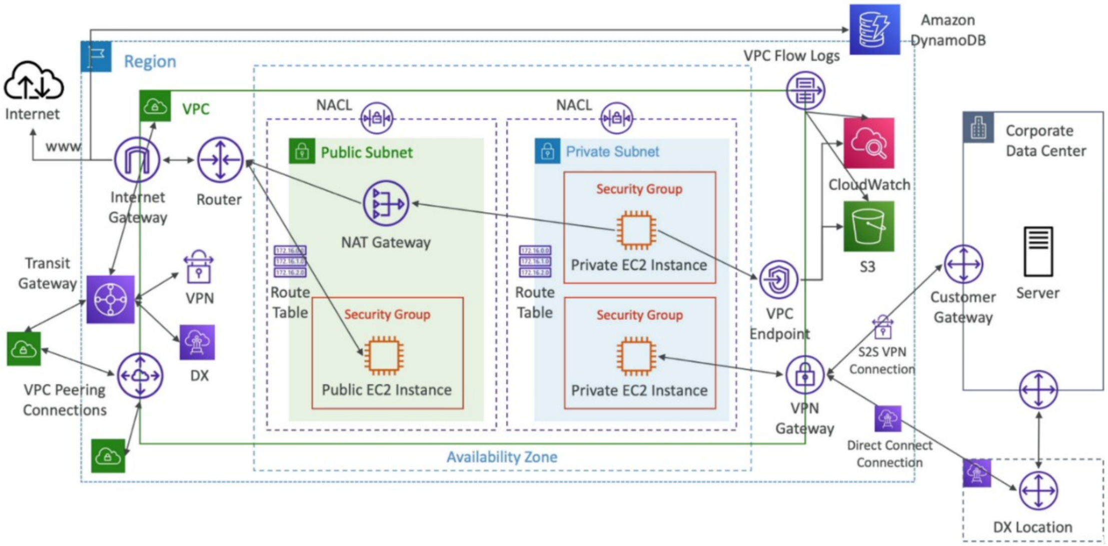
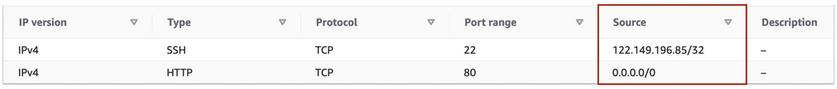
VPC (Virtual Private Cloud) Diagram



Understanding CIDR – IP4

- Classless Inter-Domain Routing – a method for allocating IP addresses
- Used in Security Groups rules and AWS networking in general



IP version	Type	Protocol	Port range	Source	Description
IPv4	SSH	TCP	22	122.149.196.85/32	–
IPv4	HTTP	TCP	80	0.0.0.0/0	–

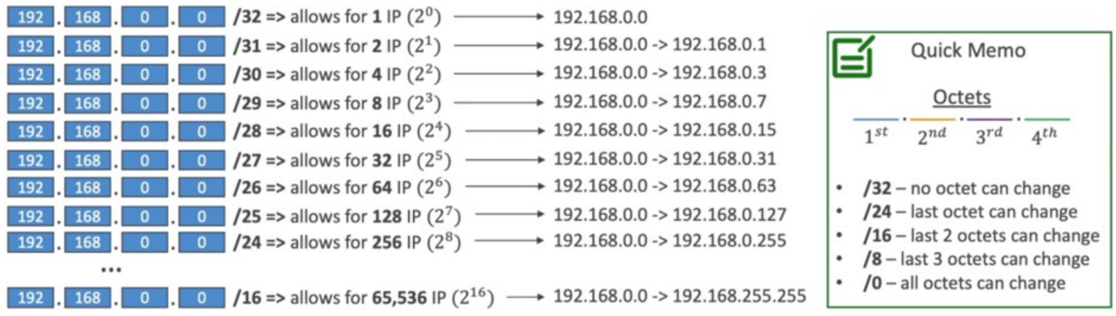
- They help to define an IP address range:
  - We've seen WW.XX.YY.ZZ/32 => one IP
  - We've seen 0.0.0.0/0 => all IPs
  - But we can define:192.168.0.0/26 =>192.168.0.0 – 192.168.0.63 (64 IP addresses)

