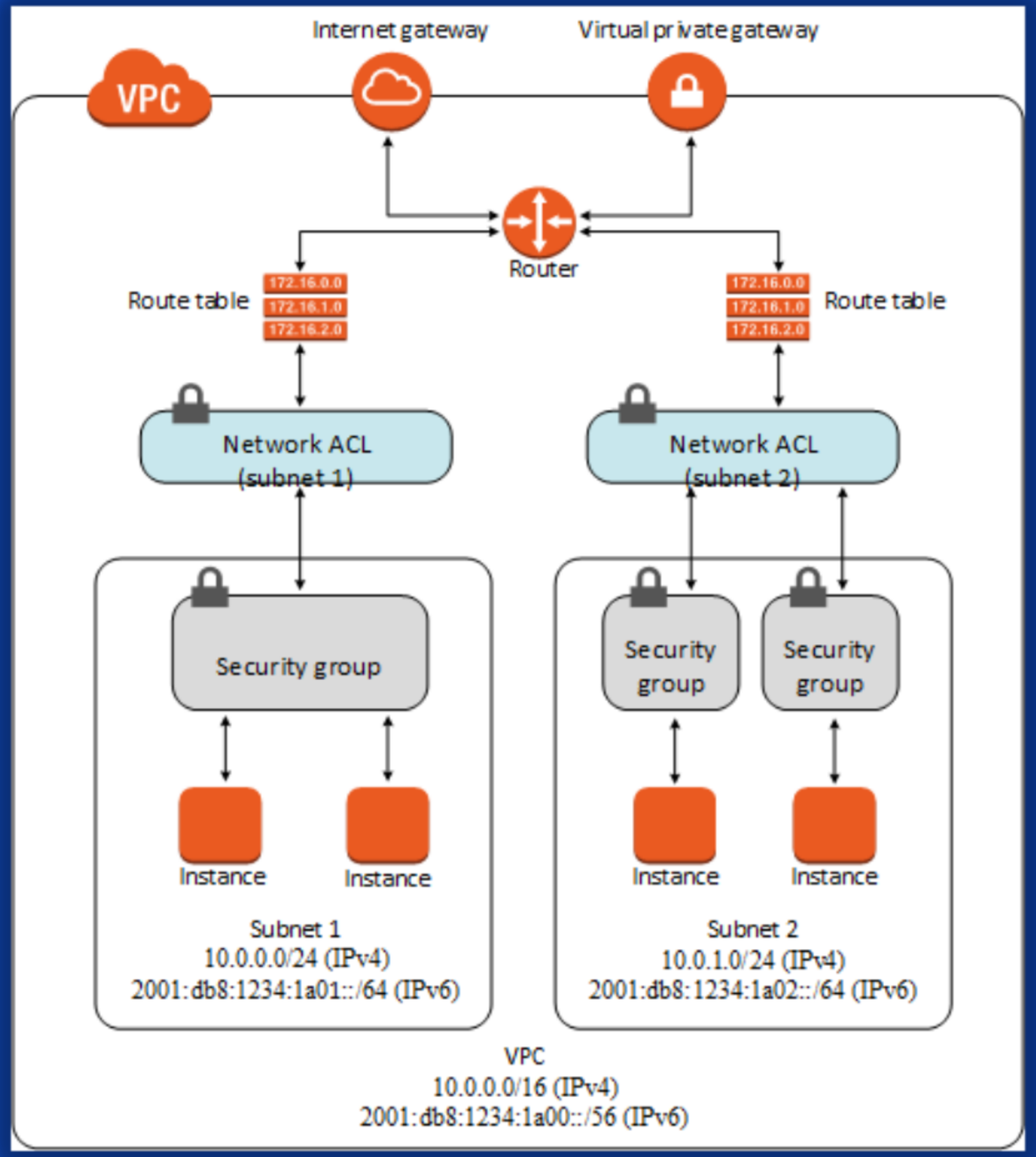
Route Table

Internet gateway

Network ACL

Security Group

Click Here to
Watch Hands-on Demo



What is VPC Route Table?

