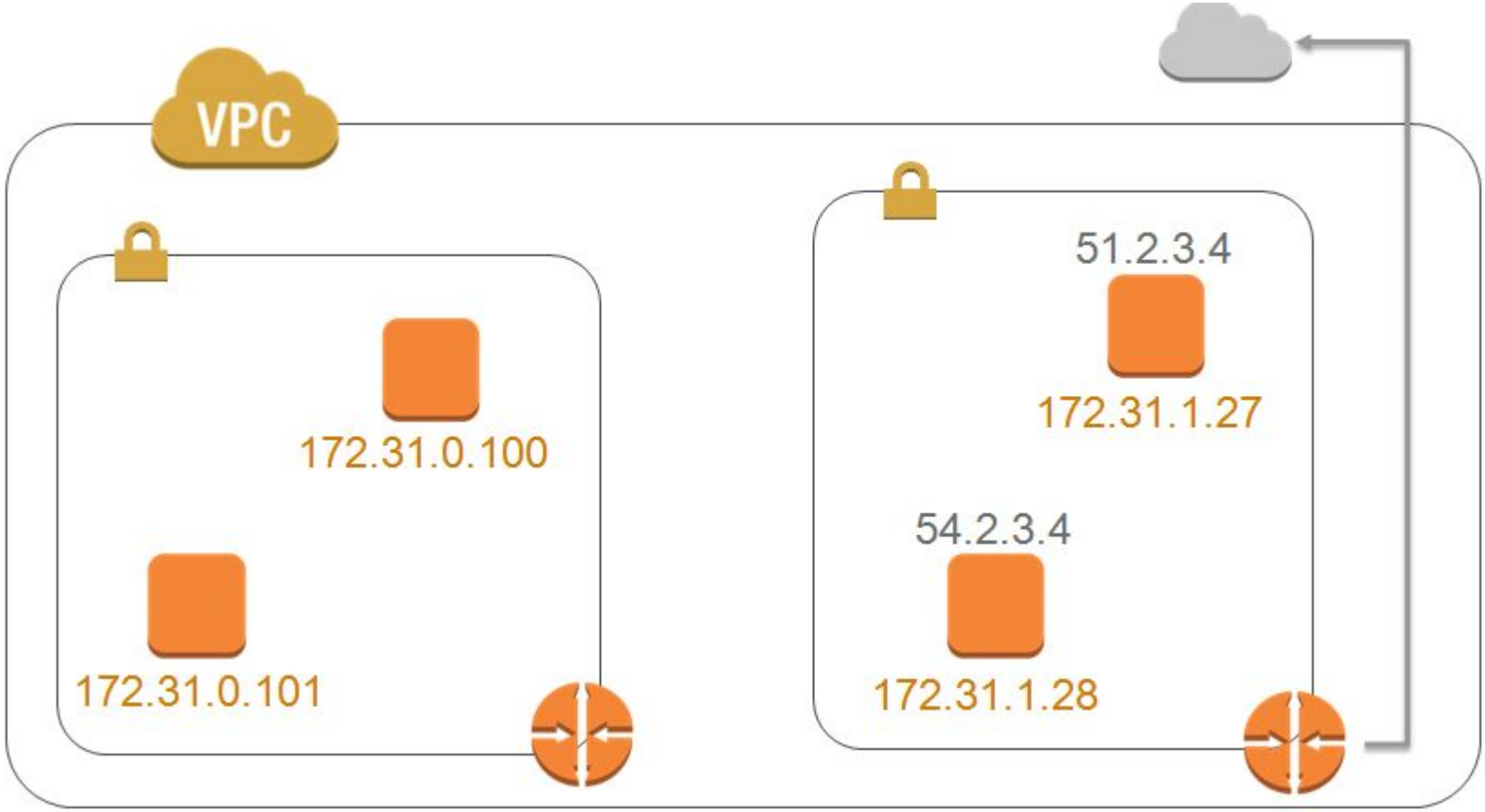
Virtual Private Cloud

July 2017

What is Amazon VPC ?