- A CIDR consists of two components
- Base IP
  - Represents an IP contained in the range (XX.XX.XX.XX)
  - Example: 10.0.0.0, 192.168.0.0, …

- Subnet Mask
  - Defines how many bits can change in the IP
  - Example: /0, /24, /32
  - Can take two forms:
    - /8 ⇔ 255.0.0.0
    - /16 ⇔ 255.255.0.0
    - /24 ⇔ 255.255.255.0
    - /32 ⇔ 255.255.255.255

Understanding CIDR – Subnet Mask

- The Subnet Mask basically allows part of the underlying IP to get additional next values from the base IP



192.168.0.0 /32 => allows for **1** IP (2^{0}) → 192.168.0.0

192.168.0.0 /31 => allows for **2** IP (2^{1}) → 192.168.0.0 -> 192.168.0.1

192.168.0.0 /30 => allows for **4** IP (2^{2}) → 192.168.0.0 -> 192.168.0.3

192.168.0.0 /29 => allows for **8** IP (2^{3}) → 192.168.0.0 -> 192.168.0.7

192.168.0.0 /28 => allows for **16** IP (2^{4}) → 192.168.0.0 -> 192.168.0.15

192.168.0.0 /27 => allows for **32** IP (2^{5}) → 192.168.0.0 -> 192.168.0.31

192.168.0.0 /26 => allows for **64** IP (2^{6}) → 192.168.0.0 -> 192.168.0.63

192.168.0.0 /25 => allows for **128** IP (2^{7}) → 192.168.0.0 -> 192.168.0.127

192.168.0.0 /24 => allows for **256** IP (2^{8}) → 192.168.0.0 -> 192.168.0.255

...

192.168.0.0 /16 => allows for **65,536** IP (2^{16}) → 192.168.0.0 -> 192.168.255.255

Quick Memo

Octets

1^{st} . 2^{nd} . 3^{rd} . 4^{th}

- **/32** – no octet can change
- **/24** – last octet can change
- **/16** – last 2 octets can change
- **/8** – last 3 octets can change
- **/0** – all octets can change

Understanding CIDR – Little Experience

- 192.168.0.0/24 = … ?
  - 192.168.0.0 – 192.168.0.255 (256 IPs)
- 192.168.0.0/16 = … ?
  - 192.168.0.0 – 192.168.255.255 (65,536 IPs)
- 134.56.78.123/32 = … ?
  - Just 134.56.78.123
- 0.0.0.0/0
  - All IPs!

When in doubt we use this website
https://www.ipaddressguide.com/cidr

Public vs Private IP4

- The Internet Assigned Numbers Authority (IANA) established certain blocks of IPv4 addresses for the use of private (LAN) and public (Internet) addresses

- Private IP can only allow certain values:
  - 10.0.0.0 – 10.255.255.255 (10.0.0.0/8) ← in big networks
  - 172.16.0.0 – 172.31.255.255 (172.16.0.0/12) ← AWS default VPC in that range
  - 192.168.0.0 – 192.168.255.255 (192.168.0.0/16) ← e.g., home networks

