

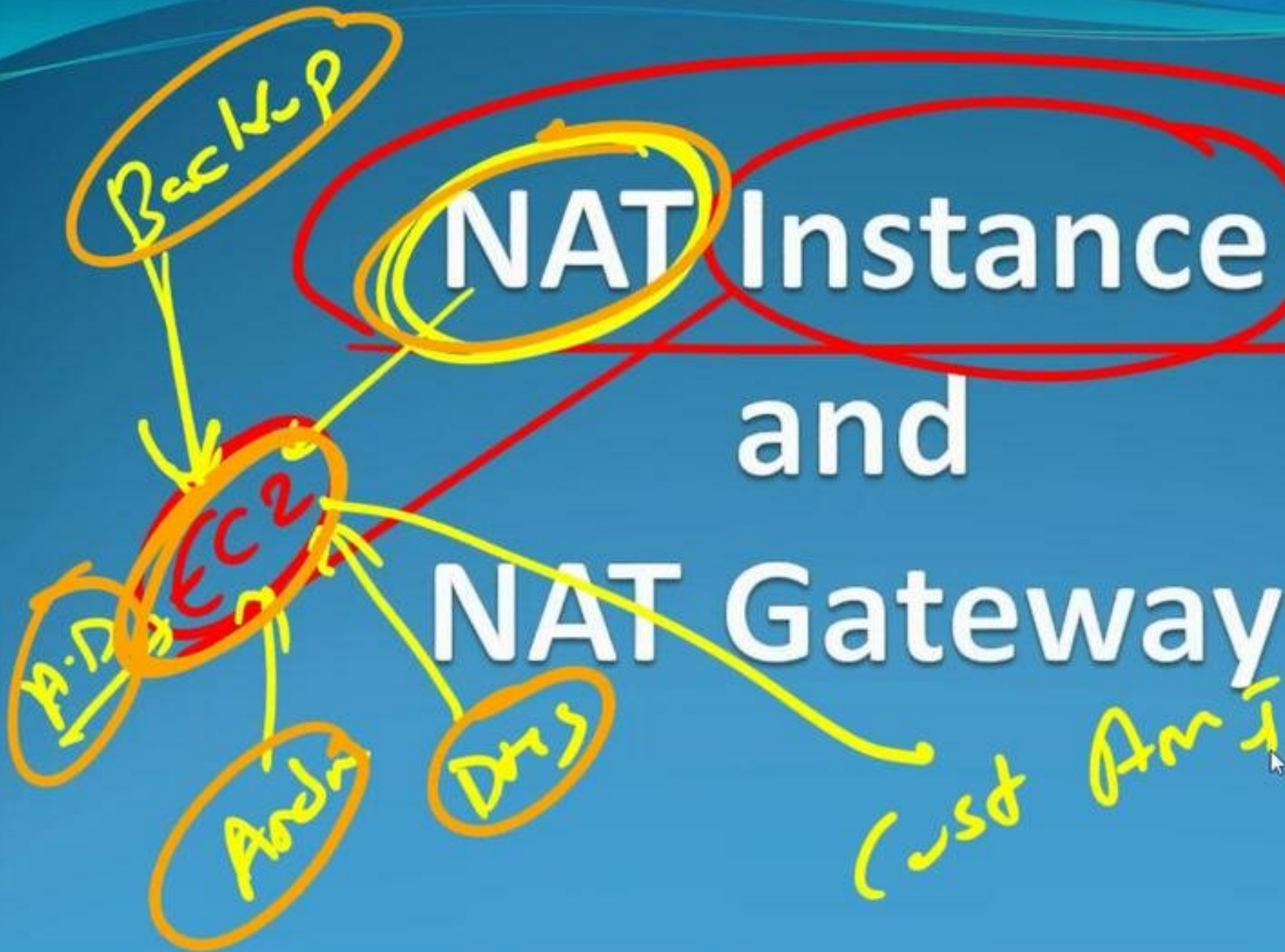
NAT Instance and NAT Gateway

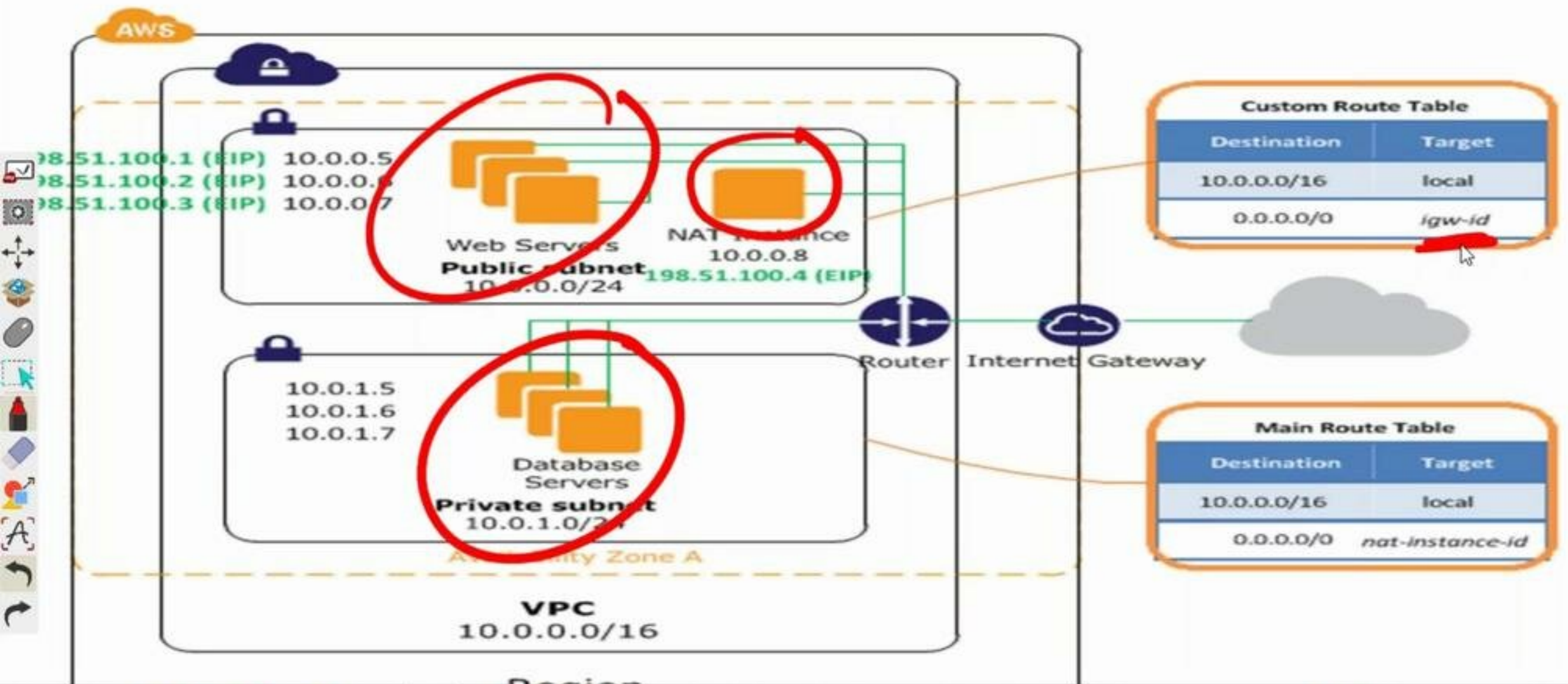


NAT Instance

and

NAT Gateway







- NAT instance allows private subnet EC2 instance to get to internet (Proxy)