Your VPC has an implicit router, and you use route tables to control where network traffic is directed. Each subnet in your VPC must be associated with a routing table, which controls the routing for the subnet (subnet route table). You can explicitly associate a subnet with a particular route table. Otherwise, the subnet is implicitly associated with the main route table. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same subnet route table.

Key Concepts

1) **Main route table** - The route table that automatically comes with your VPC. It controls the routing for all subnets that are not explicitly associated with any other route table

2) **Custom route table** - A route table that you create for your VPC.

3) **Route table association** - The association between a route table and a subnet, internet gateway, or virtual private gateway.

4) **Subnet route table** - A route table that's associated with a subnet.

5) **Destination** - The range of IP addresses where you want traffic to go (destination CIDR). For example, an external corporate network with a 172.16.0.0/12 CIDR.

6) **Target** - The gateway, network interface, or connection through which to send the destination traffic; for example, an internet gateway.

7) **Local route** - A default route for communication within the VPC.

What is Internet Gateway?

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.

An internet gateway serves two purposes:

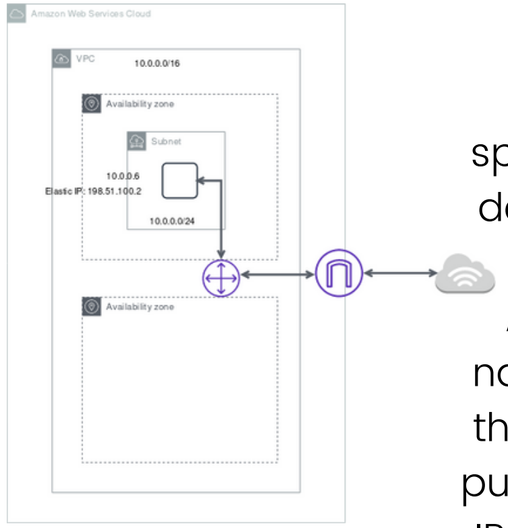
1) to provide a target in your VPC route tables for internet-routable traffic.

2) to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses. For more information, see Enable internet access.

Key Points

1) **Public Subnet:** If a subnet is associated with a route table that has a route to an internet gateway, it's known as a public subnet.

2) **Private Subnet:** If a subnet is associated with a route table that does not have a route to an internet gateway, it's known as a private subnet.



In the public subnet's route table, we can specify a route for the internet gateway to all destinations not explicitly known to the route table (0.0.0.0/0 for IPv4 or ::/0 for IPv6). Alternatively, we can scope the route to a narrower range of IP addresses; for example, the public IPv4 addresses of your company's public endpoints outside of AWS, or the Elastic IP addresses of other Amazon EC2 instances outside your VPC

What is Network ACL?

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Network ACL Rule Components

1) **Rule number**: Rules are evaluated starting with the lowest numbered rule. As soon as a rule matches traffic, it's applied regardless of any higher-numbered rule that might contradict it.

2) **Type:** The type of traffic; for example, SSH. You can also specify all traffic or a custom range.

3) **Protocol:** You can specify any protocol that has a standard protocol number.

4) **Port range**: The listening port or port range for the traffic. For example, 80 for HTTP traffic.

5) **Source**: The source of the traffic (CIDR range).

6) **Destination**. The destination for the traffic (CIDR range).

7) **Allow/Deny:** Whether to allow or deny the specified traffic.

Network ACL

Key Points

- VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic
- We can create a custom network ACL and associate it with a subnet. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
- Each subnet in your VPC must be associated with a network ACL. If we don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL
- We can associate a network ACL with multiple subnets. However, a subnet can be associated with only one network ACL at a time. When we associate a network ACL with a subnet, the previous association is removed.
- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
- Network ACLs are stateless, which means that responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).
- A network ACL contains a numbered list of rules. NACL evaluate the rules in order, starting with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the network ACL. The highest number that we can use for a rule is 32766. It is recommended that we should start by creating rules in increments (for example, increments of 10 or 100) so that you can insert new rules where you need to later on.