- All the rest of the IP addresses on the Internet are Public

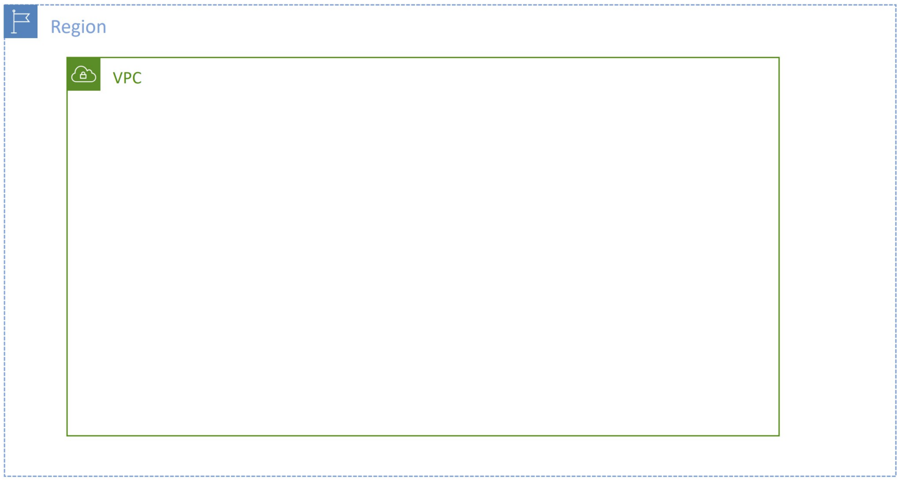
Default VPC walkthrough

- All new AWS accounts have a default VPC
- New EC2 instances are launched into the default VPC if no subnet is specified
- Default VPC has Internet connectivity and all EC2 instances inside it have public IPv4 addresses
- We also get a public and a private IPv4 DNS names

VPC in AWS – IP4

- VPC = Virtual Private Cloud
- You can have multiple VPCs in an AWS region (max. 5 per region – soft limit)
- Max. CIDR per VPC is 5, for each CIDR:
  - Min. size is /28 (16 IP addresses)
  - Max. size is /16 (65536 IP addresses)
- Because VPC is private, only the Private IPv4 ranges are allowed:
  - 10.0.0.0 – 10.255.255.255 (10.0.0.0/8)
  - 172.16.0.0 – 172.31.255.255 (172.16.0.0/12)
  - 192.168.0.0 – 192.168.255.255 (192.168.0.0/16)
- Your VPC CIDR should NOT overlap with your other networks (e.g., corporate)

State on hands-on

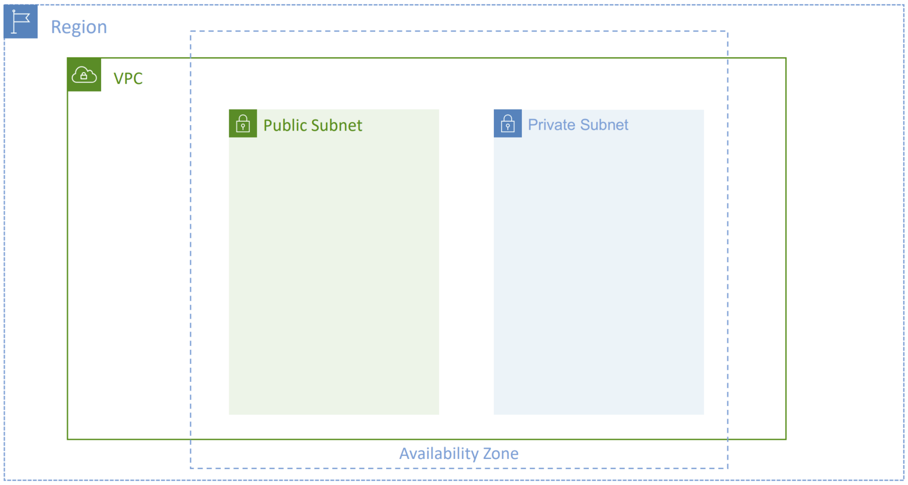


VPC – Subnet IP4

- AWS reserves **5 IP addresses (first 4 & last 1)** in each subnet
- These 5 IP addresses are not available for use and can't be assigned to an EC2 instance
- Example: if CIDR block 10.0.0.0/24, then reserved IP addresses are:
  - **10.0.0.0** – Network Address
  - **10.0.0.1** – reserved by AWS for the VPC router
  - **10.0.0.2** – reserved by AWS for mapping to Amazon-provided DNS
  - **10.0.0.3** – reserved by AWS for future use
  - **10.0.0.255** – Network Broadcast Address. AWS does not support broadcast in a VPC, therefore the address is reserved

- Exam Tip, if you need 29 IP addresses for EC2 instances:
  - You can't choose a subnet of size /27 (32 IP addresses, 32 – 5 = 27 < 29)
  - You need to choose a subnet of size /26 (64 IP addresses, 64 – 5 = 59 > 29)