Inbound: Receiving http/https request from Private Subnet

Outbound: Forwarding http/https request to Internet

- The NAT instance is configured in Public subnet
- NAT instance to be assigned to security group
- Source Destination check must be disabled

NAT Instance

- NAT instance allows private subnet EC2 instance to get to internet (Proxy)

Inbound: Receiving http/https request from Private Subnet

Outbound: Forwarding http/https request to Internet

- The NAT instance is configured in Public subnet
- NAT instance to be assigned to security group
- Source Destination check must be disabled

NAT Instance

- NAT instance allows private subnet EC2 instance to get to internet (Proxy)

Inbound: Receiving http/https request from Private Subnet

Outbound: Forwarding http/https request to Internet

- The NAT instance is configured in Public subnet
- NAT instance to be assigned to security group
- Source Destination check must be disabled



- NAT instance allows private subnet EC2 instance to get to internet (Proxy)

Inbound: Receiving http/https request from Private Subnet

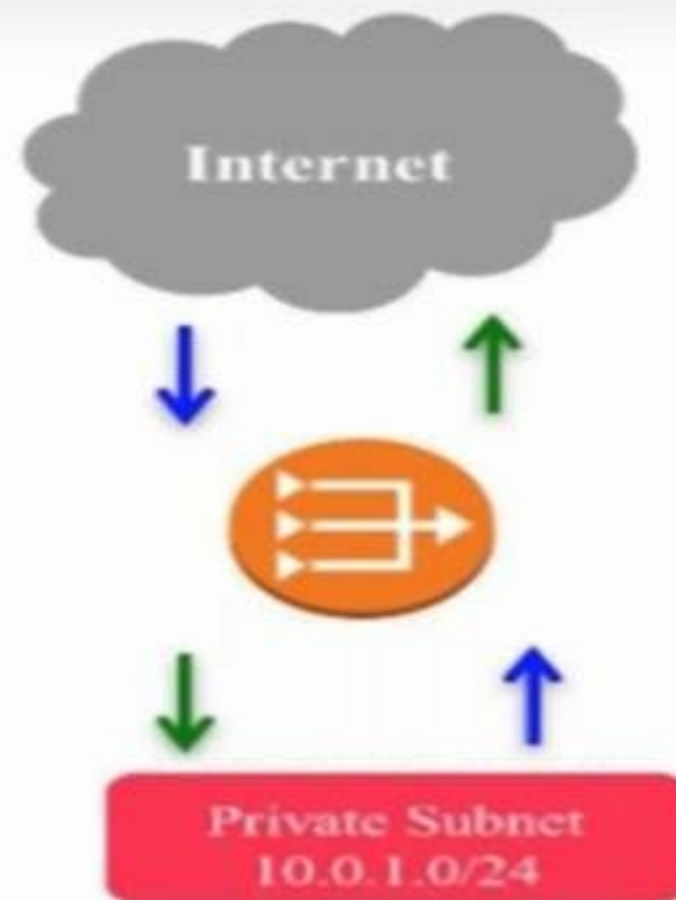
Outbound: Forwarding http/https request to Internet

- The NAT instance is configured in Public subnet
- NAT instance to be assigned to security group
- Source/Destination check must be disabled

NAT Gateway

Handwritten notes in blue and red ink on the left side of the slide. A red circle contains the text "EC2" with a checkmark. A blue circle contains the text "SG" with a checkmark. Another blue circle contains the text "NAT" with a checkmark. There are also some scribbles and arrows connecting these circles.