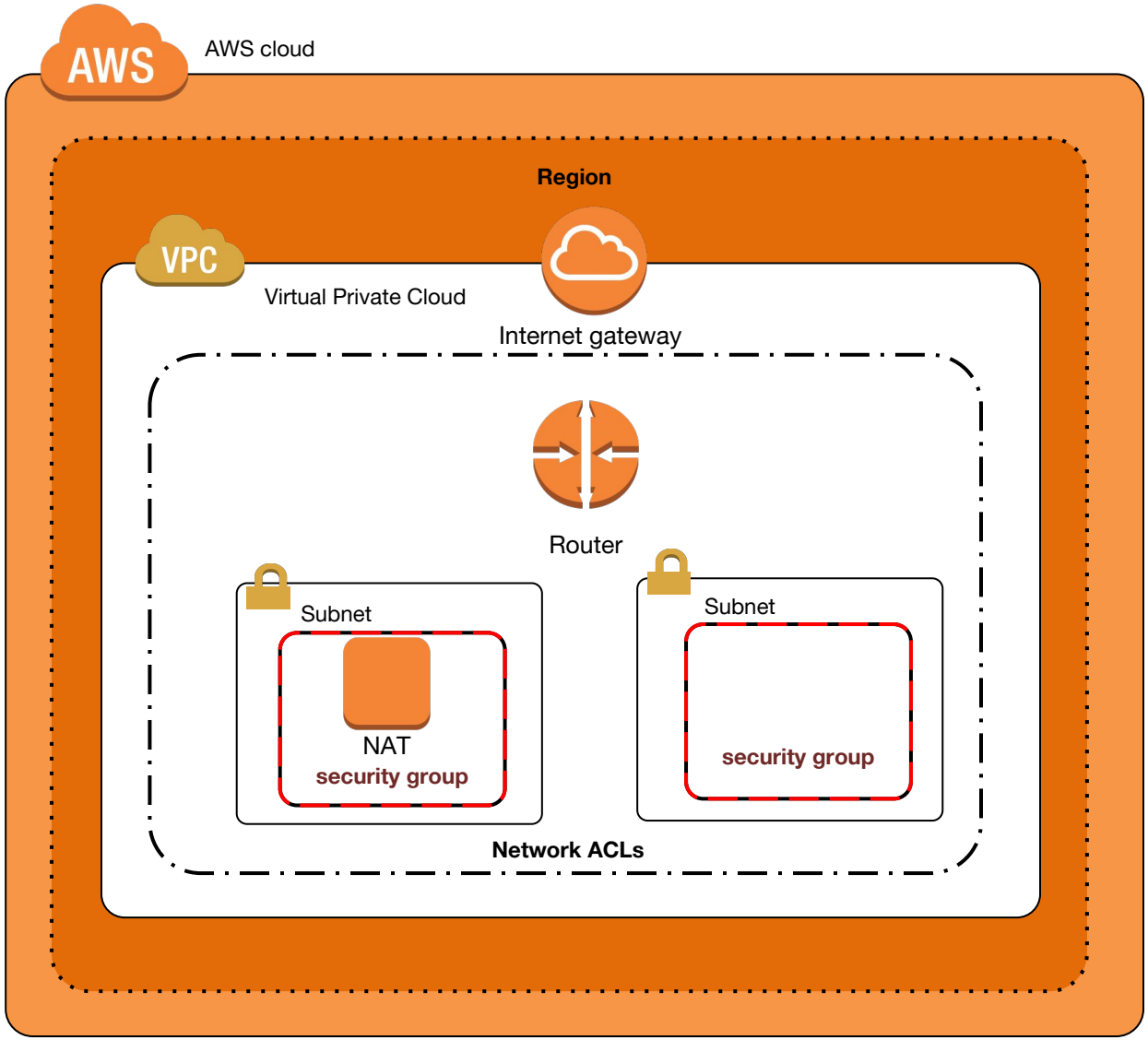
- Virtual Network in AWS
- Allow to design own network Topology
- You decide IP range , Number of subnets , Network ACL
- Provides security controls at Network level

EC2 runs within VPC



Steps for creating Internet Connected VPC

1. Choose IP range for VPC
2. Create Subnet
3. Create Internet Gateway (IGW)
4. Attach IGW to VPC
5. Change Route entries if required
6. Change Network Access Control List (if needed)
7. Setup Security Groups



Typical VPC Arrangement

- Internet Gateway
  - Horizontally scaled, redundant, and highly available VPC component
  - One VPC one IG
- NAT Instance
  - Provide internet access to private subnet instances
  - Launch in public subnet