Adding subnets

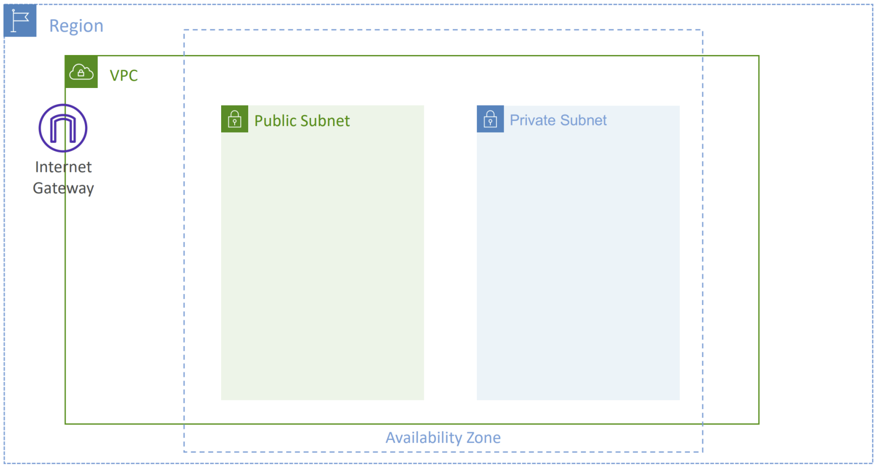


VPC – Internet Gateway (IGW)

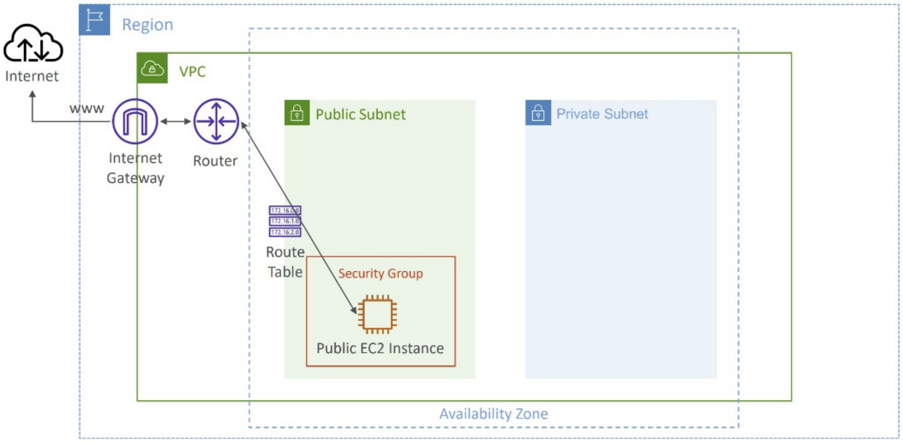
- Allows resources (e.g., EC2 instances) in a VPC connect to the Internet
- It scales horizontally and is highly available and redundant
- Must be created separately from a VPC
- One VPC can only be attached to one IGW and vice versa

- Internet Gateways on their own do not allow Internet access…
- Route tables must also be edited!

VPC – Adding Internet Gateway (IGW)

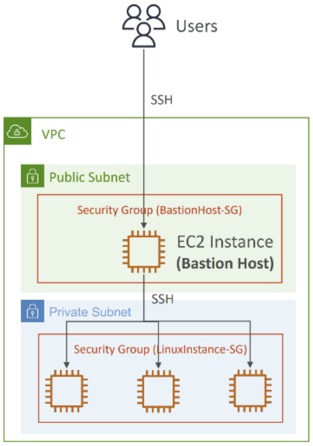


VPC – Editing Route tables.



Bastion Host

- We can use a Bastion Host to SSH into our private EC2 instances
- The bastion is in the public subnet which is then connected to all other private subnets
- Bastion Host security group must allow inbound from the internet on port 22 from restricted CIDR, for example the public CIDR of your corporation
- Security Group of the EC2 Instances must allow the Security Group of the Bastion Host, or the private IP of the Bastion host


Users
SSH
VPC
Public Subnet
Security Group (BastionHost-SG)
EC2 Instance
(Bastion Host)
SSH
Private Subnet
Security Group (LinuxInstance-SG)