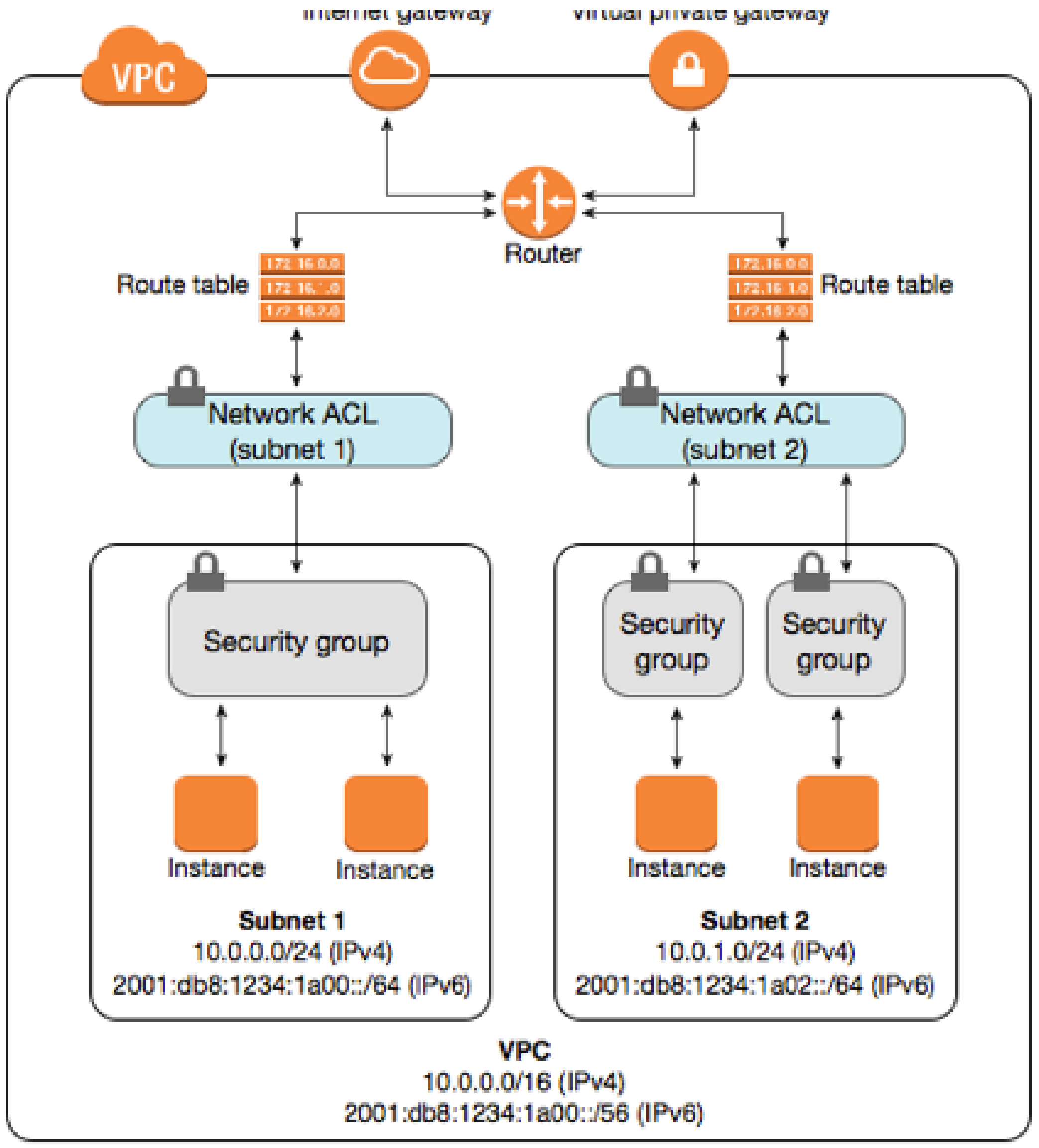
CloudSiksha

NACL

Note: All images taken for AWS Website

CloudSiksha

Network Access Control List



Network ACL

- Acts as a firewall
- Controls traffic in and out of subnets
- Default Network ACL created when VPC is created
  - Attached to all subnets initially
  - Allows all traffic to flow in both directions

Custom NACL

- Custom NACL can be attached to any subnet
  - **Default custom NACL will block all traffic**
  - **Need to put in rules to allow traffic**
- Each subnet will be associated with one NACL
  - **If no custom NACL specified will be associated with default NACL**
- One subnet one NACL
  - **One NACL can be associated with multiple subnets**

NACL Rules

- Each rule has a number
- Evaluated from lowest number to highest
  - **32766 is the highest number that can be used**
- Evaluation stops when a rule is satisfied
  - **Need to careful when writing rules else there could unintended consequences**
- Inbound and Outbound rules
- NACL is stateless

NACL Inbound Rules

Inbound Rules

Rule #	Type	Protocol	Port Range	Source	Allow/Deny	Comments
100	HTTP	TCP	80	0.0.0.0/0	Allow	Allow all traffic to this subnet
200	MySQL	TCP	3306	10.0.1.0/24	Deny	Deny traffic from 10.0.1.0/24 subnet
300	MySQL	TCP	3306	0.0.0.0/0	Allow	Allow MySQL traffic
400	SSH	TCP	22	10.0.2.0/24	Deny	Explicitly Deny SSH traffic from 10.0.2.0/24 subnet
500	SSH	TCP	22	0.0.0.0/0	Allow	Allow all SSH traffic
*	All Traffic	All	All	0.0.0.0/0	Deny	Default rule present in all NACL

NACL Outbound Rules

Outbound Rules

Rule #	Type	Protocol	Port Range	Destination	Allow/Deny	Comments
100	Custom TCP	TCP	1024-65535	0.0.0.0/0	Allow	Open all higher ports for response
200	SSH	TCP	22	10.0.1.0/24	Allow	Allow SSH to 10.0.1.0/24 subnet
300	RDP	TCP	3389	10.0.1.0/24	Deny	Explicitly deny all RDP traffic to 10.0.1.0/24 subnet
400	RDP	TCP	3389	0.0.0.0/0	Allow	Allow all RDP traffic
*	All Traffic	All	All	0.0.0.0/0	Deny	Default rule present in all NACL

NACL vs Security Groups

Security Group	NACL
Instance Level security	Subnet Level Security
Stateful (Understands difference between request and response)	Stateless (Inbound and Outbound rules must be specified)
All rules are evaluated	Evaluated from smallest rule number. Evaluation stopped when condition is matched
Permissive (Only Allow rules)	Allow and Deny rules
More than one security group can be attached to an instance	Only one NACL per subnet

CloudSiksha

Thanks