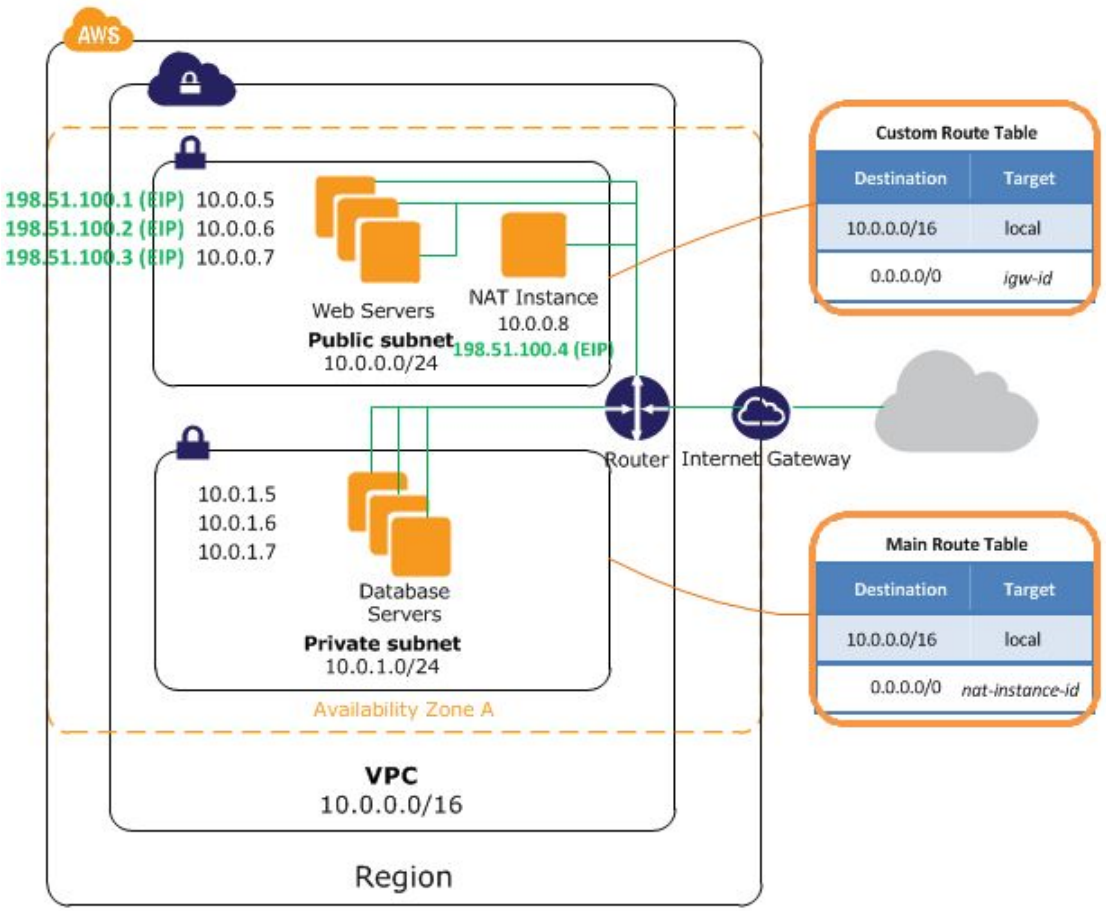


Image Source: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html

Understanding Routing Entries

CM-WORKSHOP-PUBLIC-RT	rtb-584f603d	2 Subnets	No	vp

rtb-584f603d | CM-WORKSHOP-PUBLIC-RT

Summary | **Routes** | Subnet Associations | Route Propagation | Tags

Edit

View: All rules

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-9623b2f3	Active	No

- Making Internet Routable VPC using IGW entry

Note : VPC and IP Addresses

The first 4 IP addresses and the last IP address in each subnet CIDR block are not available for you to use and cannot be assigned to an instance.

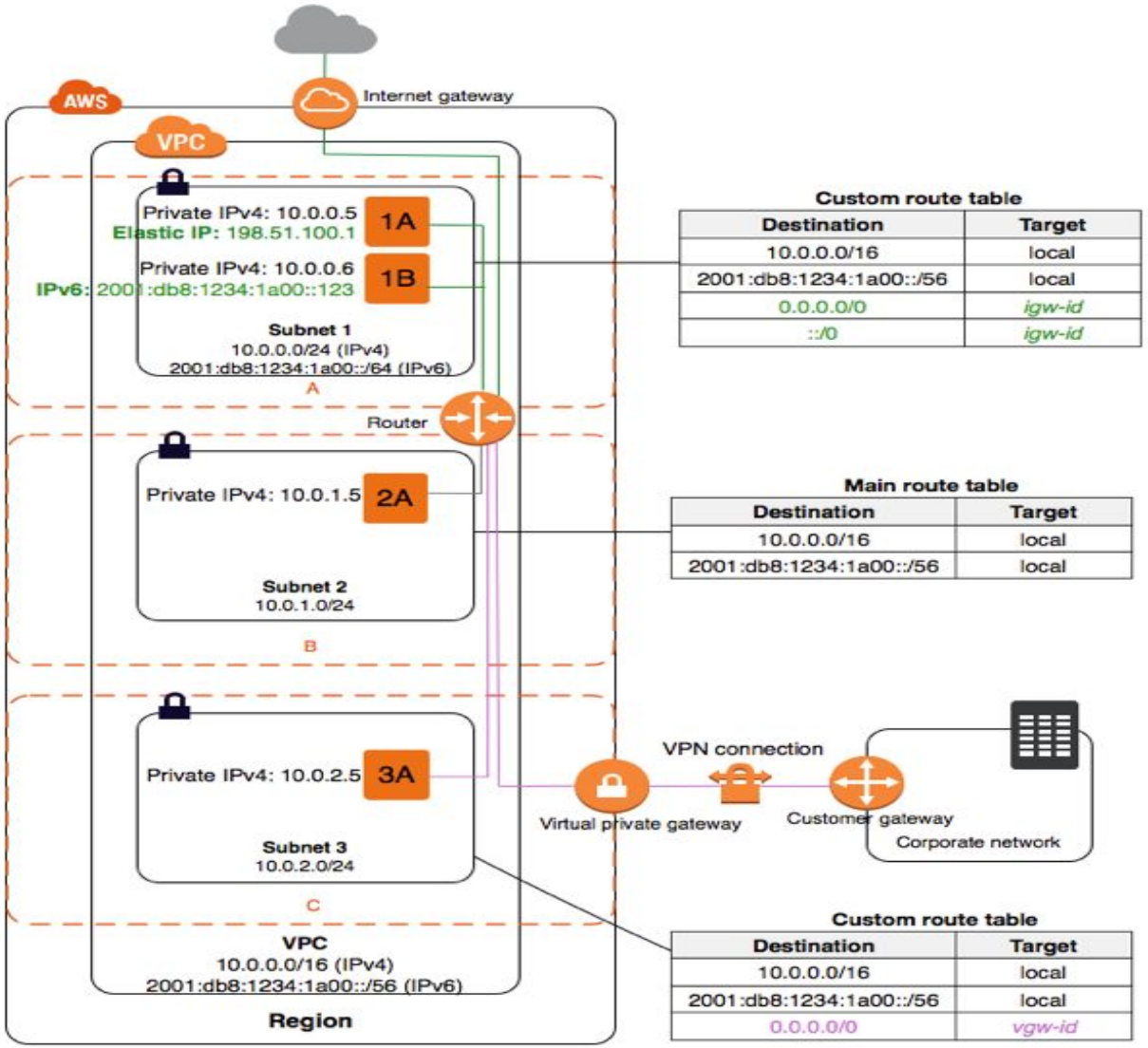
For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

