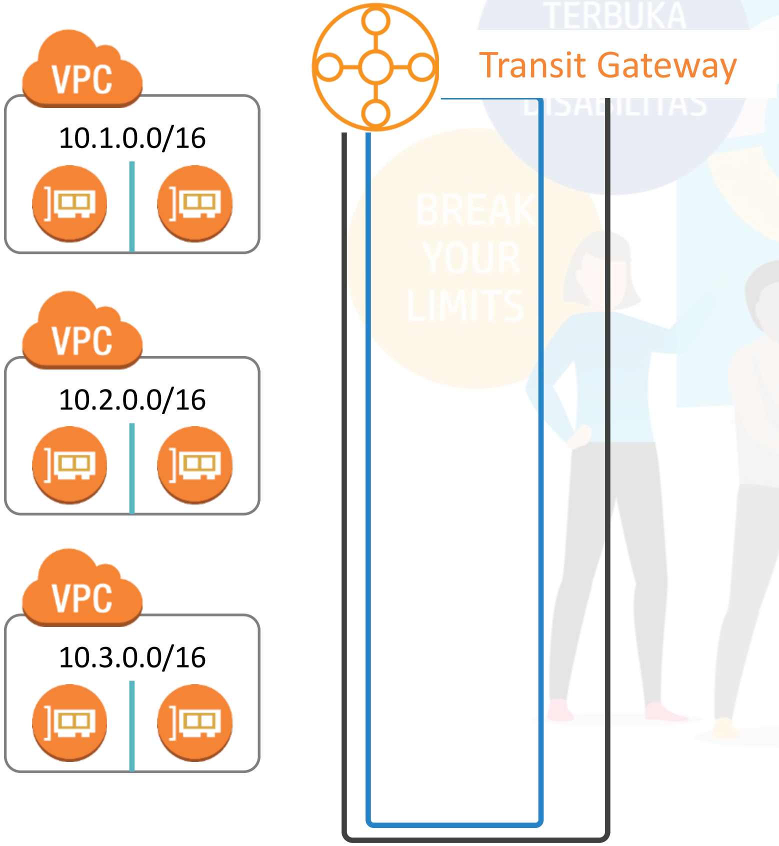
How do we do this using Transit Gateway?



Transit Gateway in Action - Connected

Scenario: We want all three VPCs to be able to be fully connected.

How do we do this using Transit Gateway?



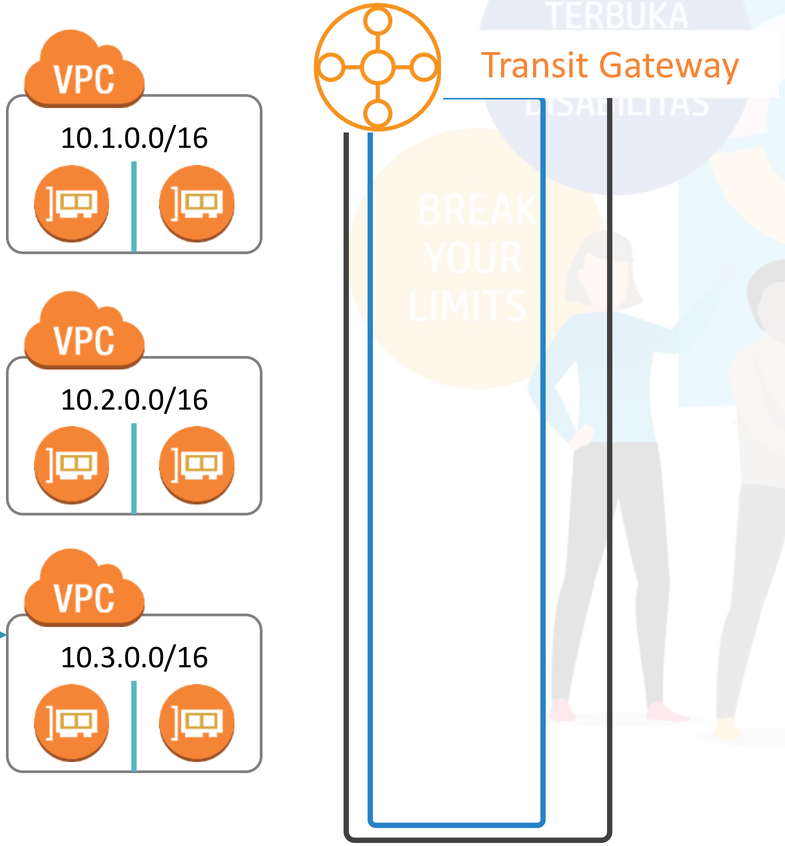
Transit Gateway in Action - Connected

Scenario: We want all three VPCs to be able to be fully connected.