NAT Gateway



NAT Gateway

NAT Gateway

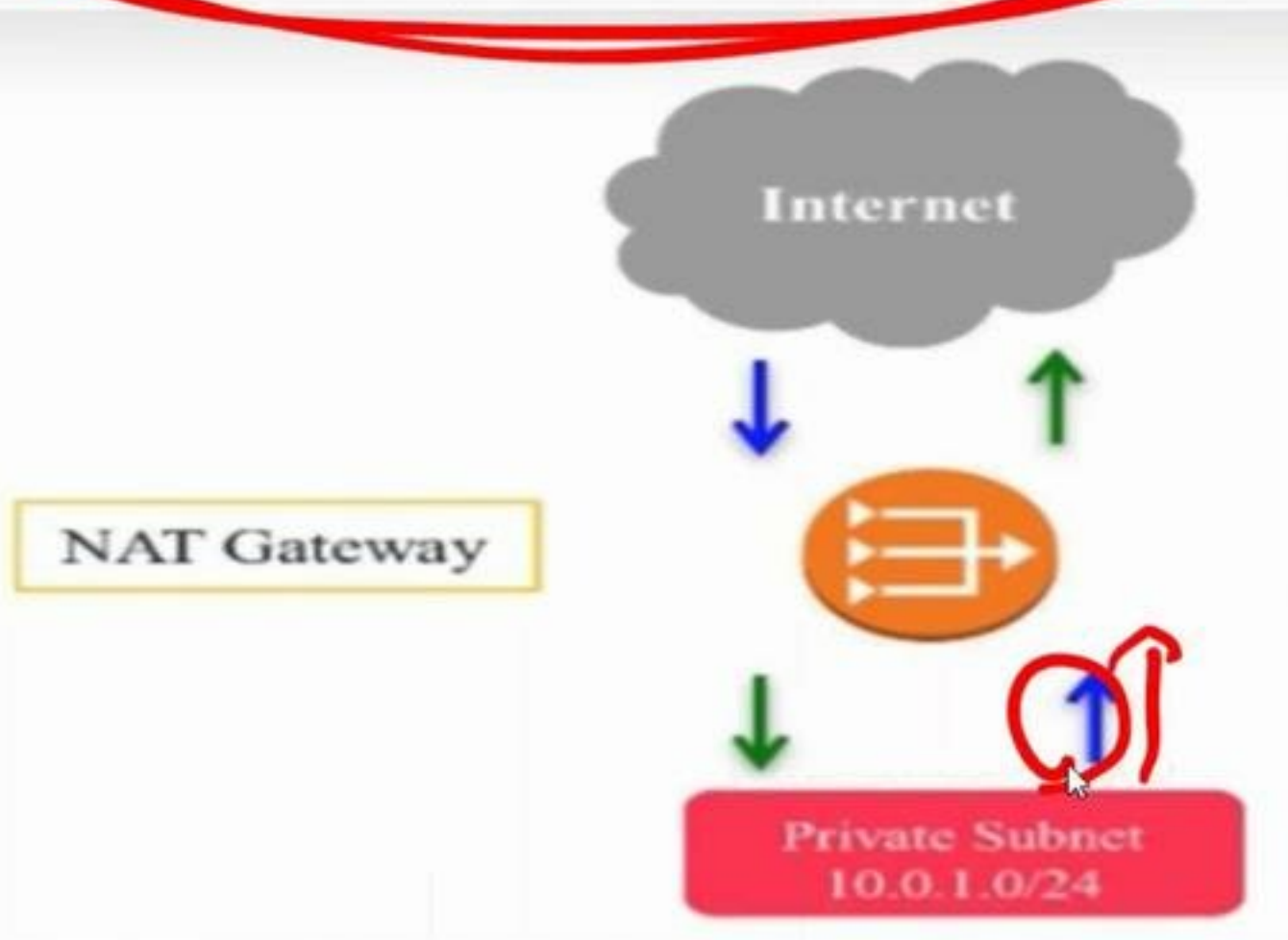
Internet

Private Subnet
10.0.1.0/24

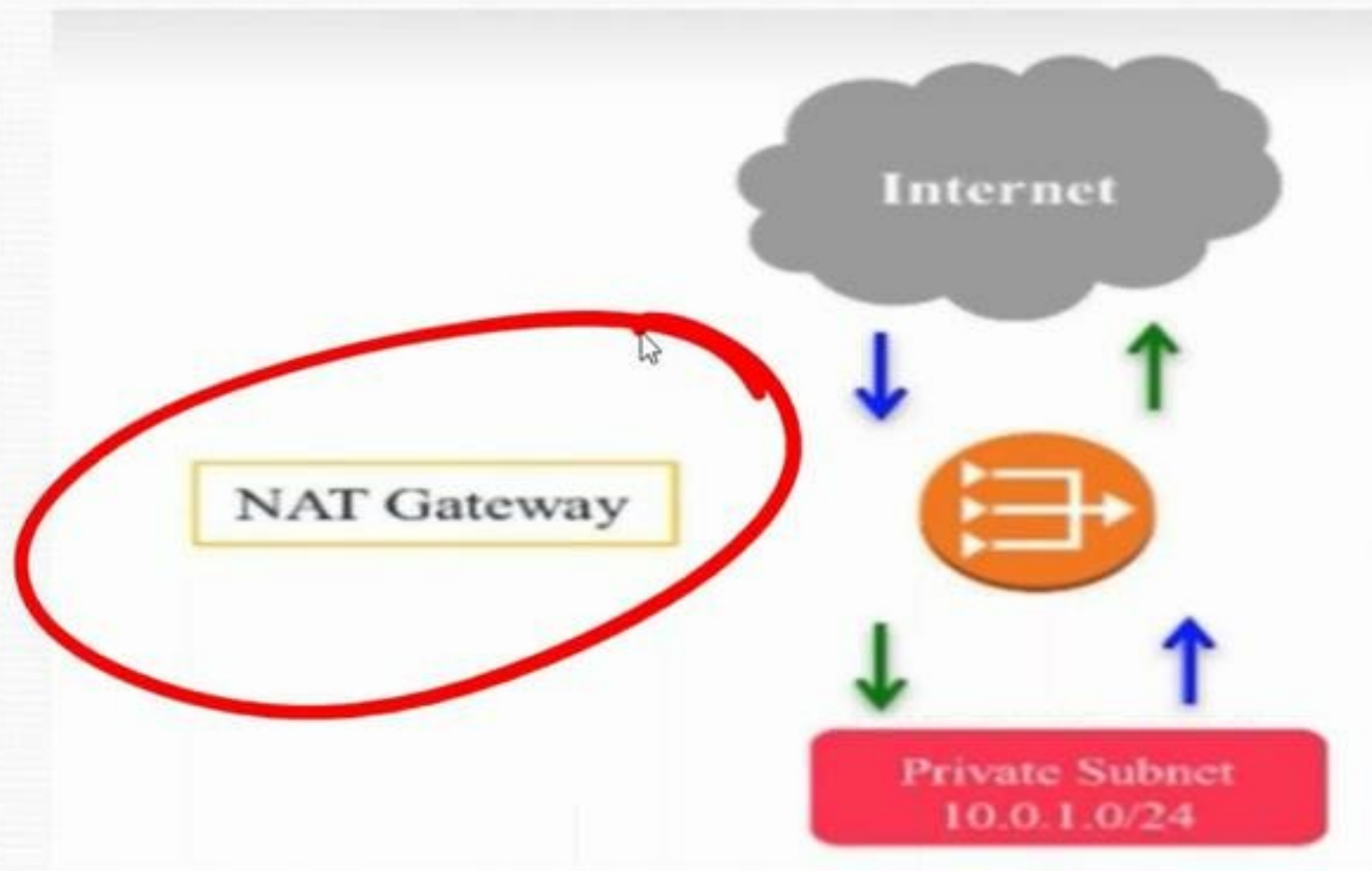


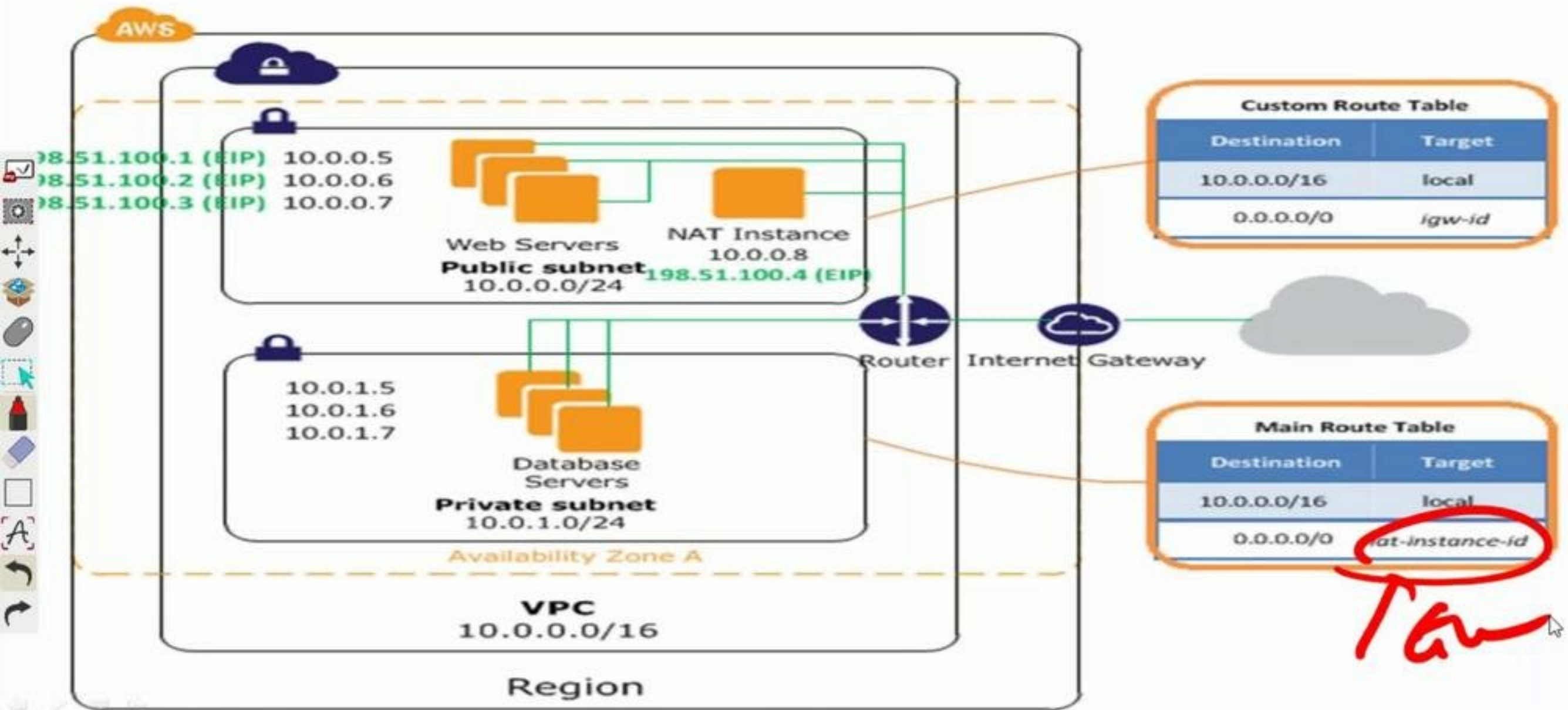
NAT Gateway

1055c



NAT Gateway





NAT Gateway

- Its AWS Managed Service
- NAT Gateway works only on Elastic IP Add
- Cannot be assigned to security Groups
- AWS responsible for security/Patching, etc

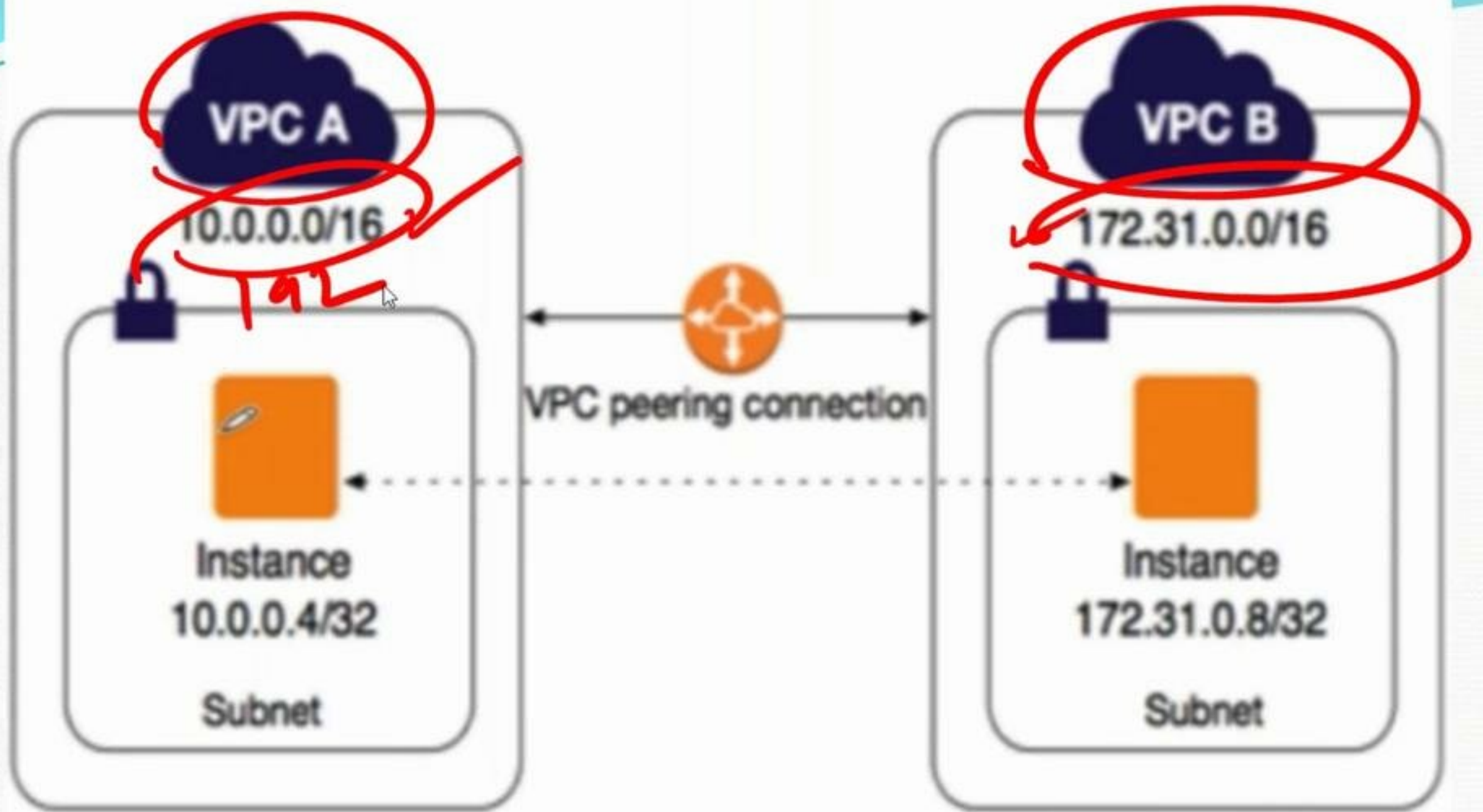


- Its AWS Managed Service
- NAT Gateway works only on Elastic IP Add
- Cannot be assigned to security Groups
- AWS responsible for security/Patching, etc

Plus Dumps

NAT Gateway

- Its AWS Managed Service
- NAT Gateway works only on Elastic IP Add
- Cannot be assigned to security Groups
- AWS responsible for security/Patching, etc



File Home Insert Design Transitions Animations Slide Show Review View Add-Ins

From Beginning From Current Slide Broadcast Slide Show Custom Slide Show Set Up Slide Show Hide Slide Rehearse Timings Record Slide Show Set Up

Play Narrations Use Timings Show Media Controls Resolution: 1360x768 Show On: Use Presenter View Monitors

