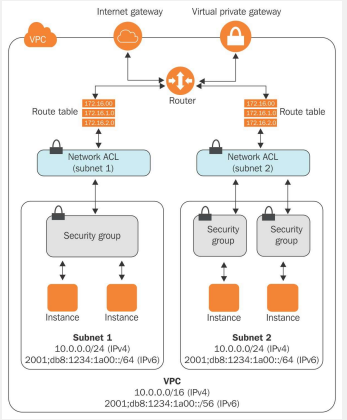
CLOUD COMPUTING APPLICATIONS

VPC: Security and Firewalls

Prof. Reza Farivar

Security and Firewalls

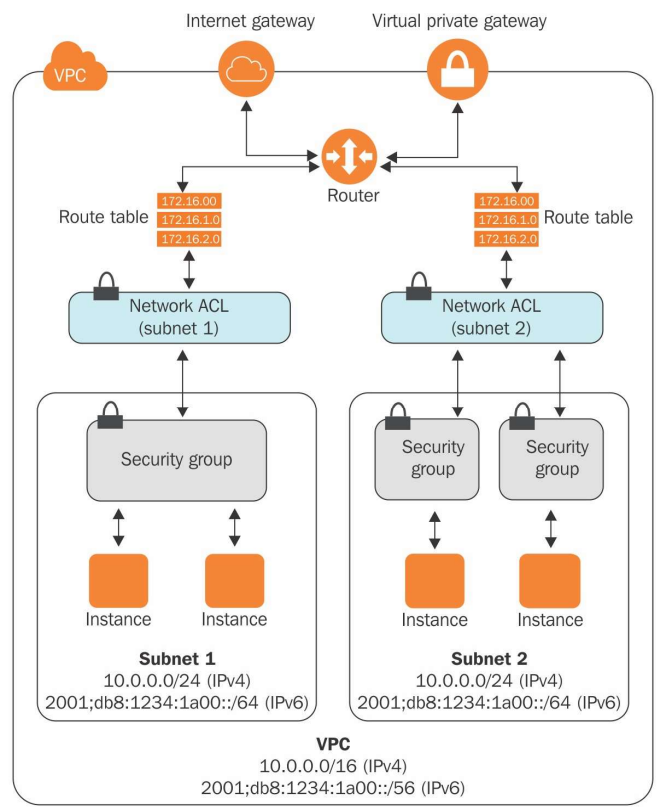
- Security
  - Security Groups
    - EC2 instance-level firewall
  - Network Access Control Lists (NACL)
    - Subnet firewall
- Monitoring
  - Flow Logs
  - Enable VPC flow logs for audit purposes
  - Study flow logs from time to time
    - highlights unauthorized attempts to access the resources



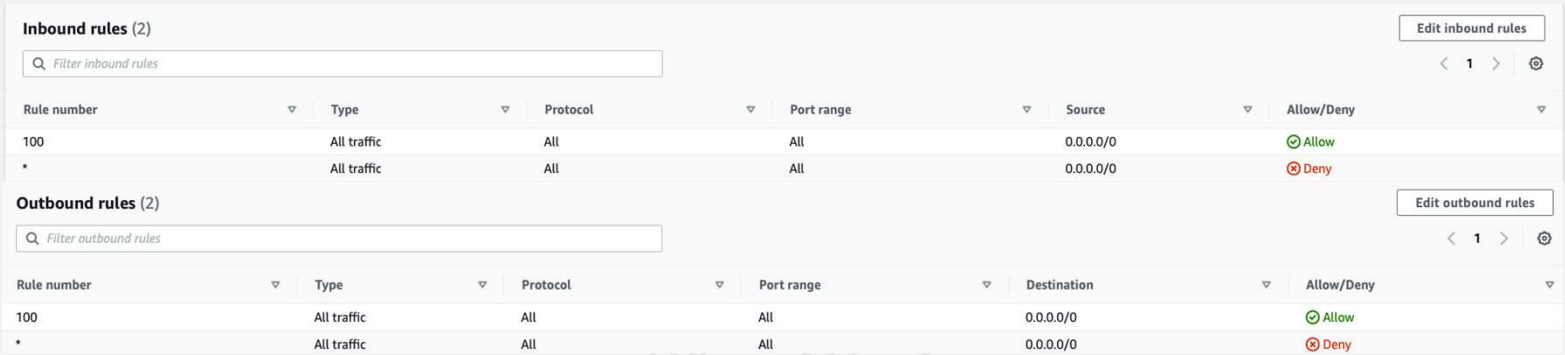
Security

- Make sure that only required ports and protocols from trusted sources can access AWS resources using security groups and NACLs
- Make sure that unwanted outgoing ports are not open in security groups
  - A security group for a web application does not need to open incoming mail server ports

Security and Firewalls



Network Access Control List



Inbound rules (2)

Edit inbound rules

Filter inbound rules

1

Rule number	Type	Protocol	Port range	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 rules (2)