How do we do this using Transit Gateway?

Per VPC Route Table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx



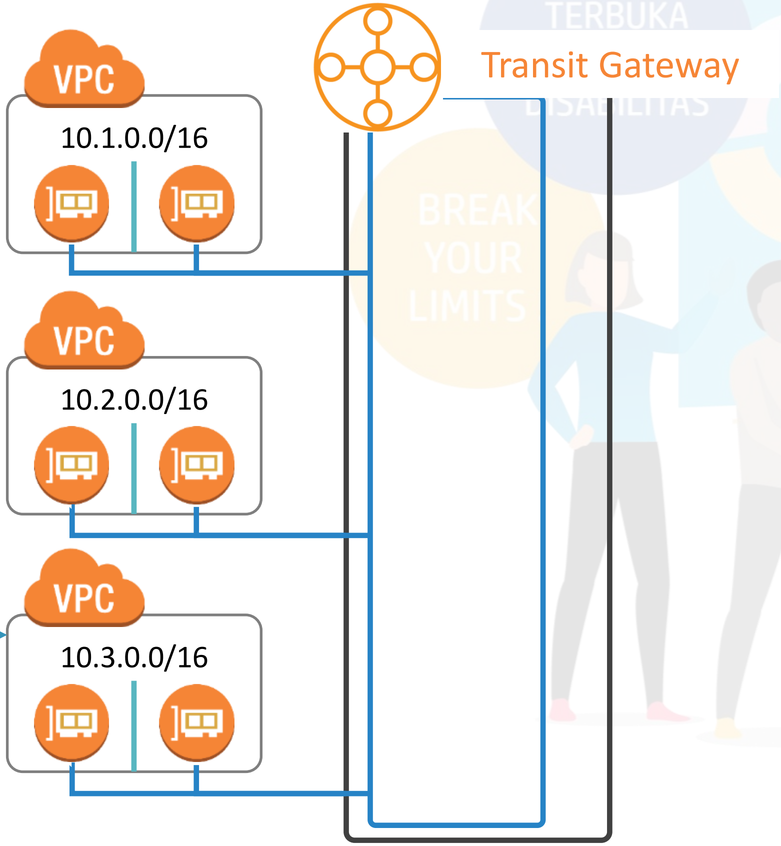
Transit Gateway in Action - Connected

Scenario: We want all three VPCs to be able to be fully connected.

How do we do this using Transit Gateway?

