Understanding AWS VPC Peering

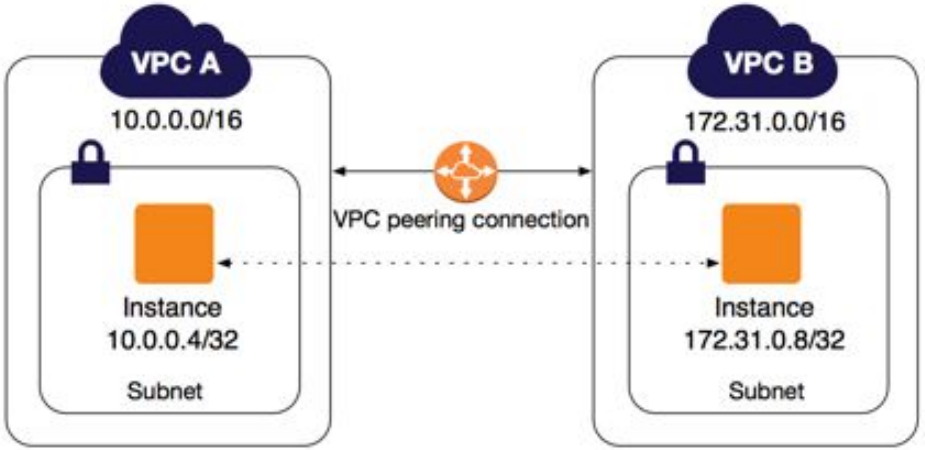
Features, Benefits, Scenarios, Limitations and unsupported configurations

www.awstrainingcenter.com

Inter VPC communication - VPC Peering

Features

- Enables private communication between 2 AWS VPCs
- Intra region and Inter region
- Across different AWS accounts
- Can connect single VPC to multiple VPCs
- There is no single point of failure for communication or a bandwidth bottleneck.



Benefits

- No need to have Internet gateway or VPN connection between VPCs.
- Saves VPN connection ($0.05/ hr) cost. You only pay in/out data transfer charges of $0.01/GB

VPC Peering Scenarios - 1

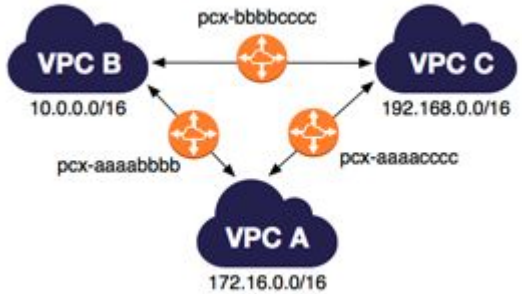
2 VPCs Peered together

Example:

You have different departments Finance, Accounting hosting machines into separate AWS VPCs. You can provide full access to all the resources from one VPC to another VPC and vice-a-versa

VPC Peering Scenarios - 2

3 VPCs Peered together

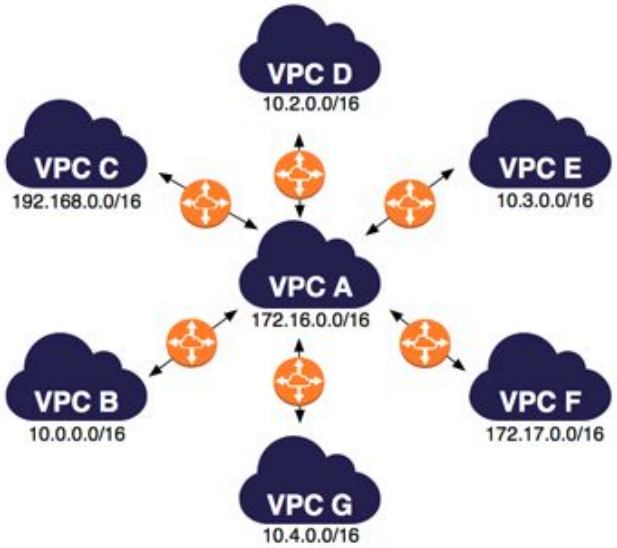


Example:

You have different office branches having separate VPCs in same of different AWS accounts and resources in these branches needs to access resources in all other branches

VPC Peering Scenarios - 3

Multiple VPCs Peered to single VPC (Spoke model)



Examples:

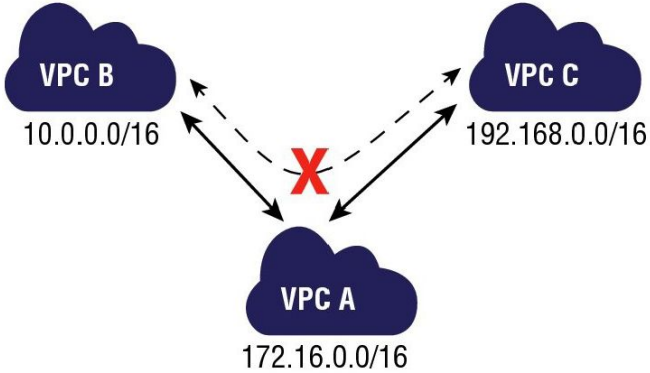
1. When you host a centralized services e.g File sharing, AD into one VPC and need to provide access to people or applications hosted into different VPCs
2. You offer SaaS service to customers having their own workloads into their AWS accounts. You can provide SaaS access to all customers making sure individual customers VPCs can not communicate with each other.
3. You have centralized Management VPC (e.g Chef server, Jenkins etc) and you have individual customer specific VPCs where you have hosted your single tenant services in each VPC. You can push your configurations as well as monitor health Infra and applications through management VPC.

VPC Peering Limitations

1. VPC CIDR's should be Non-overlapping

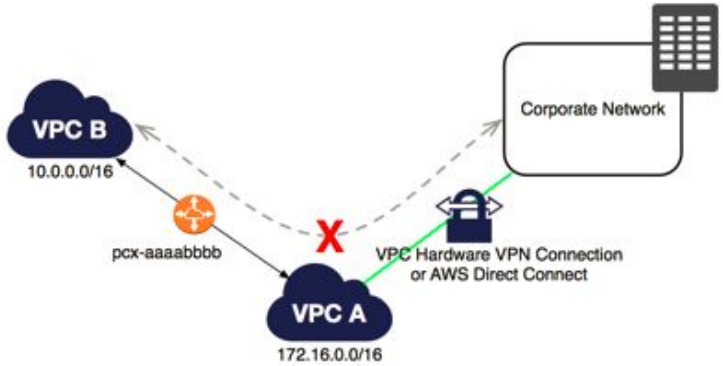
1. Only one peering between given 2 VPCs

1. Peering connection is **not transitive**

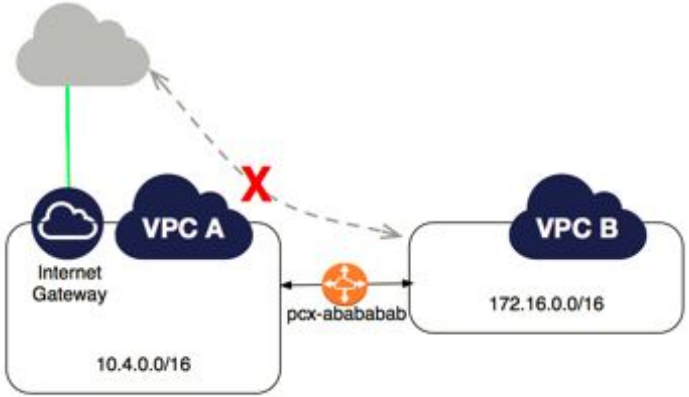


VPC Peering invalid scenarios

1. A VPN connection or an AWS Direct Connect connection to a corporate network

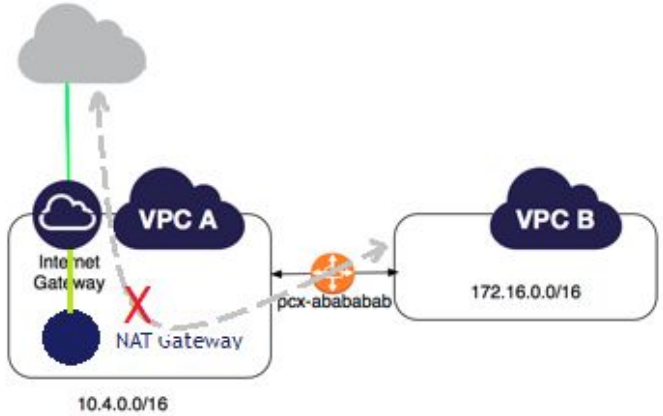


1. An internet access through an internet gateway



VPC Peering invalid scenarios

3. An internet access through a NAT device



4. A VPC endpoint to an AWS service (End

to Amazon S3, DynamoDB)