- 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 the Amazon-provided DNS.
- 10.0.0.3: Reserved by AWS for future use.
- 10.0.0.255: Network broadcast address
    a. AWS does not support broadcast in a VPC, therefore this is reserved

Subnets

- If a subnet's traffic is routed to an internet gateway, the subnet is known as a *public subnet*
- If a subnet doesn't have a route to the internet gateway, the subnet is known as a *private subnet*
- If a subnet doesn't have a route to the internet gateway, but has its traffic routed to a virtual private gateway for a VPN connection, the subnet is known as a *VPN-only subnet*.

Subnets - Public, Private & VPN Only



Custom route table

Destination	Target
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Main route table

Destination	Target
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local

Custom route table

Destination	Target
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	*vgw-id*

Network Access Control Lists

- Security Control given at Network Layer
- Stateless Firewall
- Supports Allow and Deny Rule
- Can have number of rules
- Evaluates with lowest number first and if matches exits the match
- Useful for tighter security control

subnet-3606040c | CM-WORKSHOP-PUBLIC-SUBNET-B

Summary | Route Table | **Network ACL** | Flow Logs | Tags

Edit

Network ACL: acl-7a2b611f | My ACL

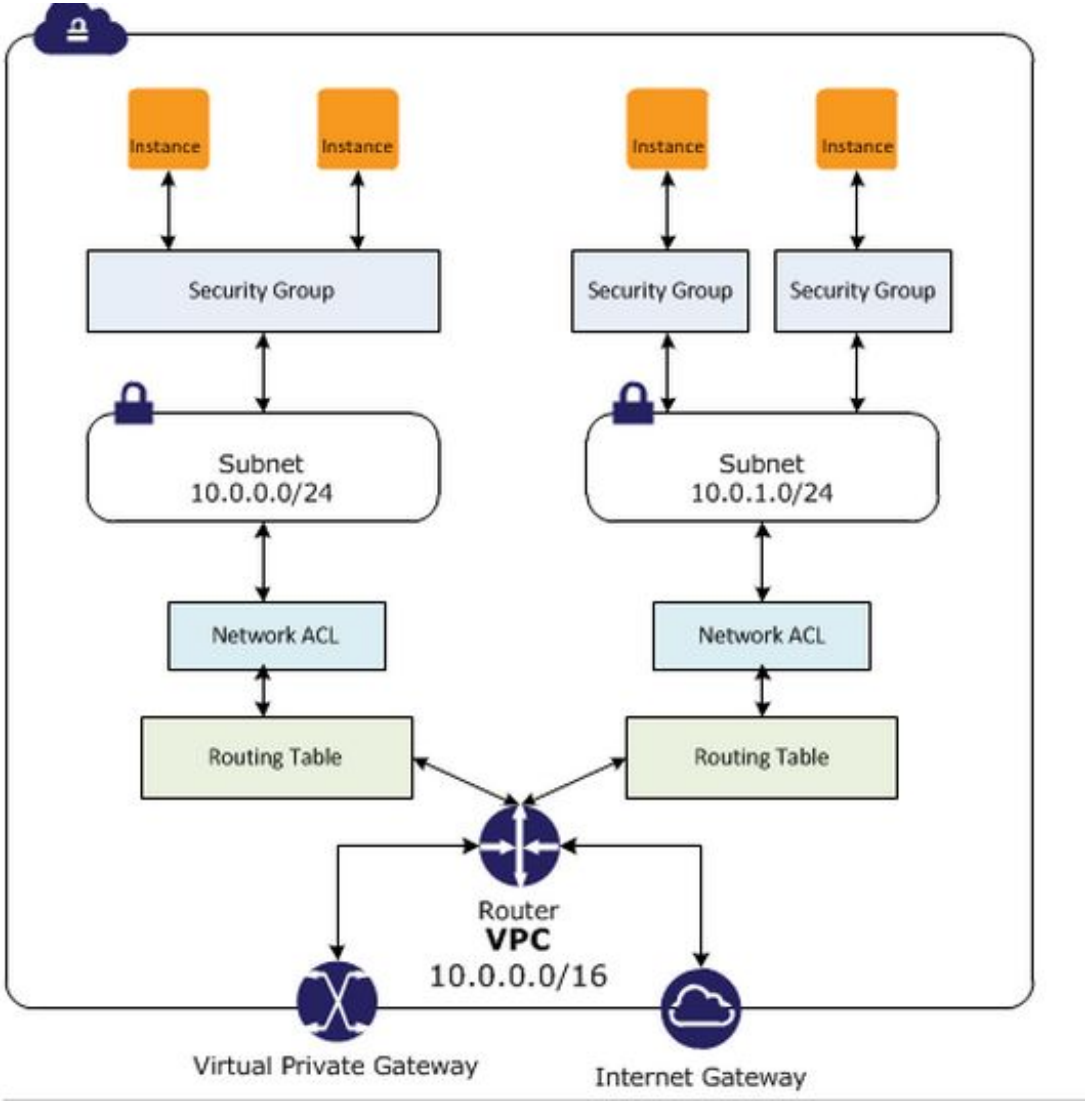
Inbound:

Rule #	Type	Protocol	Port Range / ICMP Type	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Outbound:

Rule #	Type	Protocol	Port Range / ICMP Type	Destination	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

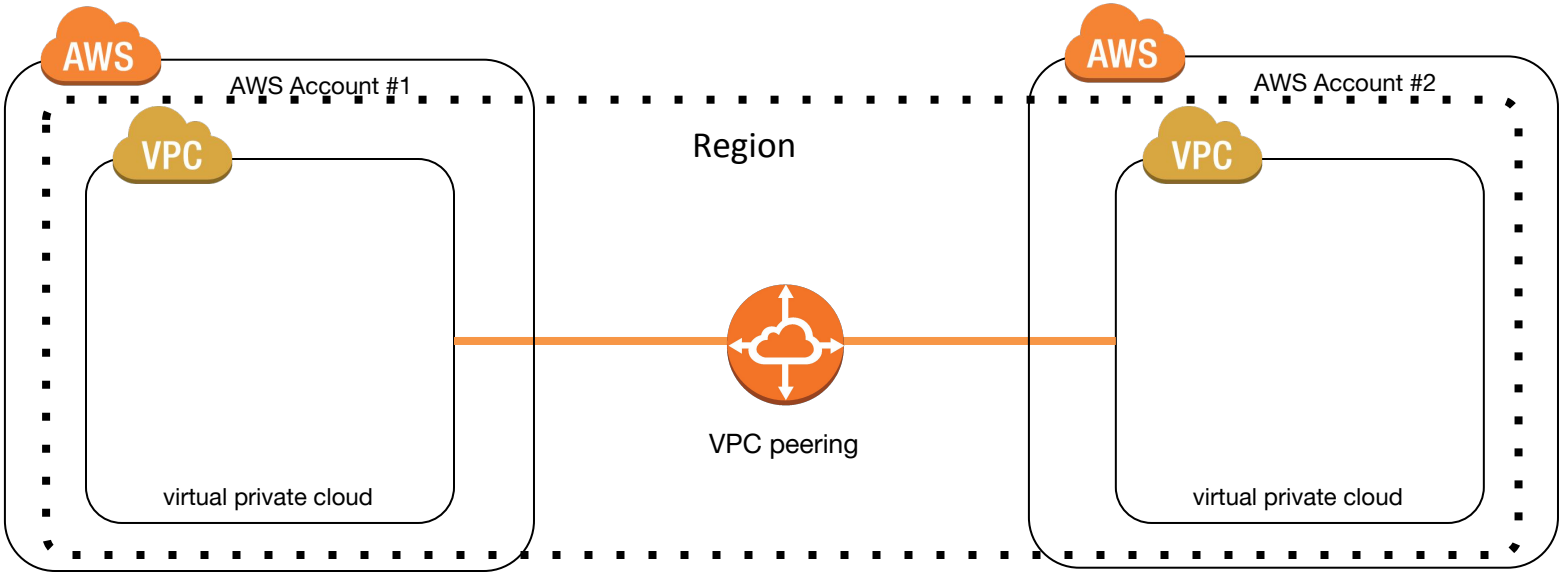
Comparing Security Groups and Network ACLs



VPCs want to talks to each other

VPC Peering

- Connection between two VPCs
- Can connect VPC in different AWS account
- One to one relationship between two VPCs
- 50 VPC peering connection per region
- Within one region ONLY
- Communicates using PRIVATE IPs