Network ACL Example

Custom Network ACL

Inbound						
Rule #	**Type**	**Protocol**	**Port range**	**Source**	**Allow/Deny**	**Comments**
100	HTTP	TCP	80	0.0.0.0/0	ALLOW	Allows inbound HTTP traffic from any IPv4 address.
110	HTTPS	TCP	443	0.0.0.0/0	ALLOW	Allows inbound HTTPS traffic from any IPv4 address.
120	SSH	TCP	22	192.0.2.0/24	ALLOW	Allows inbound SSH traffic from your home network's public IPv4 address range (over the internet gateway).
130	RDP	TCP	3389	192.0.2.0/24	ALLOW	Allows inbound RDP traffic to the web servers from your home network's public IPv4 address range (over the internet gateway).
Outbound						
Rule #	**Type**	**Protocol**	**Port range**	**Destination**	**Allow/Deny**	**Comments**
100	HTTP	TCP	80	0.0.0.0/0	ALLOW	Allows outbound IPv4 HTTP traffic from the subnet to the internet.
110	HTTPS	TCP	443	0.0.0.0/0	ALLOW	Allows outbound IPv4 HTTPS traffic from the subnet to the internet.
120	SSH	TCP	22	192.0.2.0/24	ALLOW	Allows outbound SSH traffic from your home network's public IPv4 address range (over the internet gateway).
140	Custom TCP	TCP	32768-65535	0.0.0.0/0	ALLOW	Allows outbound IPv4 responses to clients on the internet (for example, serving webpages to people visiting the web servers

Default Network ACL

Inbound					
Rule #	**Type**	**Protocol**	**Port range**	**Source**	**Allow/Deny**
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY
Outbound					
Rule #	**Type**	**Protocol**	**Port range**	**Destination**	**Allow/Deny**
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

- The default network ACL is configured to allow all traffic to flow in and out of the subnets with which it is associated. Each network ACL also includes a rule whose rule number is an asterisk. This rule ensures that if a packet doesn't match any of the other numbered rules, it's denied. You can't modify or remove this rule.

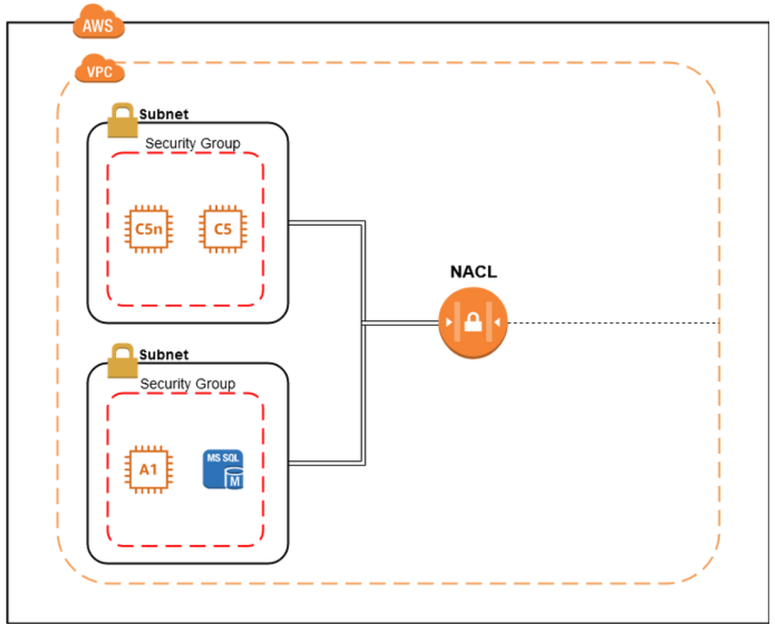
- The left table shows an example of a custom network ACL for a VPC that supports IPv4 only. It includes rules that allow HTTP and HTTPS traffic in (inbound rules 100 and 110). There's a corresponding outbound rule that enables responses to that inbound traffic (outbound rule 140, which covers ephemeral ports 32768-65535)

What is Security Group?

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be assigned to a different set of security groups.

Key Points

- We can specify allow rules, but not deny rules.
- We can specify separate rules for inbound and outbound traffic.
- Security group rules enable you to filter traffic based on protocols and port numbers.



