Training Course

Amazon Web Service

Course Schedule

Day	Presentations	Lab
Day 1	System Operations on AWS	
Day 2	Computing on AWS	X
Day 3	Networking on AWS	X
Day 4	Storage and Archiving in the Cloud	X
Day 5	Monitoring in the Cloud	X
Day 6	Managing Resource Consumption in the Cloud	X

Module 3:

Networking in AWS

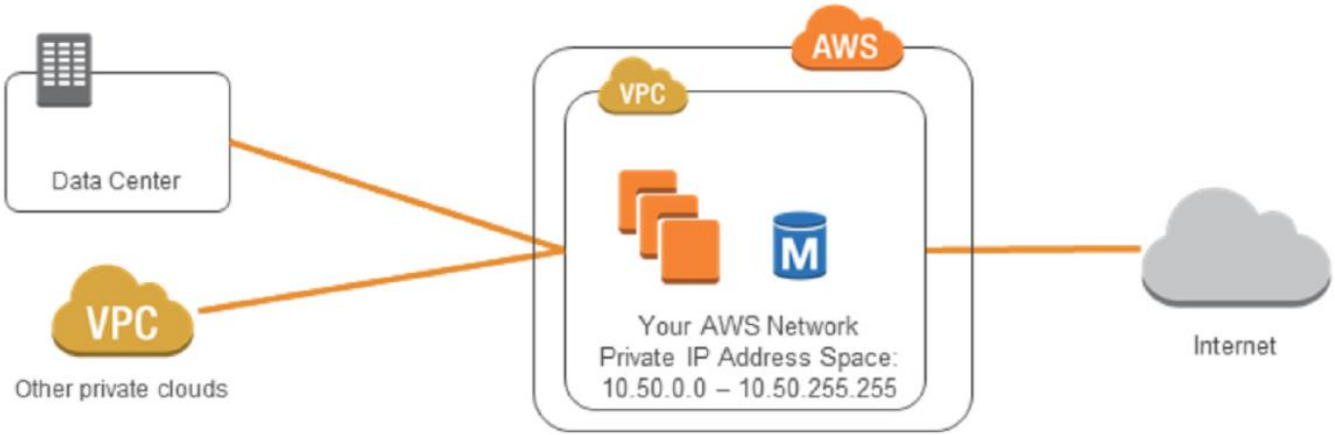
- **Goal**: Understand how to create your own custom virtual private cloud using the AWS Management Console
  - ✓ Common Amazon VPC Scenarios
  - ✓ Amazon VPC Peering and Direct Connect
  - ✓ Amazon VPC Security Troubleshooting

  Lab 2: Configuring a Virtual Private Cloud

Understanding Networking and Amazon Virtual Private Cloud (VPC)

Understanding Cloud Networking

- Cloud networks are virtual private network
- Cloud networks can connect to the Internet and corporate data centers
- Cloud networks can integrate with existing data centers

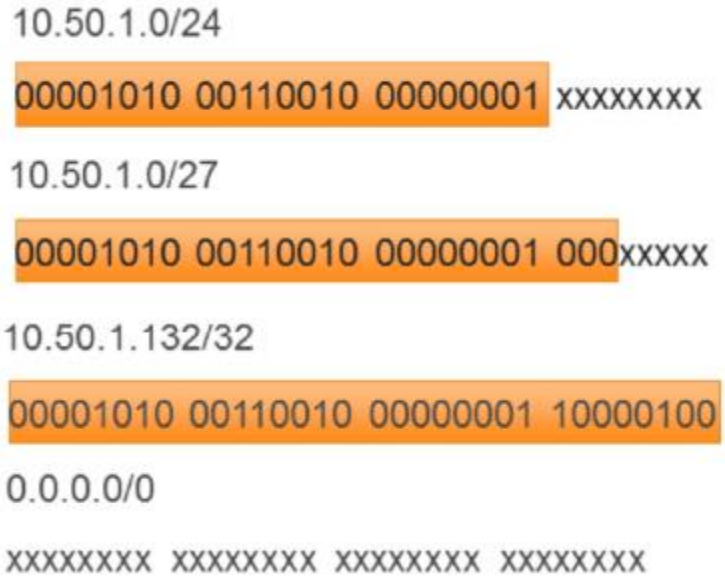


Amazon Virtual Private Cloud (VPC)

- Virtual network, isolated portion of AWS cloud for Amazon EC2 instances
  - Optional dedicated tenancy
  - Supports logical separation with subnets
  - Fine-grained security
- Private address ranges specified using Classless Inter-Domain Routing (CIDR) notation
- Replacement for EC2-Classic (flat network architecture)

CIDR Notation (IP Address scheme)
Classless Inter- Domain Routing

- Format is x.x.x.x/n, where x.x.x.x is an IP address prefix and n is the length of the bitwise prefix
- /32 specifies a single address
- 0.0.0.0/0 specifies all IP addresses



IP (Internet Protocol)