Slides Outline

1 VPC Peering

VPC Peering

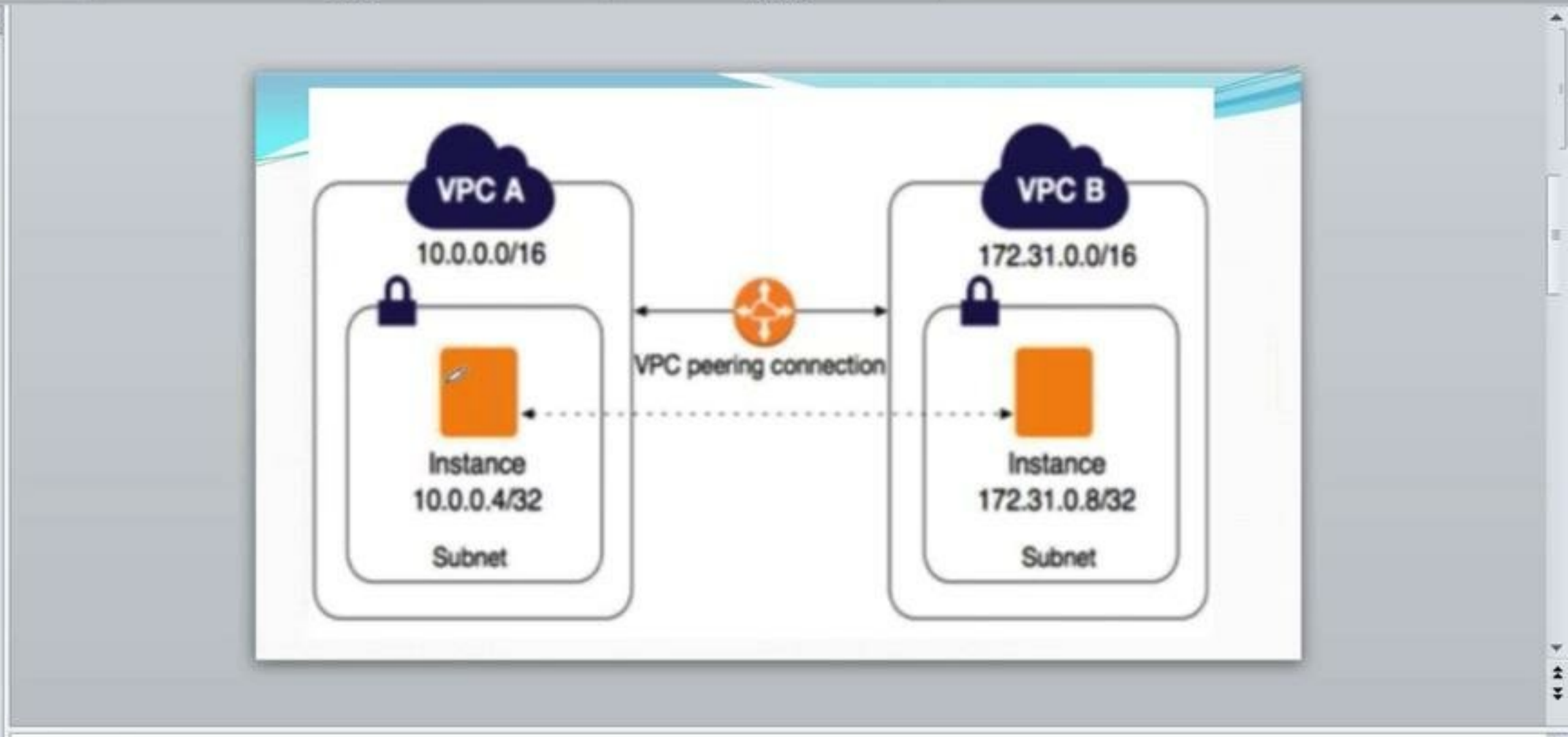
- VPC Peering is a network connection that enables two VPCs to communicate with each other (VPC to VPC).
- AWS uses the existing infrastructure of a VPC to create a VPC peering connection.

4 VPC Peering

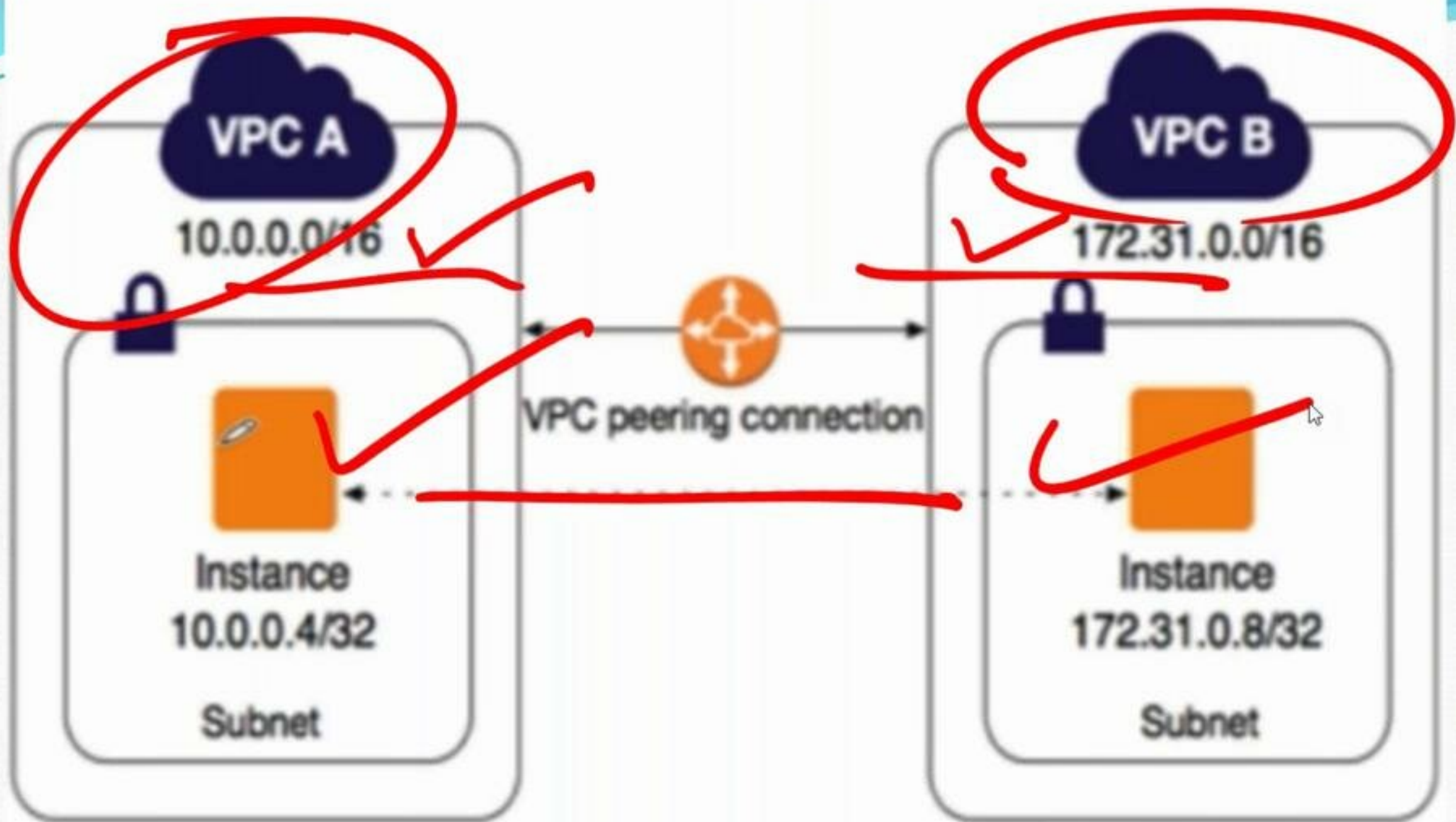
- There is no single point of failure for communication in a distributed network.
- It is a simple and cost-effective way to share resources between regions or replicate data for geographic redundancy across regions.