Per VPC Route Table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx



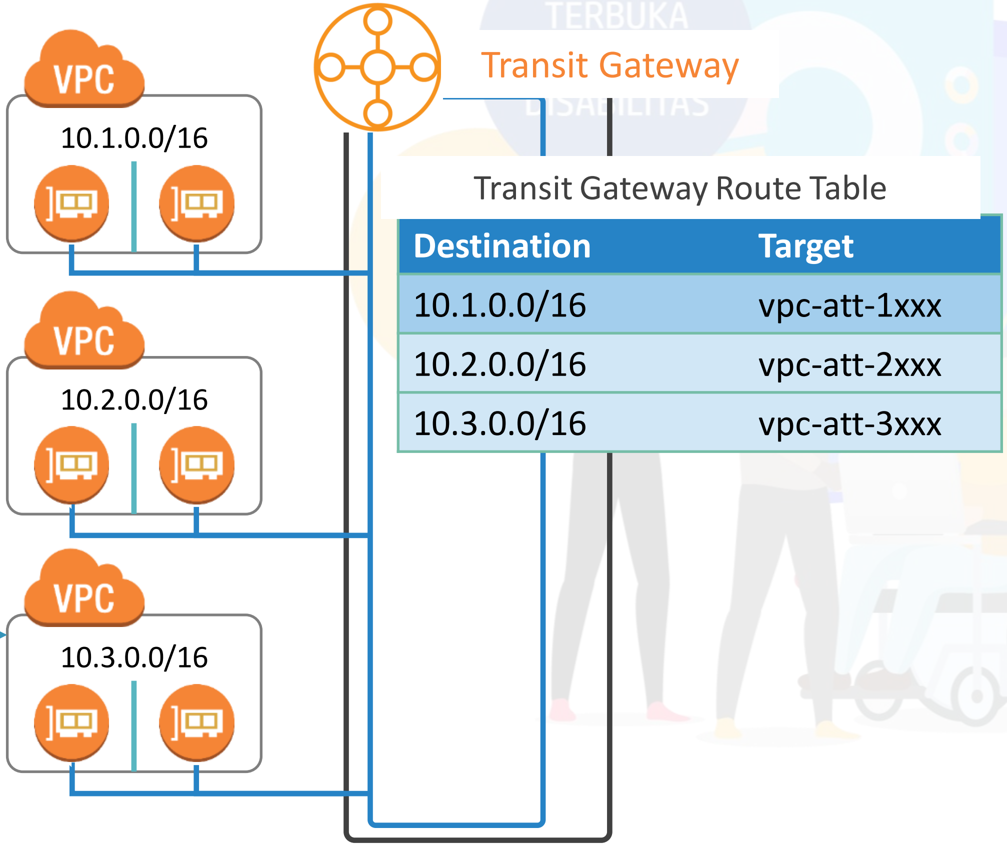
Transit Gateway in Action - Connected

Scenario: We want all three VPCs to be able to be fully connected.

How do we do this using Transit Gateway?

Per VPC Route Table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx



Transit Gateway Route Table

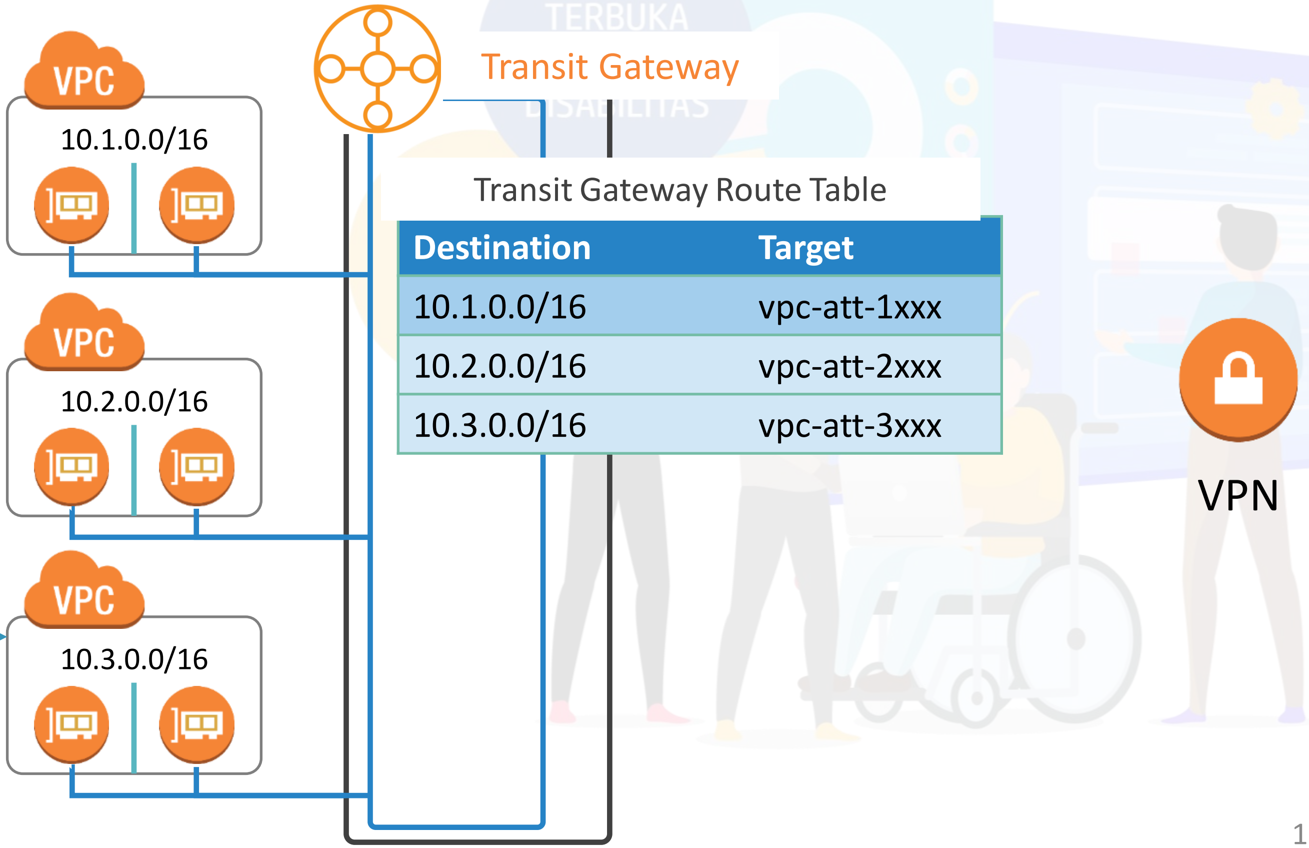
Destination	Target
10.1.0.0/16	vpc-att-1xxx
10.2.0.0/16	vpc-att-2xxx
10.3.0.0/16	vpc-att-3xxx