- IP provides the identity of the connected devices in the network
- 5 classes of addresses
  - A: 1.0.0.1 -> 126.0.0.0 (large comporation)
  - B: 128.1.0.0 -> 191.254.0.0 (medium comporation)
  - C: 192.0.1.0 -> 223.255.254.0 (small comporation, personal device)
  - D: 224.0.0.0 -> 239.255.255.255 (information transfer)
  - E: 240.0.0.0 -> 254.255.255.255 (reseach target)
  - Loopback: 127.X.X.X

Type of IP

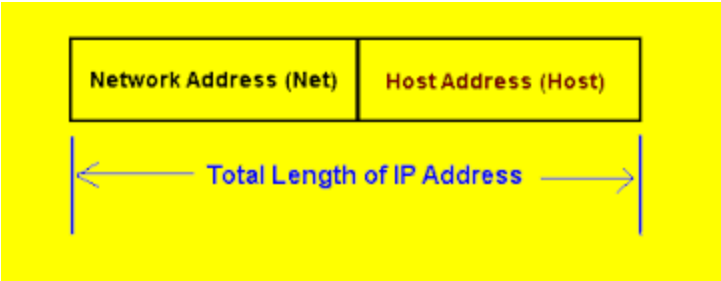
- Public IP: assign by Internet providers
- Private IP: use in LAN/private network (can not connect Internet, access through Router)

- Static IP: manual setting, no change follow time
- Dynamic IP: constantly changing, managed by DHCP Server

IP Structure

- Binary range 32 bit – 4 sets of 8 bit (Octet)
- 2 part
    - NetID: define network connect by device
    - HostID: define that device

Ex: 192.168.1.3



Subnet Mask

- An IP comes with 1 subnet mask, to define netID of that IP
- Subnet include bit 1 and 0. Number of bit 1 = number bit of netID

Ex:

11111111	11111111	11111111	00000000
255	255	255	0000

IP: 192.168.1.3 – SubnetMask: 255.255.255.0
or 192.168.1.3/24

Subnet Mask

- An IP address can belong to different networks if different subnet masks are used
- To determine which network IP belongs to, just get the corresponding ip address AND (bitwise) subnet mask mask

Ex: 192.168.1.3 AND 255.255.255.0 = 192.168.1.0
=> 192.168.1.3/24 in network 192.168.1.0/24

Default Gateway

- When the packet is sent to an address that is not on the same network, or does not know where to send it, it will be sent to the **Default Gateway**, which is usually the interface of the Router directly connected to that network. Routers use routing to forward packets in different directions

- DFs are usually the first usable IP addresses of the network

Ex: Default Gateway of 192.168.1.0/24 is **192.168.1.1/24**

Example Sequences of Contiguous Networks

Prefix	Count	Class	Starting	Ending
10/8	1	A	10.0.0.0	10.255.255.255
172.16/12	16	B	172.16.0.0	172.31.255.255
192.168/16	256	C	192.168.0.0	192.168.255.255

Amazon VPC Component

Amazon VPC Components: The VPC

- VPCs can span across multiple Availability Zones within a region
- VPCs have an implicit router and a default route table that routes local traffic within the VPC
- VPC are private networks until associated with an Internet gateway and a route table rule routing traffic through it

Amazon VPC Components: The VPC (Discussion)

- ✓ VPC: Virtual Private Cloud – Completed - 0
- ✓ Subnet (Group1)
- ✓ Internet Gateway (Group2)
- ✓ Default Security Group (Group3)
- ✓ Route Table (Group4)
- ✓ Network Access Control List (Group5)
- ✓ NAT Gateway (Group6)

Amazon VPC Components: The VPC (Discussion)

❑ Subnet

- Sub network (in VPC)
- One or more subnet in VPC
- Define CIDR when create subnet
- Each subnet must be completely located in an Availability Zone

Amazon VPC Components: The VPC (Discussion)

❑ Subnet: 2 types

- Public Subnet
  - ✓ Routing to 1 internet gateway
  - ✓ Instance in public subnet can access internet via IPv4 (or EIP)
- Private Subnet
  - ✓ Do not routing to internet gateway
  - ✓ You can’t access instance in Private Subnet from internet

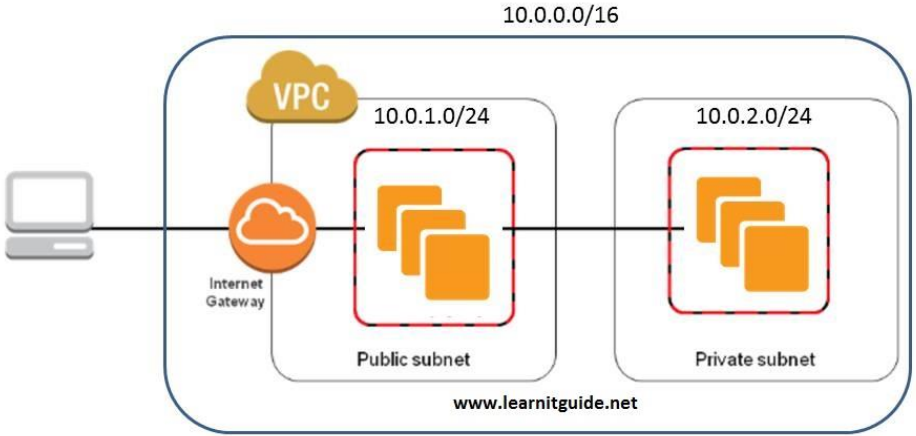
Amazon VPC Components: The VPC (Discussion)