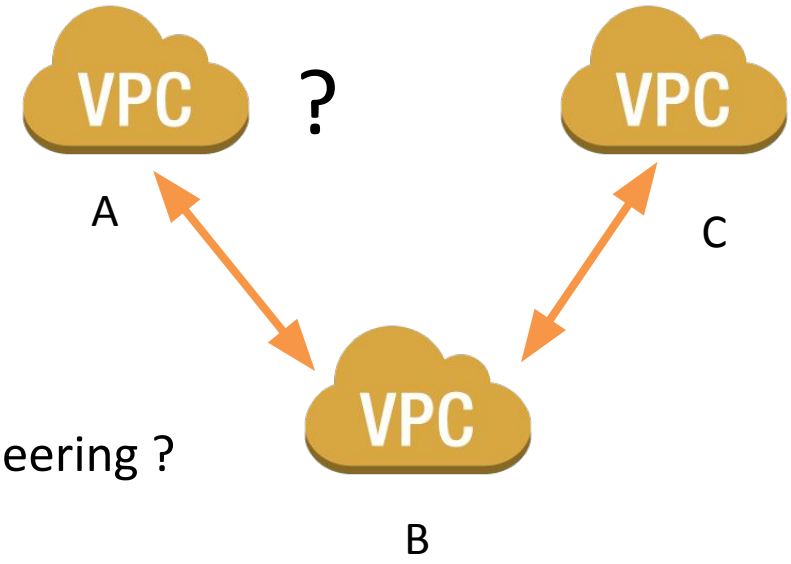


VPC Peering

- Not Transitive in nature

- If Peering exists
  - between A and B
  - Between B and C

  Then Can A & C communicate via VPC peering ?

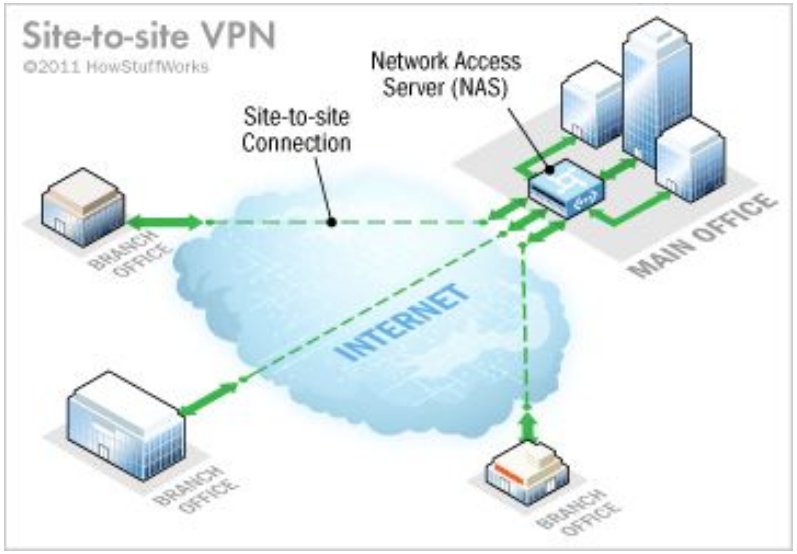


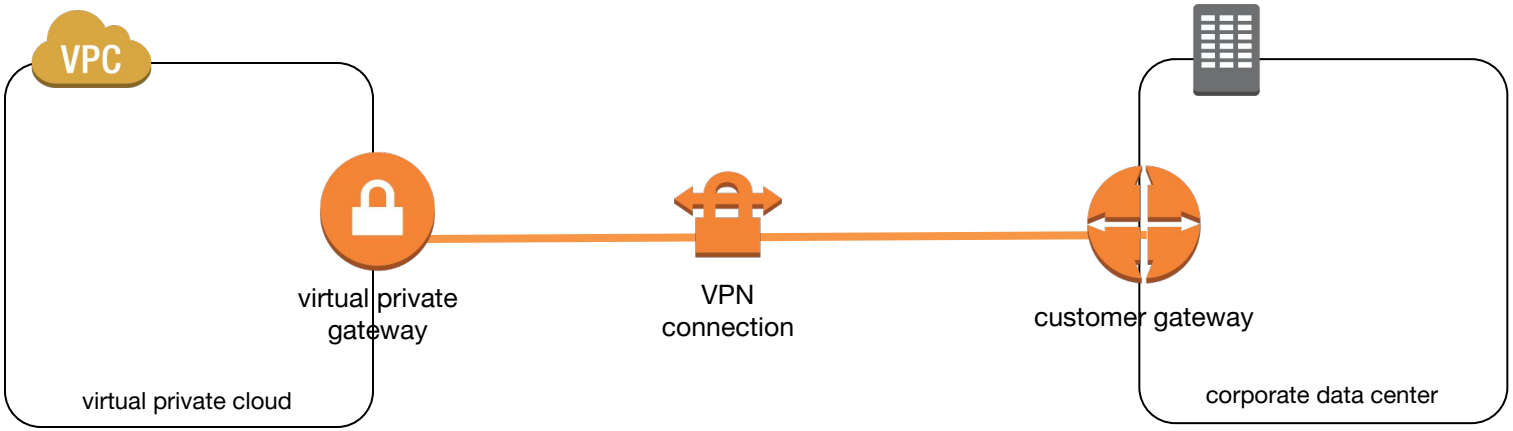
- **Scenarios**
  - One to one - DEV, STAGING , UAT – want to connect / patch
  - Common VPC to Many VPC
    - Active Directory on Common VPC
    - AV solution on common VPC
    - Management Box on Common VPC
    - Third party backup solution