Transit Gateway in Action - Isolation

Scenario: We now want isolated connectivity and VPN access.

Per VPC Route Table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx

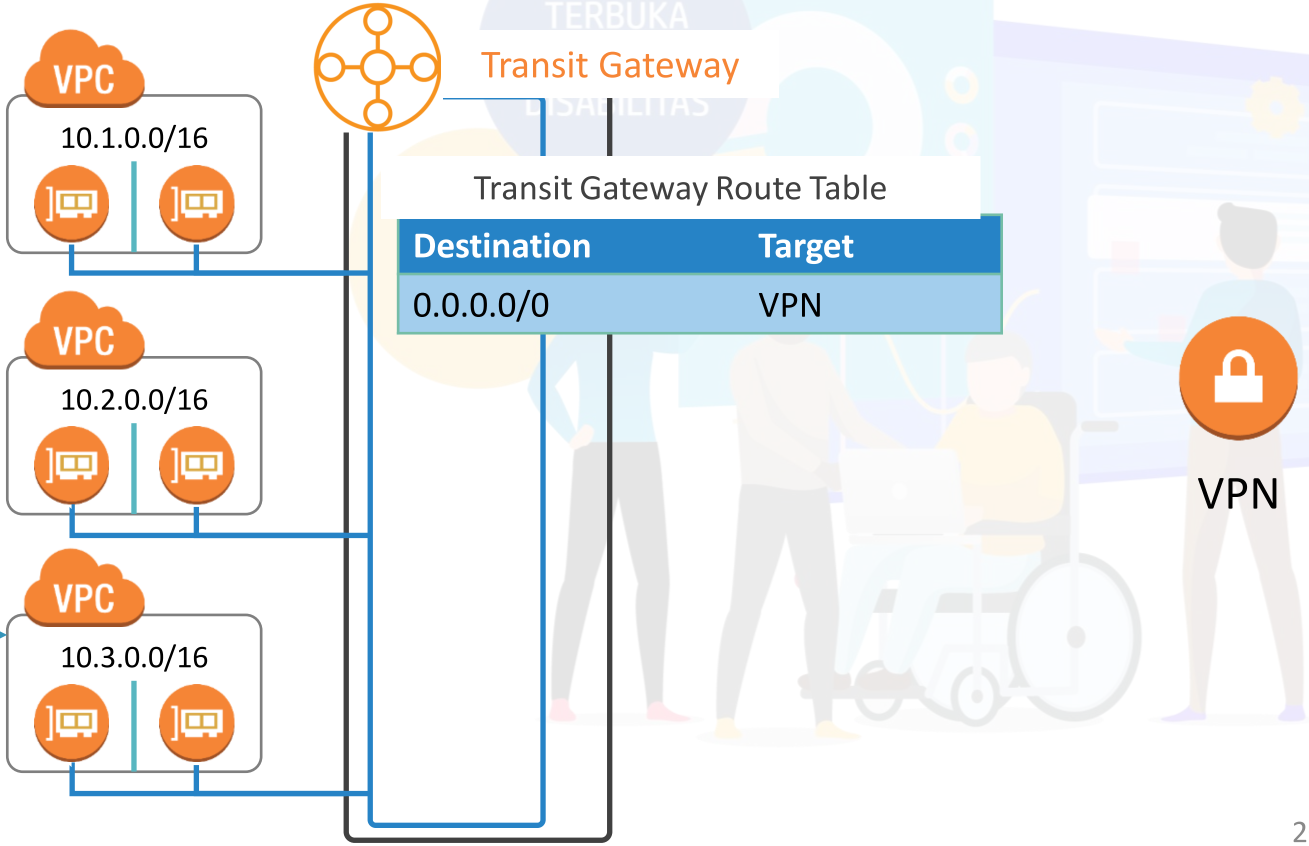


Transit Gateway Route Table

Destination	Target
10.1.0.0/16	vpc-att-1xxx
10.2.0.0/16	vpc-att-2xxx
10.3.0.0/16	vpc-att-3xxx

Transit Gateway in Action - Isolation

Scenario: We now want isolated connectivity and VPN access.