❑ Subnet: Limitations

Resource	Default limit
VPCs per region	5
Subnets per VPC	200
IPv4 CIDR blocks per VPC	5 (1)
IPv6 CIDR blocks per VPC	1

Amazon VPC Components: The VPC (Discussion)

❑ Subnet: Example



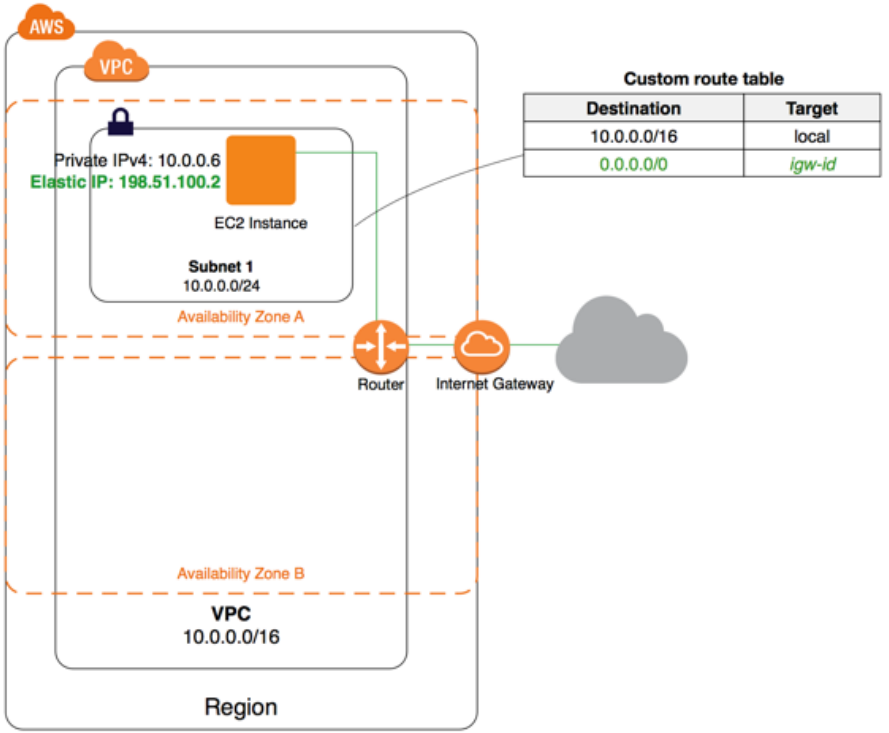
Amazon VPC Components: The VPC (Discussion)

❑ Internet Gateway

- An Internet Gateway is a VPC component that allows communication between VPC and Internet
- Support IPv4 and IPv6

Amazon VPC Components: The VPC (Discussion)

- ❑ **Internet Gateway**



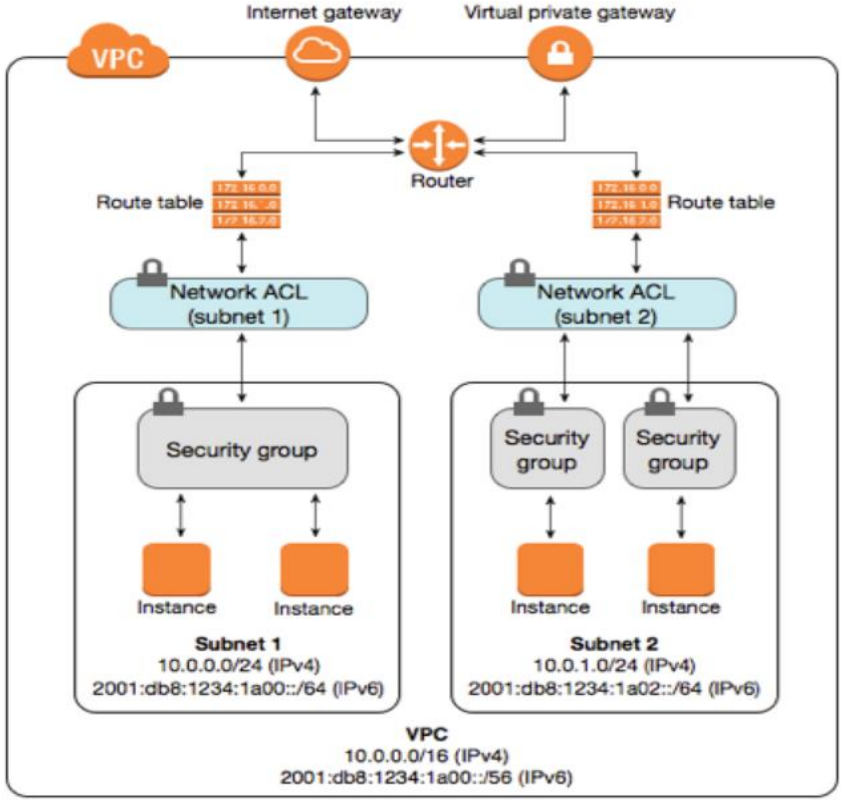
Amazon VPC Components: The VPC (Discussion)