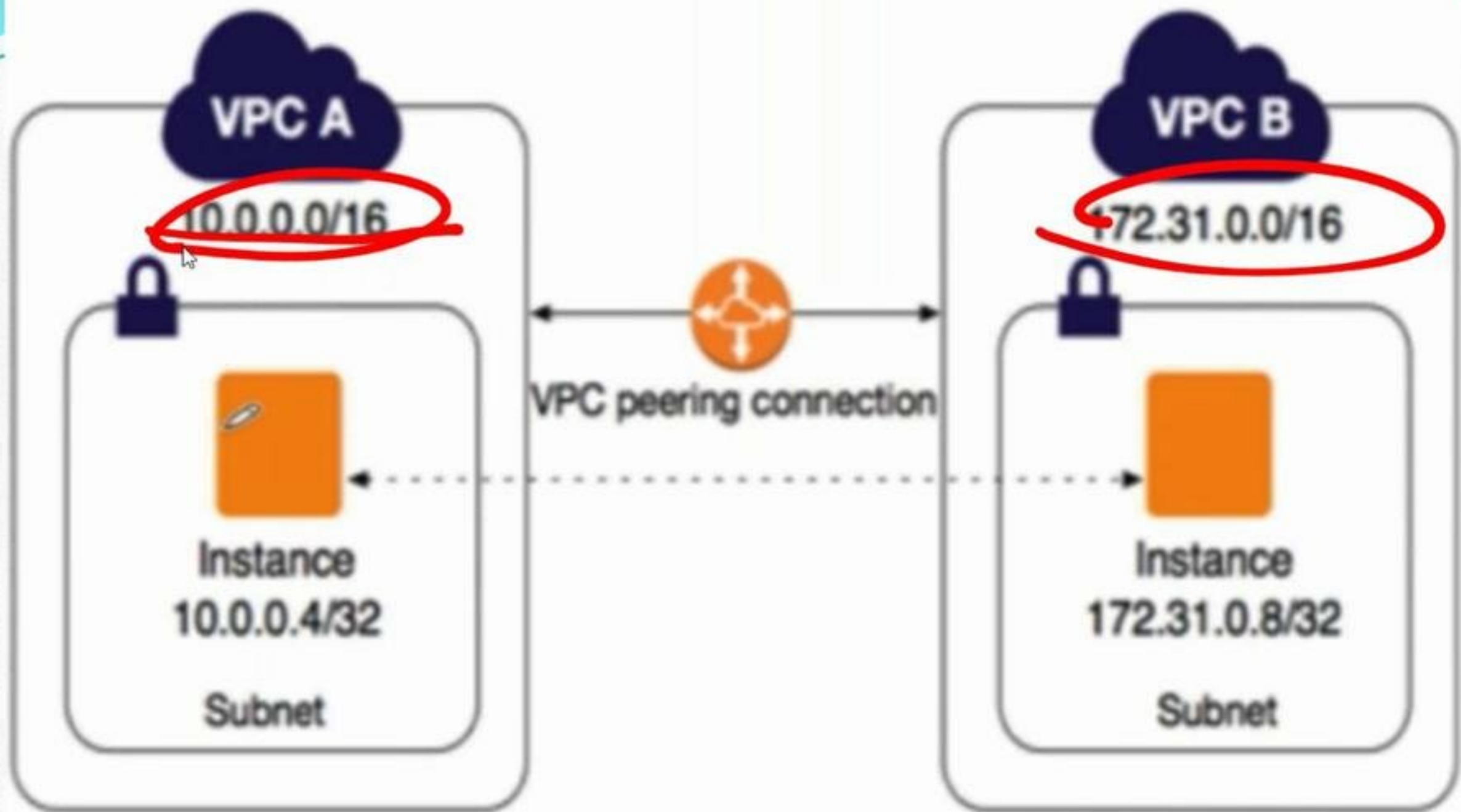
5 To establish a VPC peering connection

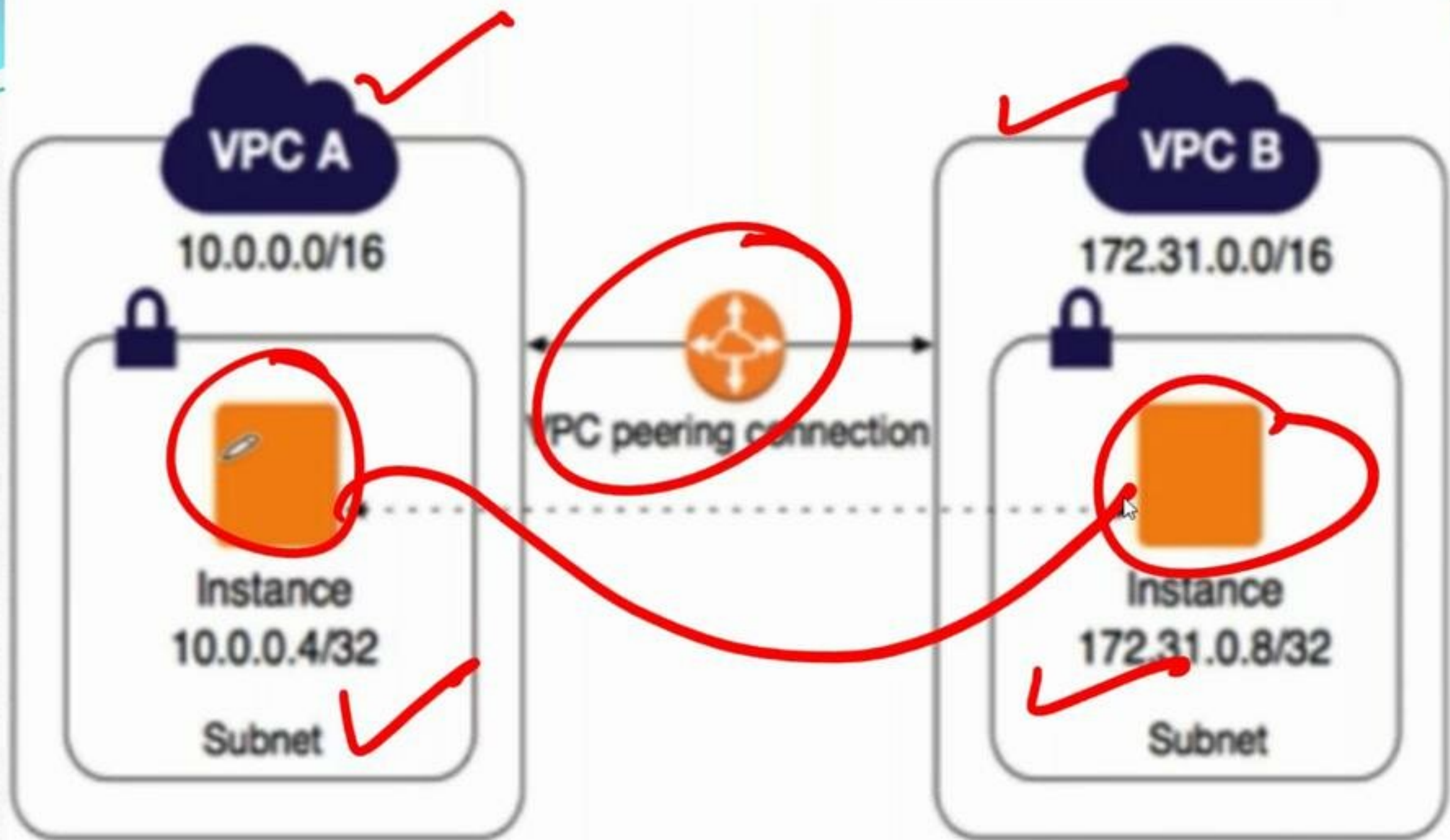
1. Peer VPCs across two CIDR blocks that overlap with regional VPC.
2. Add a route to one or more of your VPC's route tables that points to the IP address range of peer VPC.
3. Update the security group rules so that instances can communicate to and from peer VPC.