Connecting VPC and On-Premise World

Extending On-Premise Network to Cloud

- Virtual Private Gateway
  - VPN concentrator on the Amazon side
  - One VPC one Virtual Private Gateway
  - 5 Virtual Private Gateway per region
  - One to many connection
- Customer Gateway
  - physical device or software application on Corporate side
  - 50 Customer Gateway per region
- VPN Connection
  - Static and Dynamic routing



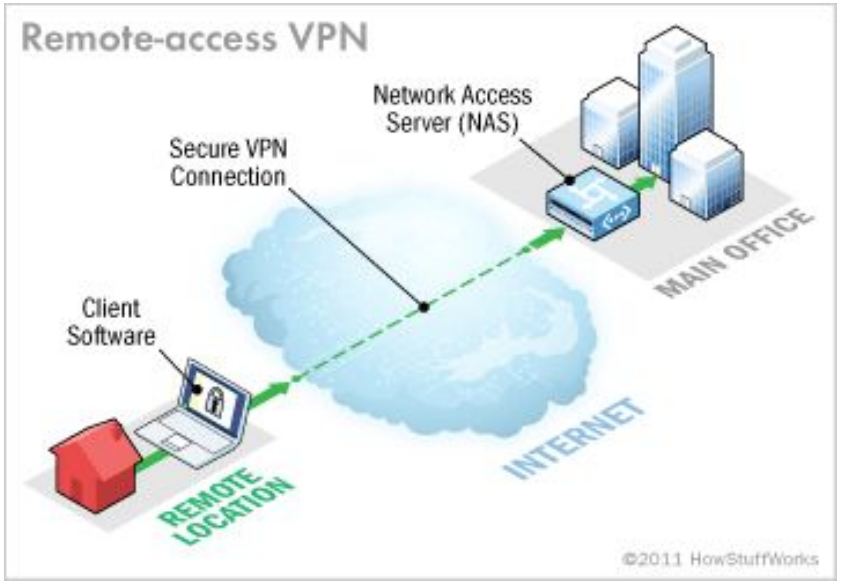


Extending On-Premise Network to Cloud

- If you do need site to site VPN use VPN server such as OpenVPN server on EC2 server

- Clients would need to have VPN client and connect it to the EC2 premise

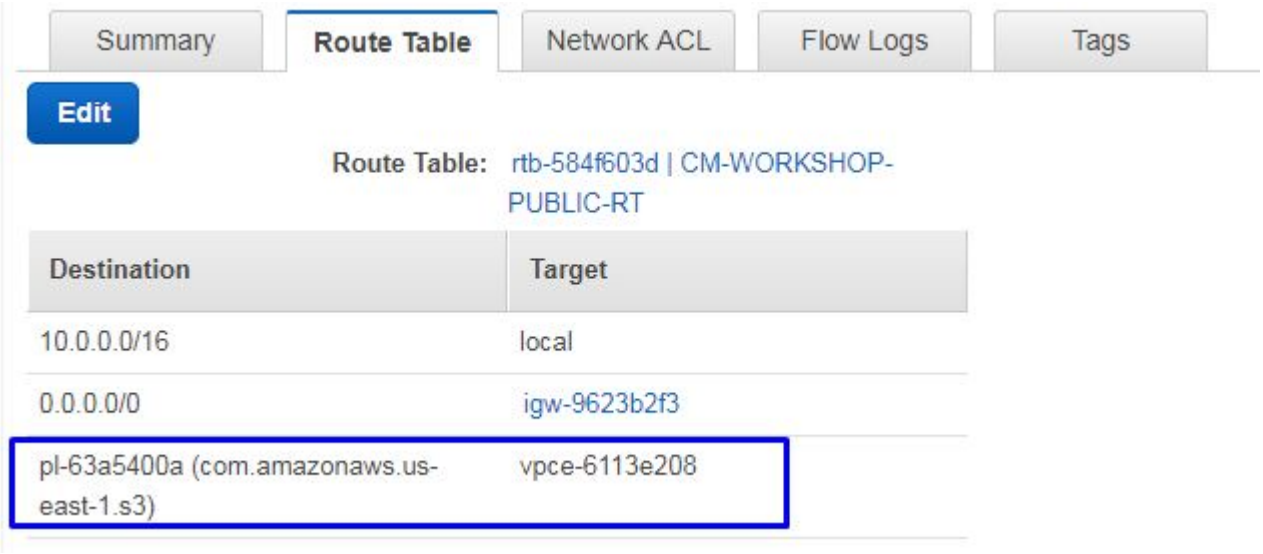
- https://docs.openvpn.net/how-to-tutorialsguides/virtual-platforms/amazon-ec2-appliance-ami-quick-start-guide/