❑ Default Security Group

- AWS account have a Default security group for VPC in each region
- Instance will auto attach to default security group if you not attach them
- Name default: <default-ID>
- Some rules:
  - ➢ Allow access between instances that are assigned to the same default security group
  - ➢ Allow traffic from the instance to go out
  - ➢ You can add or remove rules for any default security group

Amazon VPC Components: The VPC (Discussion)

❑ Default Security Group



Amazon VPC Components: The VPC (Discussion)

❑ Route Table

- A routing table contains rules called 'routes', which determine the path of incoming and outgoing network traffic.
- Each subnet in your VPC will be associated with a route table, which will manage the route in the subnet.
- A subnet can only be associated with 1 routing table at a time, but conversely you can associate multiple subnets with a routing table.

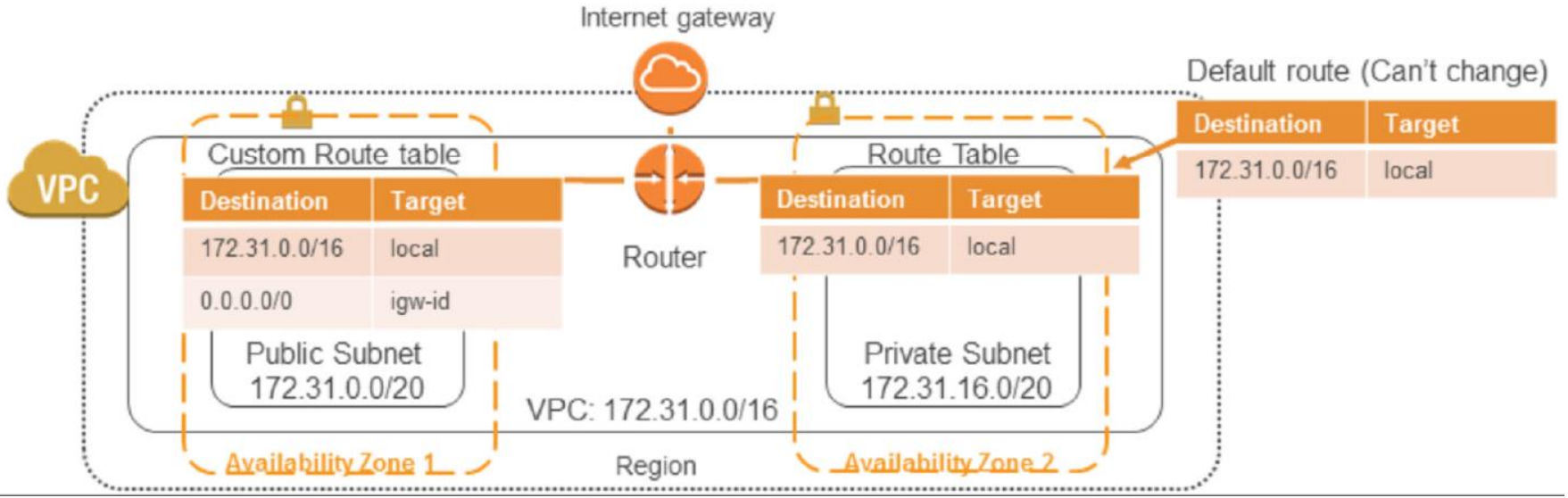
Amazon VPC Components: The VPC (Discussion)

❑ Route Table

- Route Table (default route, can’t change)
  - ➢ Private subnet
- Custom route table
  - ➢ Public subnet

Amazon VPC Components: The VPC (Discussion)