Click to add notes







VPC Peering

- VPC Peering is a network connection done between two VPC that enables to route traffic between them (Ipv4 or Ipv6)
- AWS uses the existing infrastructure of a VPC to create a VPC peering connection



VPC Peering

- VPC Peering is a network connection done between two VPC that enables to route traffic between them (Ipv4 or Ipv6)
- AWS uses the existing infrastructure of a VPC to create a VPC peering connection

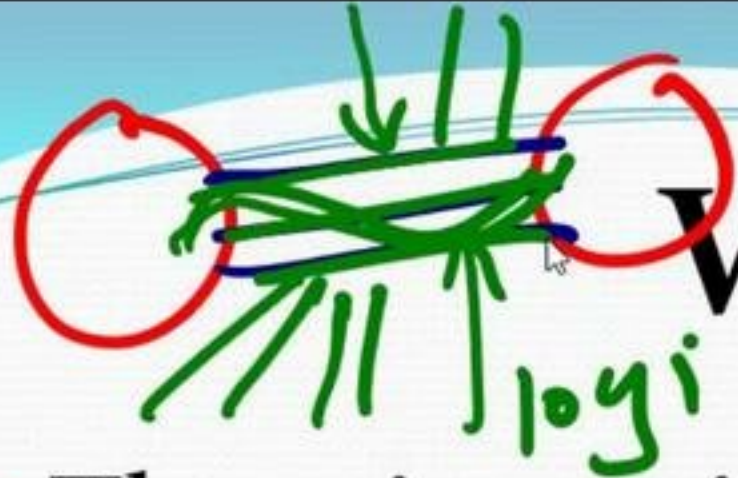


VPC Peering



- VPC Peering is a network connection done between two VPC that enables to route traffic between them (Ipv4 or Ipv6)
- AWS uses the existing infrastructure of a VPC to create a VPC peering connection






VPC Peering

- There is no single point of failure for communication or a bandwidth bottleneck
- It is simple and cost-effective way to share resources between regions or replicate data for geographic redundancy across regions



VPC Peering

- There is no single point of failure for communication or a bandwidth bottleneck
 - It is simple and cost-effective way to share resources between regions or replicate data for geographic redundancy across regions
- 

VPC Peering

- There is no single point of failure for communication or a bandwidth bottleneck
- It is simple and cost-effective way to share resources between regions or replicate data for geographic redundancy across regions



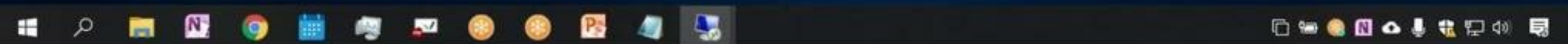
VPC Peering

- There is no single point of failure for communication or a bandwidth bottleneck
- It is simple and cost-effective way to share resources between regions or replicate data for geographic redundancy across regions



3.34.182.81

Hostname: EC2AMAZ-60R4VE2
Instance ID: i-0b90574e1a4a55cdc
Public IP Address: 3.34.182.81
Private IP Address: 172.31.14.208
Instance Size: t2.micro
Availability Zone: ap-northeast-2a
Architecture: AMD64
Total Memory: 1024 MB
Network Performance: Low to Moderate



3.34.182.81

Hostname: EC2AMAZ-60R4VE2
Instance ID: i-0b90574e1a4a55cdc
Public IP Address: 3.34.182.81
Private IP Address: 172.31.14.208
Instance Size: t2.micro
Availability Zone: ap-northeast-2a
Architecture: AMD64

*Untitled - Notepad

File Edit Format View Help

SEOUL

3.34.182.81

172.31.14.208

MUMBAI

52.66.201.19

192.168.1.113

Ln 12, Col 14 100% Windows (CRLF) UTF-8




Recycle Bin

3.34.182.81



Filters

Best match

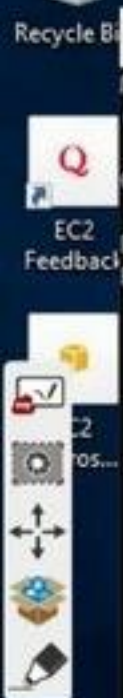
 **Command Prompt**
Desktop app

Settings

☐ Replace Command Prompt with Windows PowerShell when using Windows + X menu

cmd

Hostname: EC2AMAZ-60R4VE2
Instance ID: i-0b90574e1a4a55cdc
Public IP Address: 3.34.182.81
Private IP Address: 172.31.14.208
Instance Size: t2.micro
Availability Zone: ap-northeast-2a
Architecture: AMD64
Total Memory: 1024 MB
Network Performance: Low to Moderate



```
Administrator: Command Prompt - ping 192.168.1.113 -t
Microsoft Windows [Version 10.0.17763.2114]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ping 192.168.1.113 -t
Pinging 192.168.1.113 with 32 bytes of data:
```

Hostname: EC2AMAZ-60R4VE2
Instance ID: i-0b90574e1a4a55cdc
Public IP Address: 3.34.182.81
Private IP Address: 172.31.14.208
Instance Size: t2.micro
Availability Zone: ap-northeast-2a
Architecture: AMD64
Total Memory: 1024 MB
Network Performance: Low to Moderate