- Security groups are stateful — if we send a request from our instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.
- When we first create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to the instance is allowed until you add inbound rules to the security group and vise e versa for outbound rules, no rules mentioned, it will not allow any outbound traffic.
- Instances associated with a security group can't talk to each other unless you add rules allowing the traffic (exception: the default security group has these rules by default)

Security Group Example

Custom Security Group

Inbound			
Source	**Protocol**	**Port range**	**Description**
0.0.0.0/0	TCP	80	Allow inbound HTTP access from all IPv4 addresses
::/0	TCP	80	Allow inbound HTTP access from all IPv6 addresses
0.0.0.0/0	TCP	443	Allow inbound HTTPS access from all IPv4 addresses
::/0	TCP	443	Allow inbound HTTPS access from all IPv6 addresses
Your network's public IPv4 address range	TCP	22	Allow inbound SSH access to Linux instances from IPv4 IP addresses in your network (over the internet gateway)
Your network's public IPv4 address range	TCP	3389	Allow inbound RDP access to Windows instances from IPv4 IP addresses in your network (over the internet gateway)
Outbound			
Destination	**Protocol**	**Port range**	**Description**
The ID of the security group for your Microsoft SQL Server database servers	TCP	1433	Allow outbound Microsoft SQL Server access to instances in the specified security group
The ID of the security group for your MySQL database servers	TCP	3306	Allow outbound MySQL access to instances in the specified security group

The following table describes example rules for a security group that's associated with web servers. The web servers can receive HTTP and HTTPS traffic from all IPv4 and IPv6 addresses and can send SQL or MySQL traffic to a database server.

Default Security Group

Inbound			
Source	**Protocol**	**Port range**	**Description**
The security group ID (sg-*xxxxxxxx*)	All	All	Allow inbound traffic from network interfaces (and their associated instances) that are assigned to the same security group.
Outbound			
Destination	**Protocol**	**Port range**	**Description**
0.0.0.0/0	All	All	Allow all outbound IPv4 traffic.
::/0	All	All	Allow all outbound IPv6 traffic. This rule is added by default if you create a VPC with an IPv6 CIDR block or if you associate an IPv6 CIDR block with your existing VPC.

Each VPC automatically comes with a default security group. If we don't specify a different security group when you launch the instance, the default security group gets associated with your instance.

Security Group Vs Network ACL

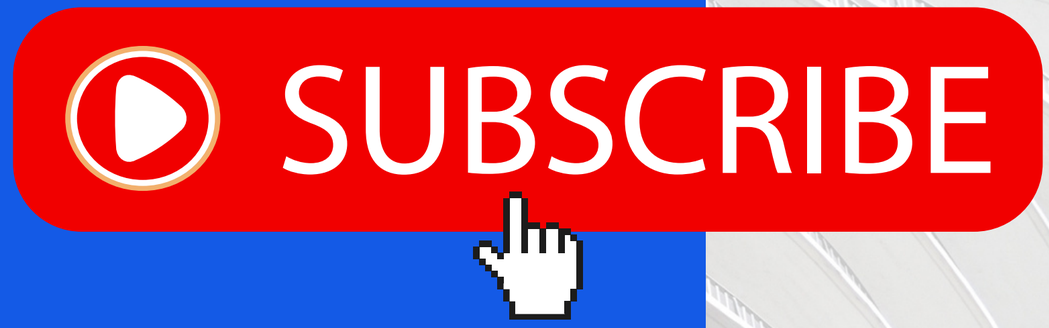
Security Group

- Operates at the instance level
- Supports allow rules only
- Is stateful: Return traffic is automatically allowed, regardless of any rules
- We evaluate all rules before deciding whether to allow traffic
- Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on

Network ACL

- Operates at the subnet level
- Supports allow rules and deny rules
- Is stateless: Return traffic must be explicitly allowed by rules
- We process rules in order, starting with the lowest numbered rule, when deciding whether to allow traffic
- Automatically applies to all instances in the subnets that it's associated with (therefore, it provides an additional layer of defense if the security group rules are too permissive)

Thank You



See Your in my next Session