❑ Route Table

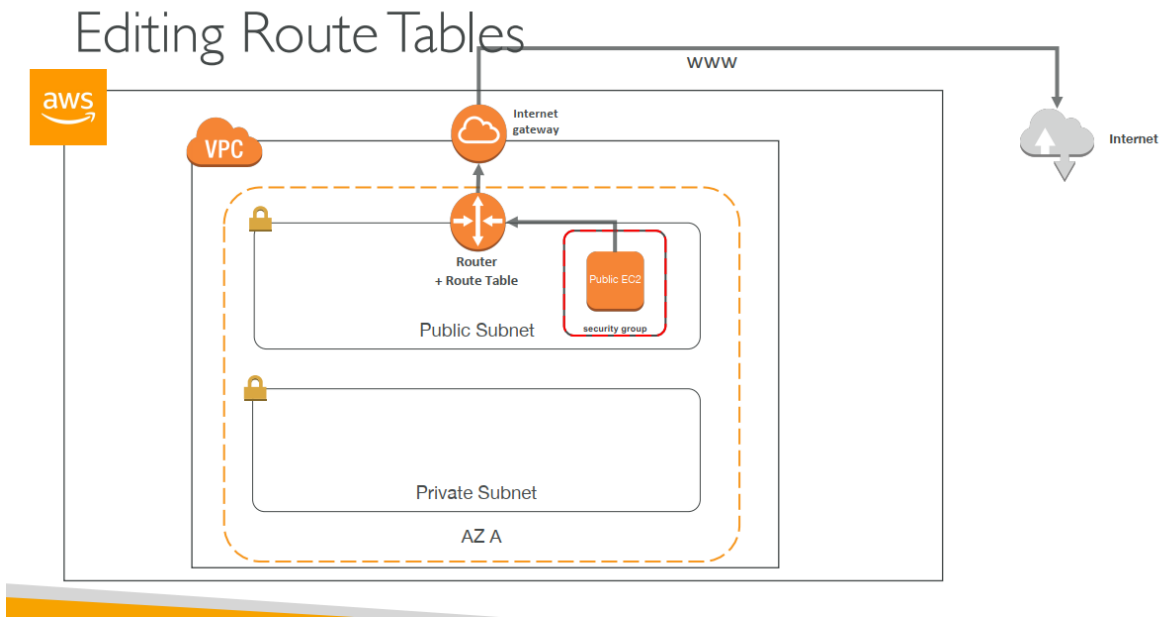


Amazon VPC Components: The VPC (Discussion)

- ❑ VPC, Subnet, Internet Gateway, Security Group (default)
- ❑ Describle by Powerpoint

Amazon VPC Components: The VPC (Discussion)

❑ VPC Summary – Hands-on – Lab1

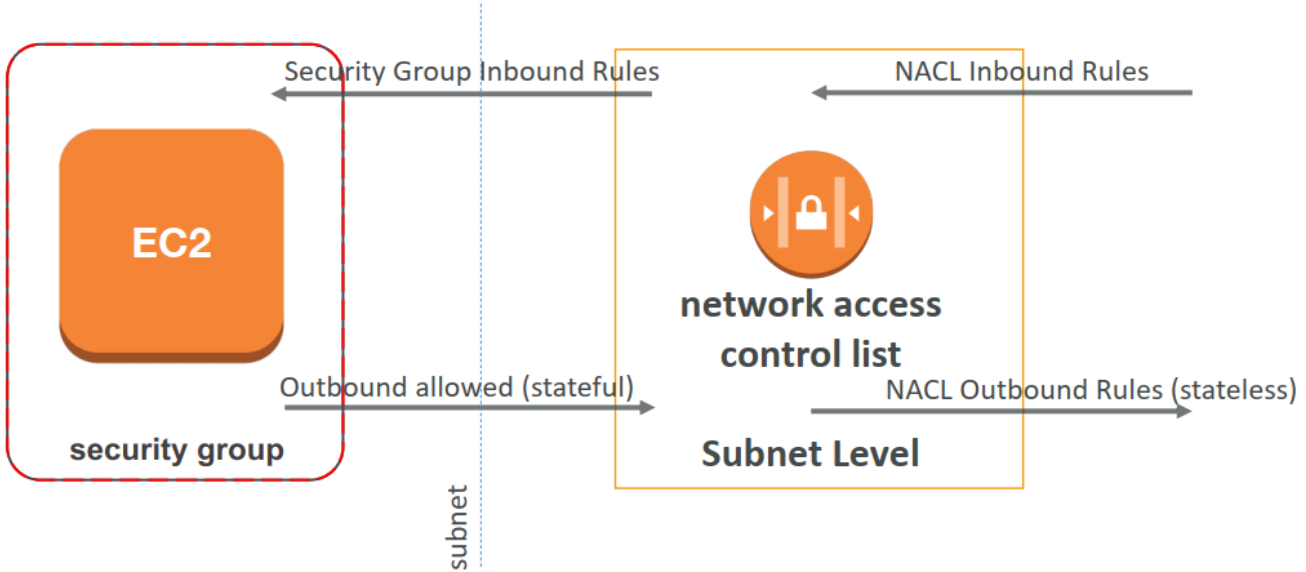


Amazon VPC Components: The VPC (Discussion)

❑ Network Access Control List

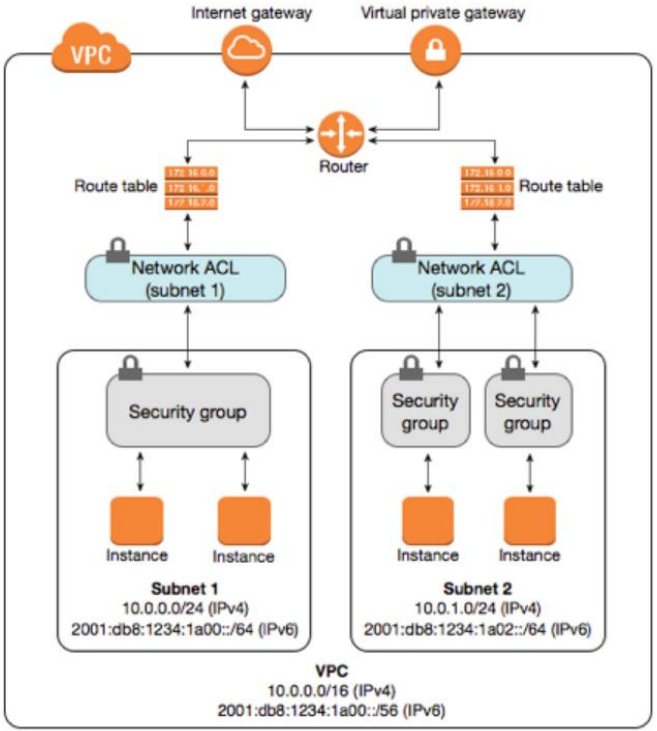
- A layer of security that acts no different than a firewall
- Allows you to control the incoming and outgoing traffic of one or more different **subnets**.
- You will probably configure the Network ACL