Edit outbound rules

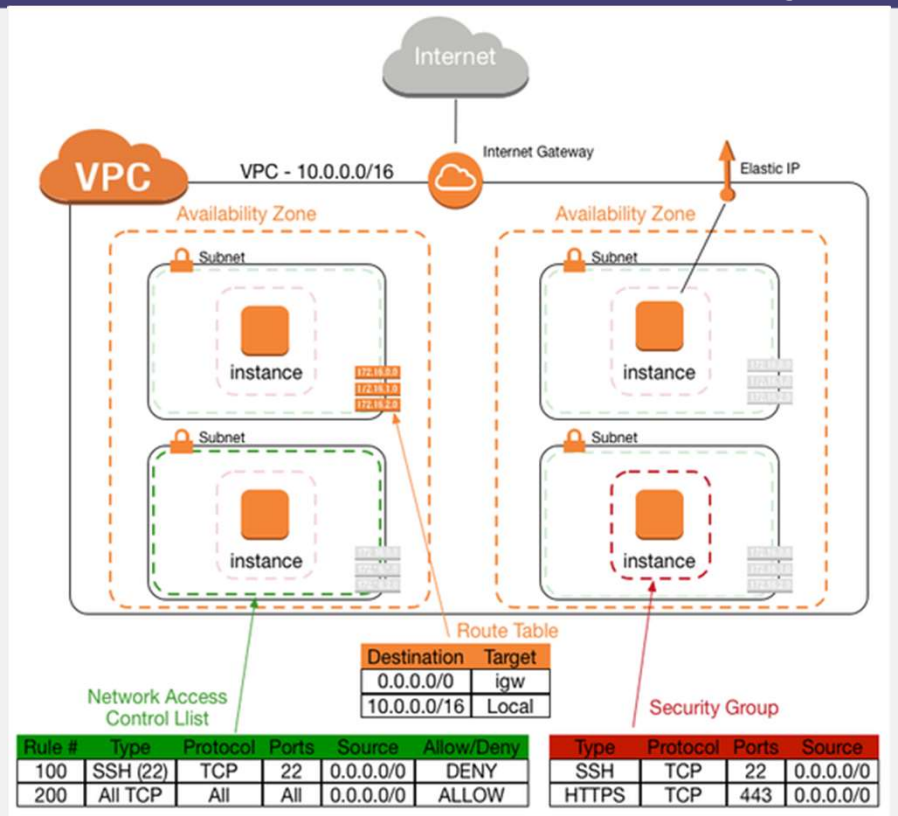
Filter outbound rules

1

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

- NACL acts as a virtual firewall at the subnet level
- Every VPC has a default NACL
- Every subnet, whether it is private or public in a VPC, must be associated to one NACL
- One NACL can be associated with one or more subnets; but each subnet can have ONE NACL associated with it
- NACL rules are evaluated based on its rule numbers. It evaluates the rule starting from the lowest number to the highest number
- NACL is stateless:
  - Separate rules to allow or deny can be created for inbound and outbound traffic
  - If a port is open for allowing inbound traffic, it does not automatically allow outbound traffic
- The default NACL for any VPC contains a rule numbered as * in both inbound and outbound rules
  - This rule appears and executes last

Anatomy of a VPC with Route Table, Network ACL and Security Group



Security Group

Inbound rules — Edit inbound rules

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	0.0.0.0/0	-
HTTP	TCP	80	::/0	-
Custom TCP	TCP	8080	0.0.0.0/0	-
Custom TCP	TCP	8080	::/0	-
SSH	TCP	22	0.0.0.0/0	-
SSH	TCP	22	::/0	-
HTTPS	TCP	443	0.0.0.0/0	-
HTTPS	TCP	443	::/0	-

Outbound rules — Edit outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	0.0.0.0/0	-

- Firewall at the instance level
- One or more security groups can be associated with each EC2 instance
- A security group can be attached to many EC2 instances
- Each SG contains rules allowing inbound and outbound traffic
- Using CIDR notation, a source IP can be fixed to a particular IP, such as 10.108.20.107/32
- Any source IP can be allowed by a 0.0.0.0/0

Security Group as Source IP

Inbound rules Edit inbound rules

Type	Protocol	Port range	Source	Description - optional
Custom TCP	TCP	4003 - 65535	sg-00fbbeba74e062d16 (nodes.dev.k8s.mp3-k8.in)	-
Custom TCP	TCP	2382 - 4000	sg-00fbbeba74e062d16 (nodes.dev.k8s.mp3-k8.in)	-
All traffic	All	All	sg-003e7c9121913dca3 (masters.dev.k8s.mp3-k8.in)	-
SSH	TCP	22	0.0.0.0/0	-
Custom UDP	UDP	1 - 65535	sg-00fbbeba74e062d16 (nodes.dev.k8s.mp3-k8.in)	-
Custom TCP	TCP	1 - 2379	sg-00fbbeba74e062d16 (nodes.dev.k8s.mp3-k8.in)	-
HTTPS	TCP	443	0.0.0.0/0	-

- A security group ID can be specified as a source IP to allow communication from all the instances that are attached to that security group
- For example, in the case of autoscaling, the number of EC2 instances and their IP addresses keeps changing.
- In such situations, it is best practice to attach a security group to such EC2 instances with the help of an autoscaling template and place a security group ID as a source IP in another security group.