Transit Gateway Route Table

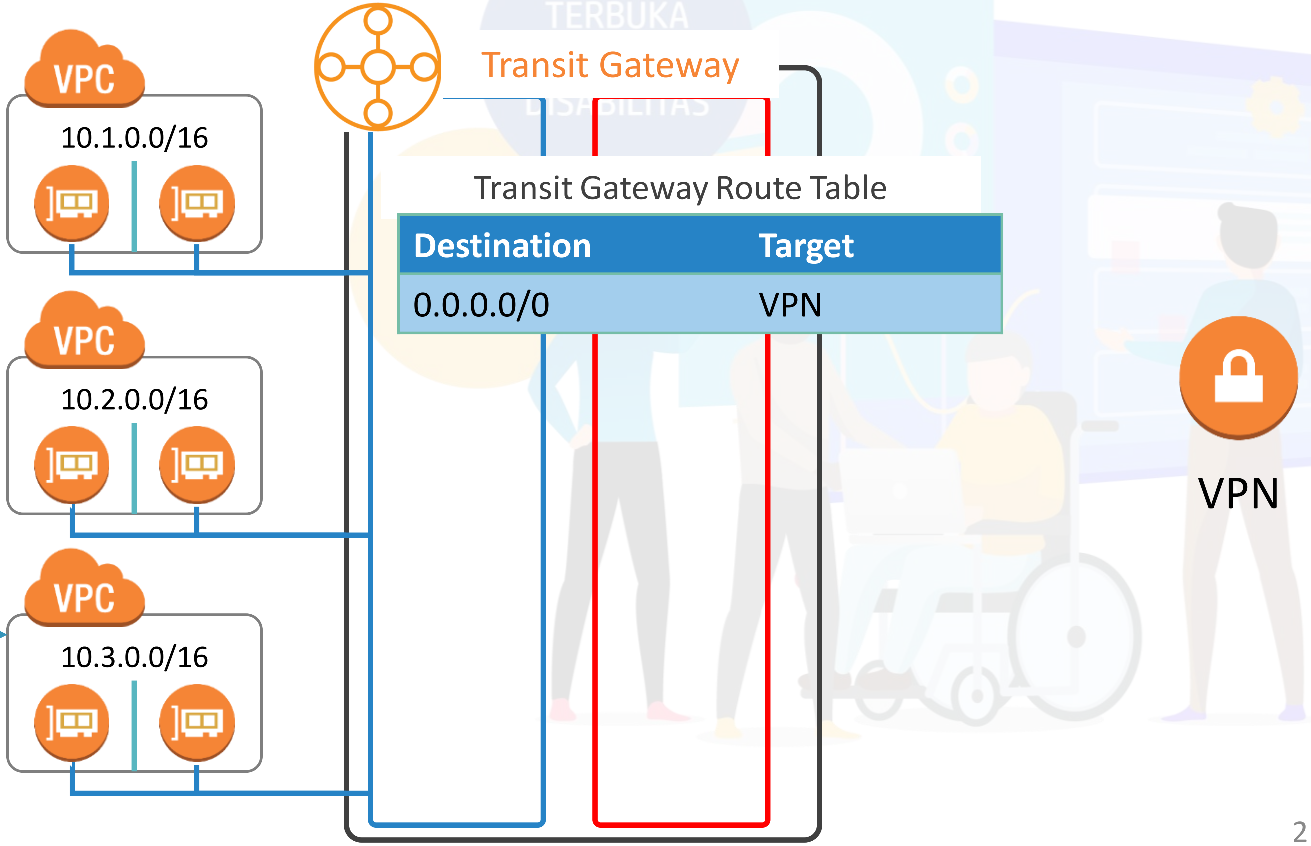
Destination	Target
0.0.0.0/0	VPN

Per VPC Route Table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx

Transit Gateway in Action - Isolation