Amazon VPC Components: The VPC (Discussion)



Amazon VPC Components: The VPC (Discussion)

❑ Network Access Control List



https://vinasupport.com

Amazon VPC Components: The VPC (Discussion)

❑ Network Access Control List and Security group

Security Group	Network ACL
Managed in Instance Level	Managed in Subnet Level
Only support Allow Rule	Support both Allow rule and Deny rule
If have respond > allow	If have respond > check respond
AWS evaluate all rule before decide allow access	AWS evaluate rule step by step
Only apply for 1 instance	Auto apply for all instance in subnet

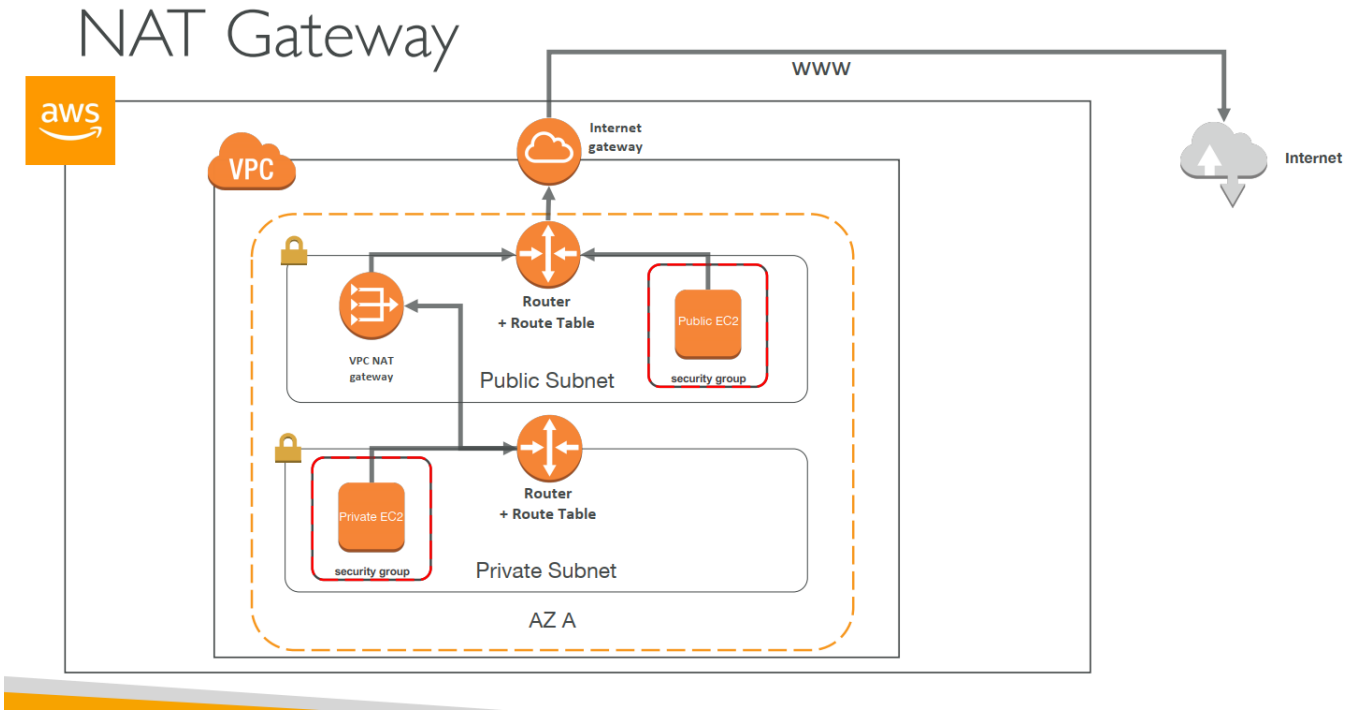
Amazon VPC Components: The VPC (Discussion)

❑ Nat Gateway

- To connect internet, device need have a Public IP, local device is not
- Network Address Translation - IP address conversion technique
- Convert IP private to global IP (router or firewall, …)
- NAT provides a single public IP address for all devices in the local network. This is both easy to manage and saves costs.