VPC Endpoints

VPC Endpoints

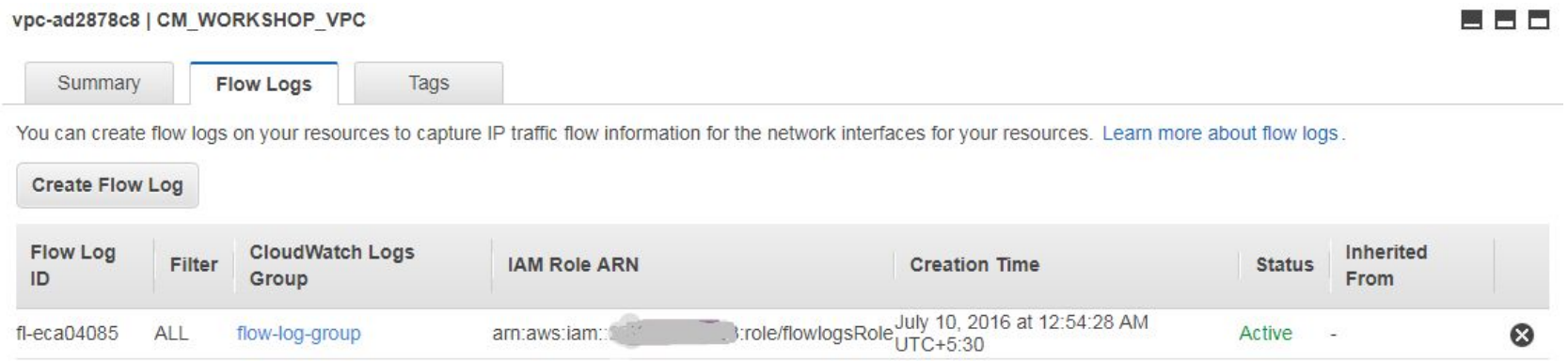
- Enables you to create a private connection between your VPC and another AWS service without requiring access over the Internet
- EC2 servers does not require PUBLIC IP address or does not require a NAT gateway or NAT instances
- Easy to configure and Highly Available



VPC Flow Logs

Monitor your VPC traffic

- To troubleshoot connectivity and security issues
- To test network access rules functionality
- Alarms if unwanted traffic are detected
- Logs are saved into log groups in CloudWatch Logs



VPC Pricing

- No charge for VPC
- However VPN Connection , Gateway and Data Transfer are chargeable

For details please refer to https://aws.amazon.com/vpc/pricing/

VPC Limits

Resource	Default Limit	Comments
# of VPCs /region	5	Can be increased upon request
# Internet Gateways/region	5	Linked with VPC limit, Can be increased upon request
Elastic IP addresses	5	Can be increased upon request
Subnets/VPC	200	Can be increased upon request
Security Groups/VPC	200	..
Security Group/ENI	5	
...		

Best Practices

- Selecting right VPC Architecture design
- One time CIDR Block Selection
- Isolate VPC according to Use Case
- Unpopulated Public Subnet
- Control your In-Out traffic in VPC using ACLs and SG
- Tier your Security Groups
- Use EIP when needed
- Use Multi AZ deployment model

End of Module

Networking Basics

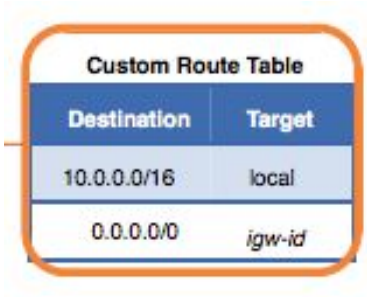
0.0.0.0 IP Address

In the context of servers

- A computer can have multiple Network Interface Cards (NICS)
- In case there are two IP addresses for a machine 192.68.0.5 and and 10.0.0.5 if a server is listening on 0.0.0.0 IP address then the traffic will reach on both the the IP addresses

In the context of routing tables

- it is the default route



Custom Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Broadcast Address

- Special values in the **host identification part** of the address
- Broadcast address for an IPv4 host can be obtained by
  - performing a bitwise OR operation between the bit complement of the subnet mask and the host's IP address.
  - In other words, take the host's IP address, and set to '1' any bit positions which hold a '0' in the subnet mask.
- Example:
  - For broadcasting a packet to an entire IPv4 subnet using the private IP address space 172.16.0.0/12, which has the subnet mask 255.240.0.0, the broadcast address is 172.16.0.0 | 0.15.255.255 = 172.31.255.255.

255.255.255.255

- It is the broadcast address of ‘zero network’ / 0.0.0.0 or this network

Default Gateway

- Node that knows how to forward packets to other networks
- Gateway is by definition ‘**router’**