Scenario: We now want isolated connectivity and VPN access.



Transit Gateway Route Table

Destination	Target
0.0.0.0/0	VPN

Per VPC Route Table

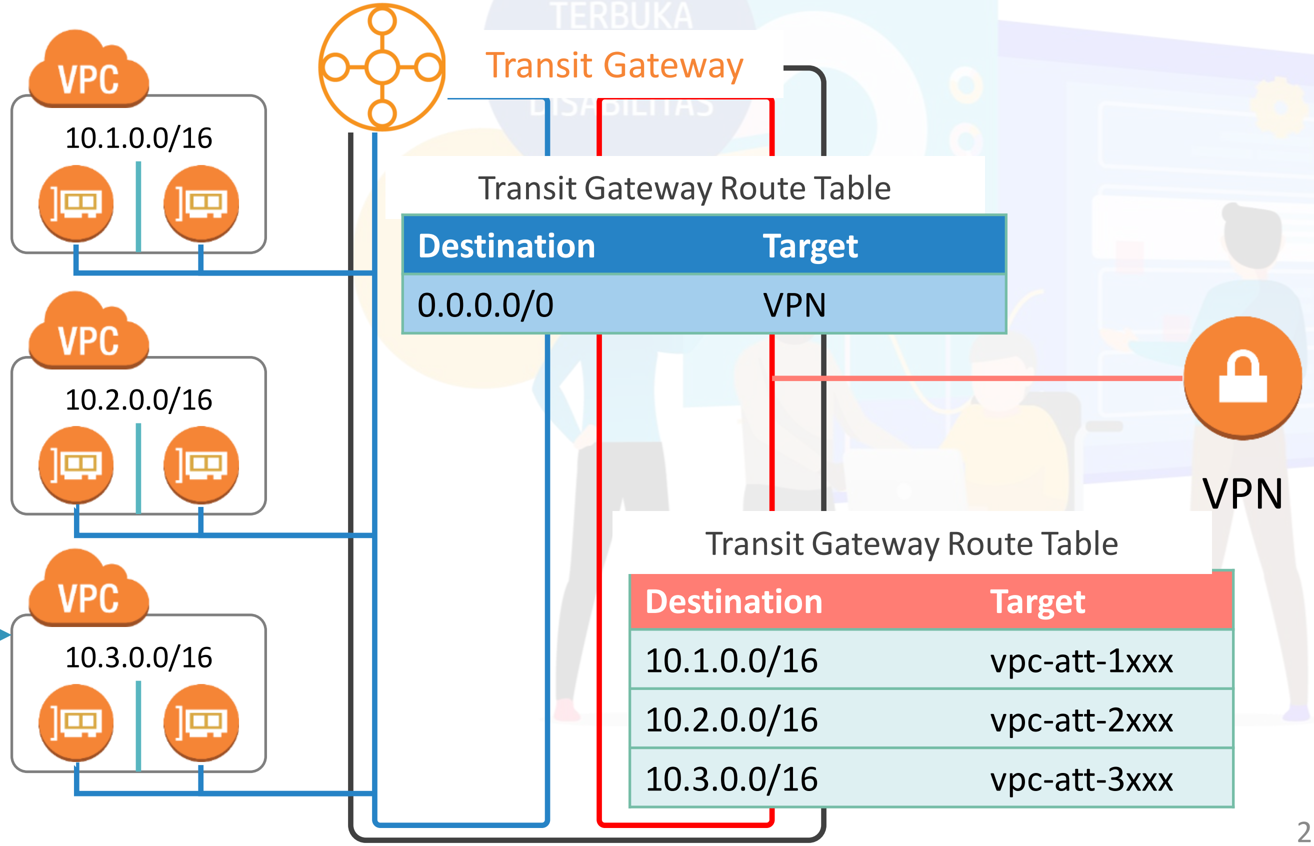
Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx

Transit Gateway in Action - Isolation

Scenario: We now want isolated connectivity and VPN access.

Per VPC Route Table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx



Transit Gateway Route Table

Destination	Target
0.0.0.0/0	VPN

Transit Gateway Route Table

Destination	Target
10.1.0.0/16	vpc-att-1xxx
10.2.0.0/16	vpc-att-2xxx
10.3.0.0/16	vpc-att-3xxx

VPC Endpoints

Privately connect your EC2 instances to services outside your VPC without leaving AWS.

Don't need to use an internet gateway, VPN, network address translation (NAT) devices, or firewall proxies.

- Does not require traversal over the internet
- Must be in the same region
- They are horizontally scaled, redundant, and highly available

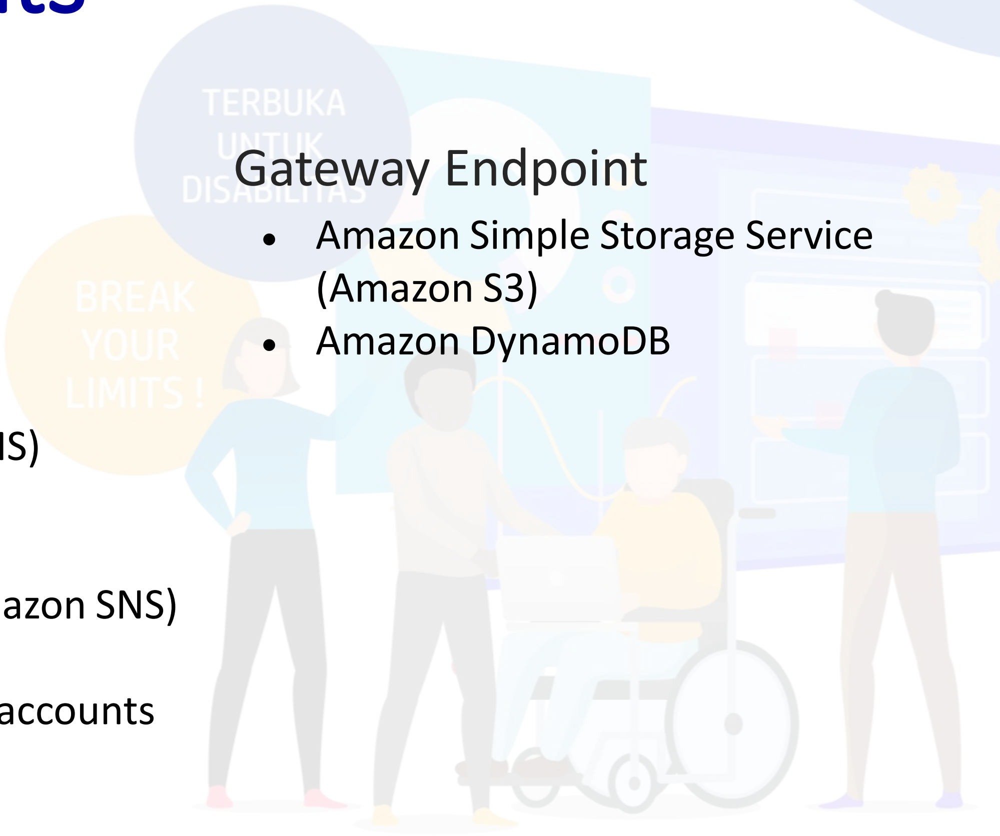
Two Types of Endpoints

Interface Endpoint