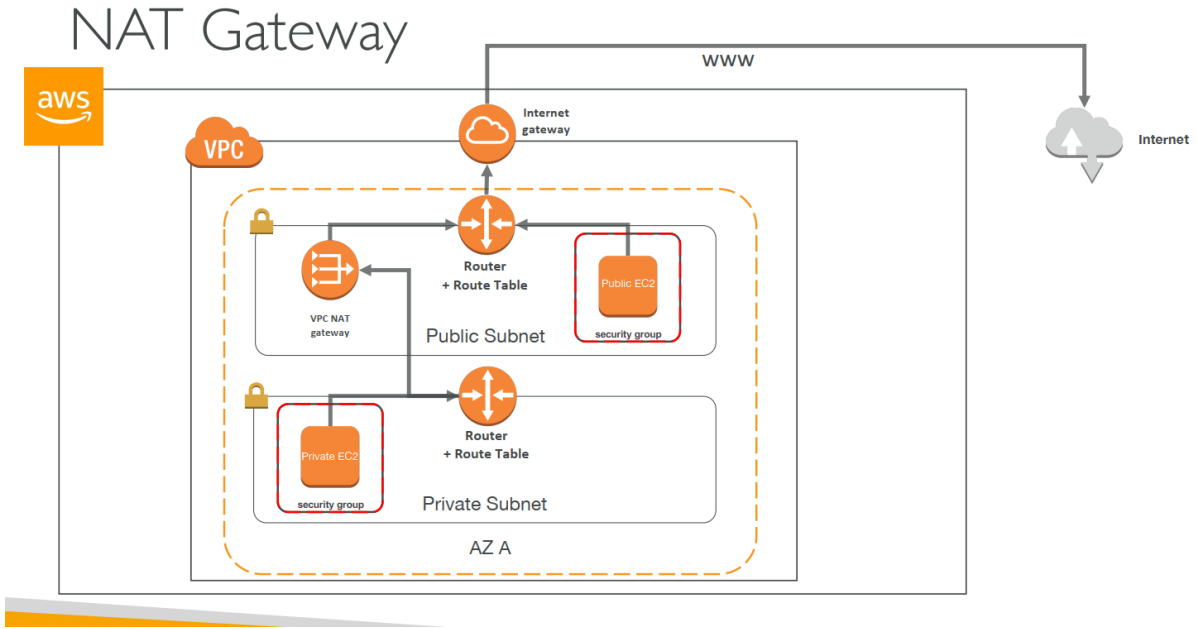
Amazon VPC Components: The VPC (Discussion)

❑ Nat Gateway



Amazon VPC Components: The VPC (Discussion)

❑ VPC Summary – Hands-on – Lab2

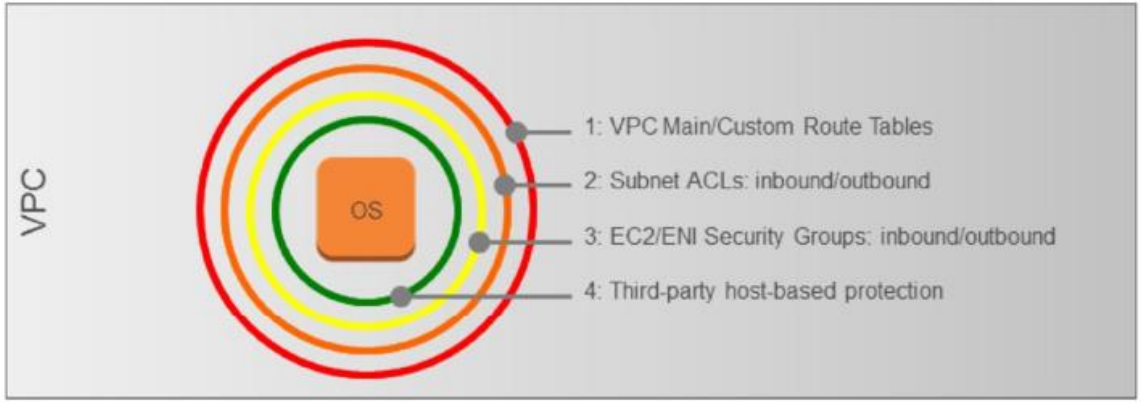


Amazon VPC Components: The VPC (Discussion)

- ✓ VPC: Virtual Private Cloud - Completed
- ✓ Subnet (Group1)
- ✓ Internet Gateway (Group2)
- ✓ Default Security Group (Group3)
- ✓ Route Table (Group4)
- ✓ Network Access Control List (Group5)
- ✓ NAT Gateway (Group6)

Securing Your Network

Layered Network Defense for VPCs



AWS also performs DDoS and intrusion detection at the network level.