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.2114]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 172.31.14.208 -t
```

Hostname: EC2AMAZ-PJ2MB2F
Instance ID: i-087d16c93b20748a3
Public IP Address: 52.66.201.19
Private IP Address: 192.168.1.113
Instance Size: t2.micro
Availability Zone: ap-south-1a
Architecture: AMD64
Total Memory: 1024 MB
Network Performance: Low to Moderate





Hostname: EC2AMAZ-PJ2MB2F
Instance ID: i-087d16c93b20748a3
Public IP Address: 52.66.201.19
Private IP Address: 192.168.1.113
Instance Size: t2.micro
Availability Zone: ap-south-1a
Architecture: AMD64
Total Memory: 1024 MB
Network Performance: Low to Moderate

```
Administrator: Command Prompt - ping 172.31.14.208 -t
Microsoft Windows [Version 10.0.17763.2114]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 172.31.14.208 -t

Pinging 172.31.14.208 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 172.31.14.208:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\Users\Administrator>ping 172.31.14.208 -t

Pinging 172.31.14.208 with 32 bytes of data:
-
```



Recycle Bin

52.66.201.19



Filters

Best match

Windows Defender Firewall
Control panel

Settings

Check firewall status

Allow an app through Windows Firewall

Firewall & network protection

Security at a glance

Apps

Windows Defender Firewall with Advanced Security

firewall

Hostname: EC2AMAZ-PJ2MB2F
Instance ID: i-087d16c93b20748a3
Public IP Address: 52.66.201.19
Private IP Address: 192.168.1.113
Instance Size: t2.micro
Availability Zone: ap-south-1a
Architecture: AMD64
Total Memory: 1024 MB
Network Performance: Low to Moderate

AWS L3.3 Peering 5.Days - Microsoft PowerPoint

File Home Insert Design Transitions Animations Slide Show Review View Add-Ins

From Beginning From Current Slide Broadcast Slide Show Custom Slide Show Set Up Slide Show Hide Slide Rehearse Timings Record Slide Show Set Up Play Narrations Use Timings Show Media Controls Resolution: 1360x768 Show On: Use Presenter View Monitors

Slides Outline

1 VPC Peering

2 VPC Peering

3 VPC Peering

4 VPC Peering

5 To establish a VPC-peering Connection

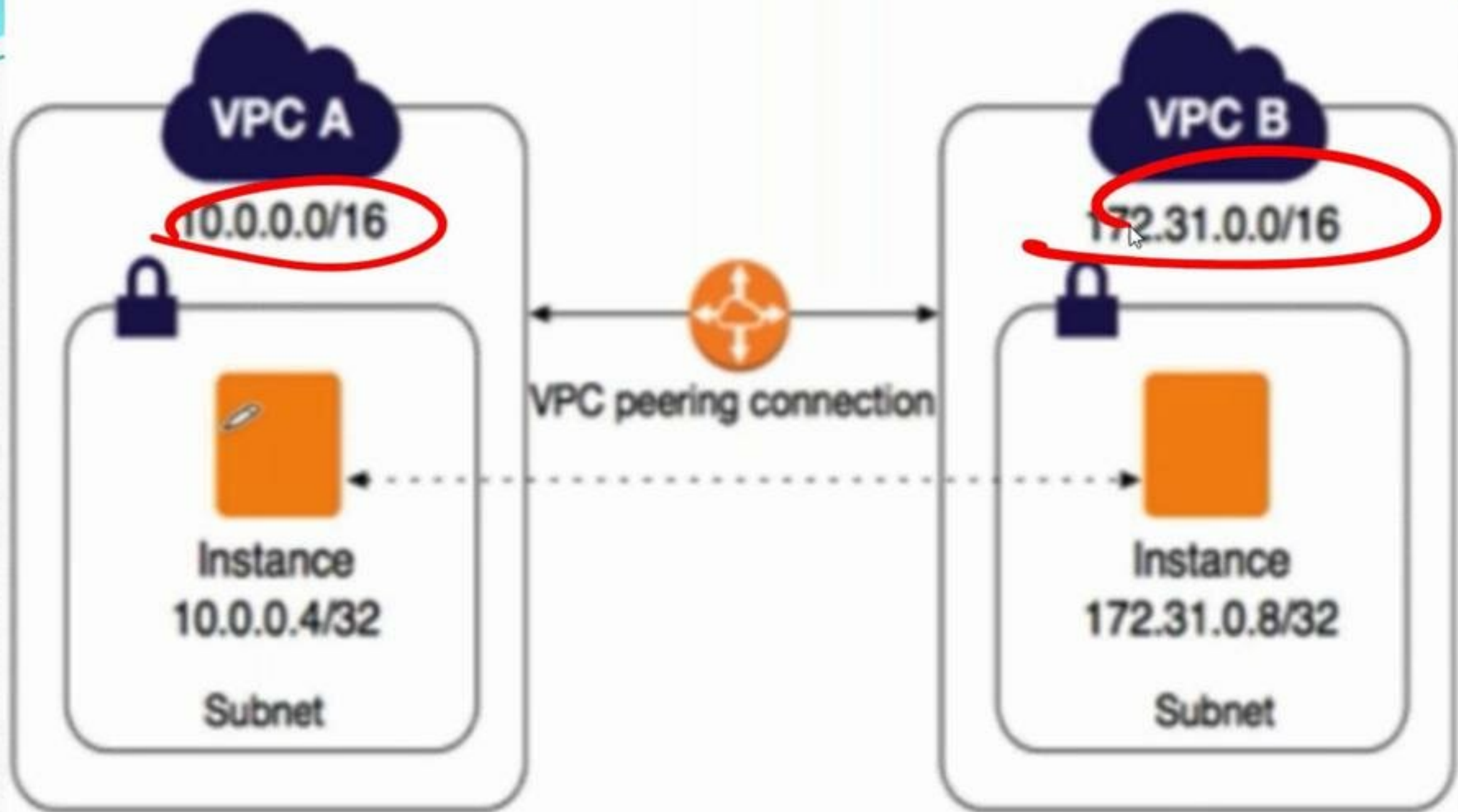
VPC Peering

- There is no single point of failure for communication or a bandwidth bottleneck
- It is simple and cost-effective way to share resources between regions or replicate data for geographic redundancy across regions

Click to add notes

Slide 4 of 5 "Flow" English (India) 80%

Windows taskbar icons: File Explorer, Microsoft Edge, PowerPoint, etc.



To establish a VPC-peering Connections

- ☒ Peer VPC cannot have CIDR block that overlaps with requester VPC
- ☒ Add a route to one or more of Your VPC's Route tables that points to the IP address range of peer VPC
- ☒ Update the security group rules so that instance can communicate to and from peer VPC

To establish a VPC-peering Connections

- ☐ Peer VPC cannot have CIDR block that overlaps with requester VPC
- ☐ Add a route to one or more of Your VPC's Route tables that points to the IP address range of peer VPC
- ☐ Update the security group rules so that instance can communicate to and from peer VPC