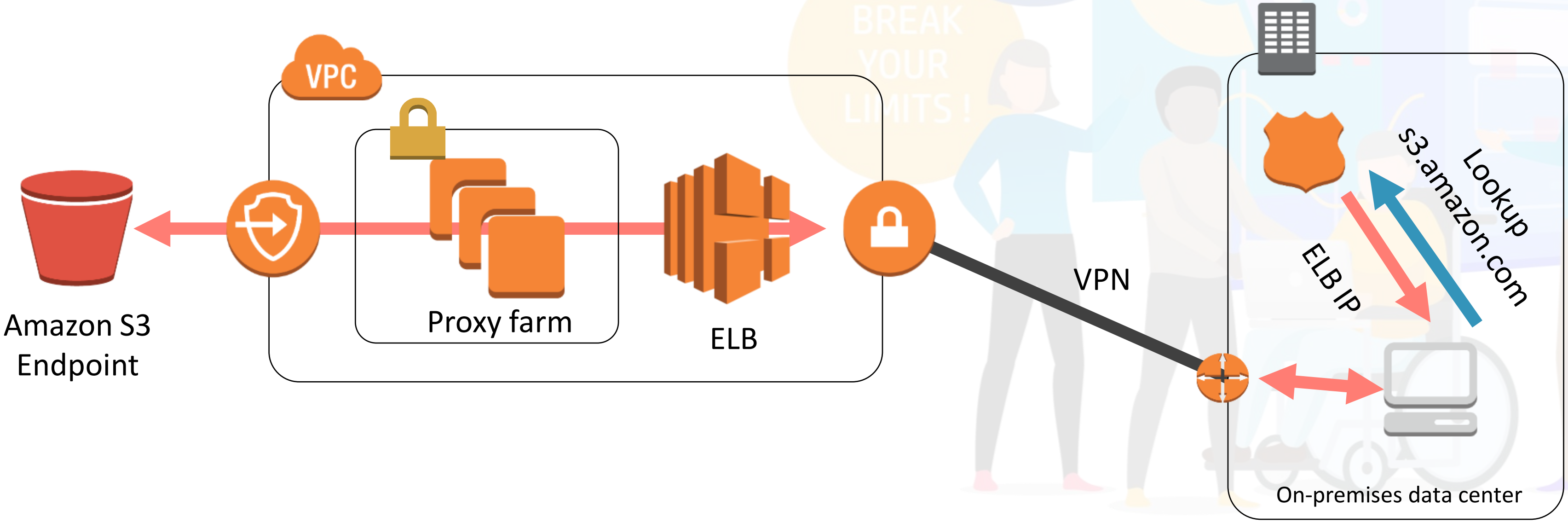
- Amazon CloudWatch Logs
- AWS CodeBuild
- Amazon EC2 API
- Elastic Load Balancing API
- AWS Key Management Service (AWS KMS)
- Amazon Kinesis Data Streams
- AWS Service Catalog
- Amazon Simple Notification Service (Amazon SNS)
- AWS Systems Manager
- Endpoint services hosted by other AWS accounts
- And MANY MORE!

Gateway Endpoint

- Amazon Simple Storage Service (Amazon S3)
- Amazon DynamoDB



Accessing VPC Endpoints from Outside the VPC



Follow our social media!

- digitalent.kominfo
- digitalent.kominfo
- DTS_kominfo
- Digital Talent Scholarship 2020

Pusat Pengembangan Profesi dan Sertifikasi
Badan Penelitian dan Pengembangan SDM
Kementerian Komunikasi dan Informatika
Jl. Medan Merdeka Barat No. 9
(Gd. Belakang Lt. 4 - 5)
Jakarta Pusat, 10110

digitalent.kominfo.go.id