- **Security Groups**
  - ✓ Used to allow traffic to/from EC2 instances at the ENI (interface) level
  - ✓ By default configured to deny all inbound and allow all oubout traffic
  - ✓ Stateful
    - If rules allow traffic to flow in one direction, response can automatically flow in the opposite direction
    - Usually administered by application developers

- **Placement Groups**

  - ✓ Physical grouping of high performance instance in a single Availability Zone
  - ✓ Instance will use enhanced networking for faster, more consistent throughput
  - ✓ Placement Groups are suitable for clustered databases,big data, and graphics processing in parallel

Troubleshooting Network on AWS

Troubleshooting Network on AWS

❑ Subnets cannot communicate with one another

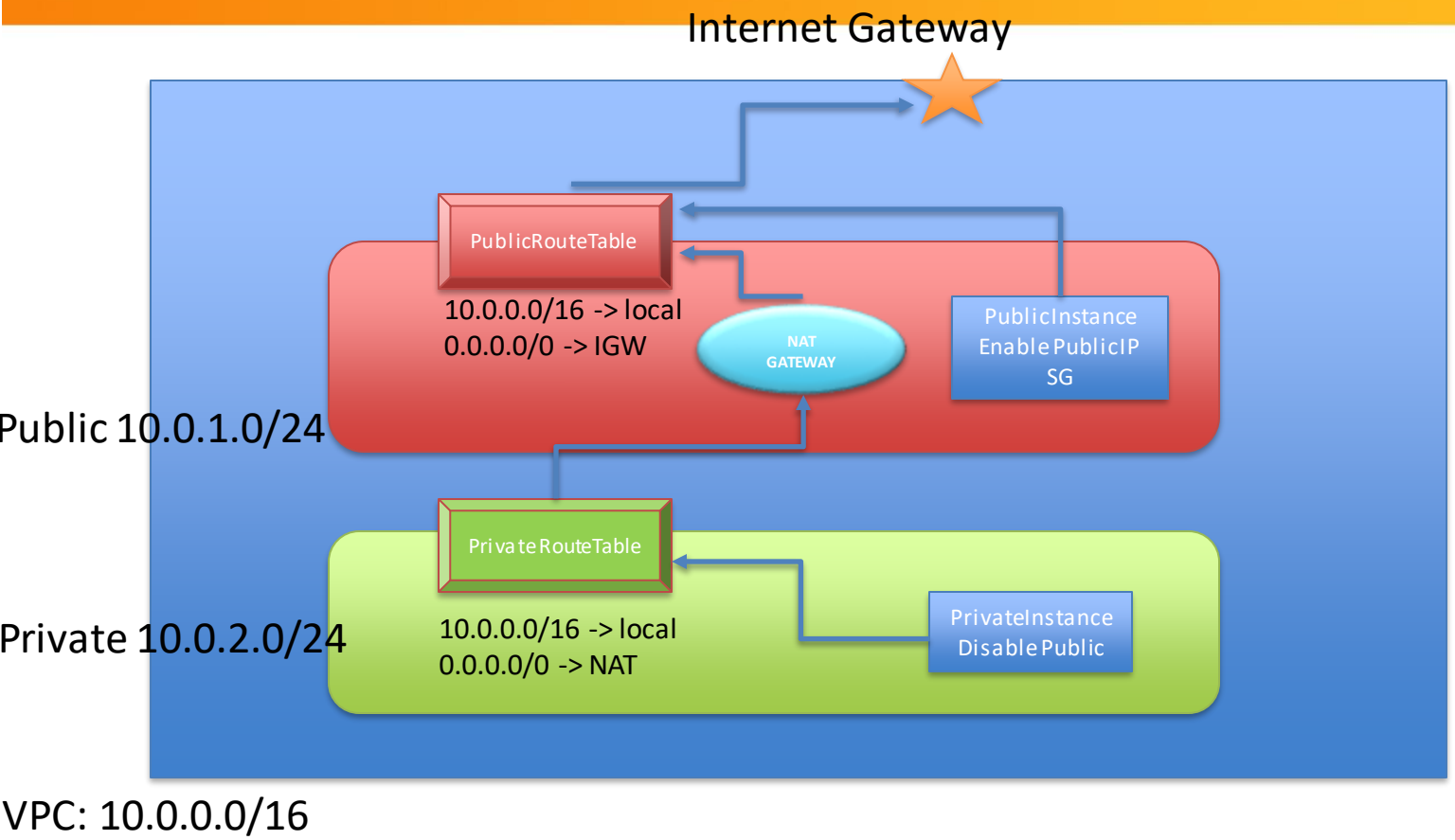
- ➢ Use standard network tools (ping, traceroute, WinMTR) to verify that there is a network issue, not an instance issue
- ➢ Check that the correct route table is attached
- ➢ Check NACLs
- ➢ Check that route table definitions and CIDR ranges are correct
- ➢ If enabled, Check VPC flow logs

❑ NAT configuration doesn't work

- ➢ Is Source/Dest Check disabled?
- ➢ Ensure that NAT has masquerade configured
- ➢ Restart Nat

Troubleshooting Network on AWS

- **Cannot reach resources in peered network**
  - Check routes with traceroute, if no route, verify route table configuration.
  - Check Network ACLs: are you forbidding all external traffic?
    - Create ACLs to allow traffic for allowed peer
  - Check security group configurations on resources
    - Use CIDR block rules in VPC A to allow access from VPC B


Internet Gateway
PublicRouteTable
10.0.0.0/16 -> local
0.0.0.0/0 -> IGW
NAT GATEWAY
PublicInstance
Enable PublicIP
SG
Public 10.0.1.0/24
PrivateRouteTable
10.0.0.0/16 -> local
0.0.0.0/0 -> NAT
PrivateInstance
Disable Public
Private 10.0.2.0/24
VPC: 10.0.0.0/16