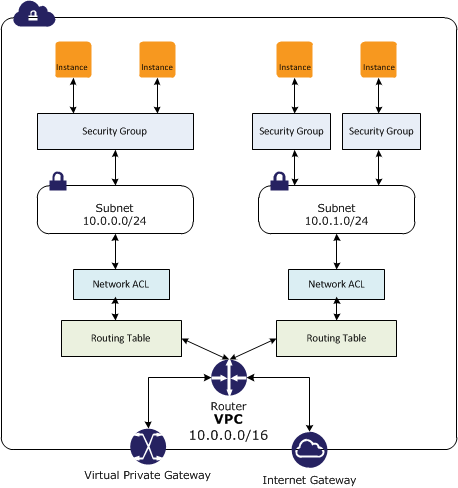
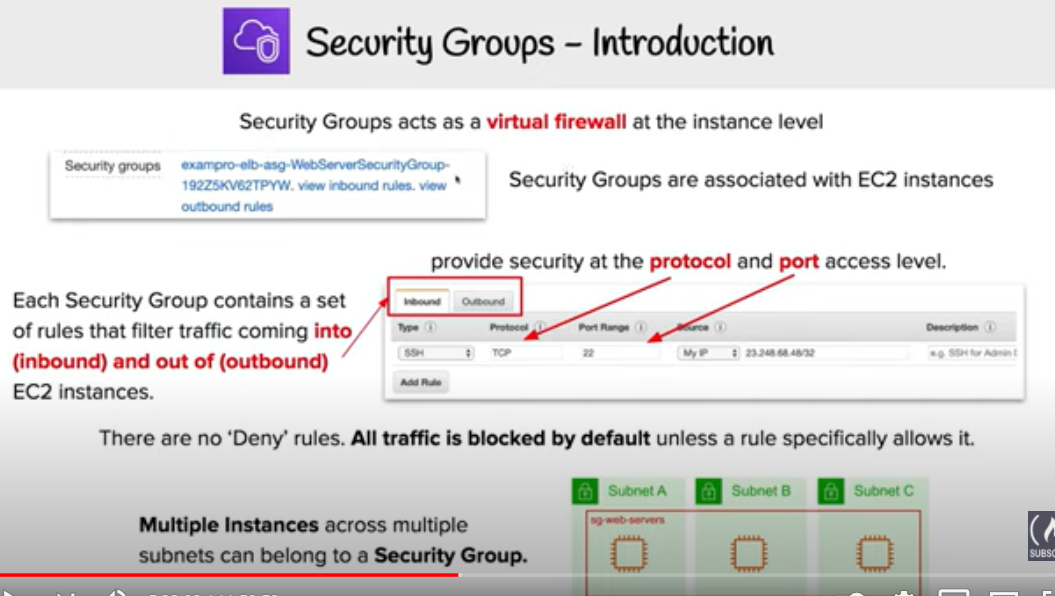
AWS VPC Security – Security Group vs NACLs

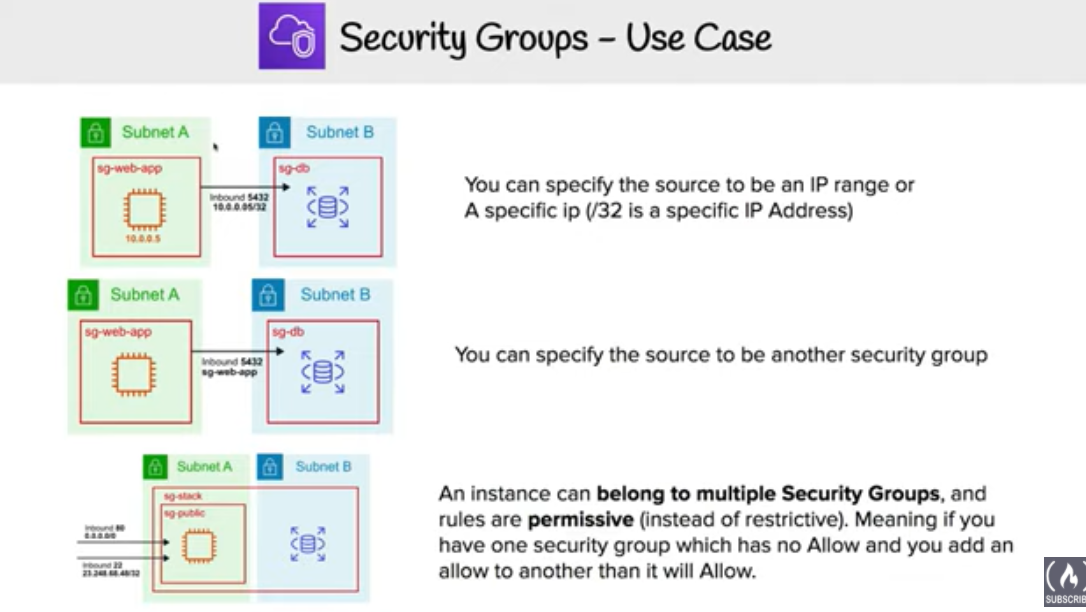
# AWS VPC Security Overview

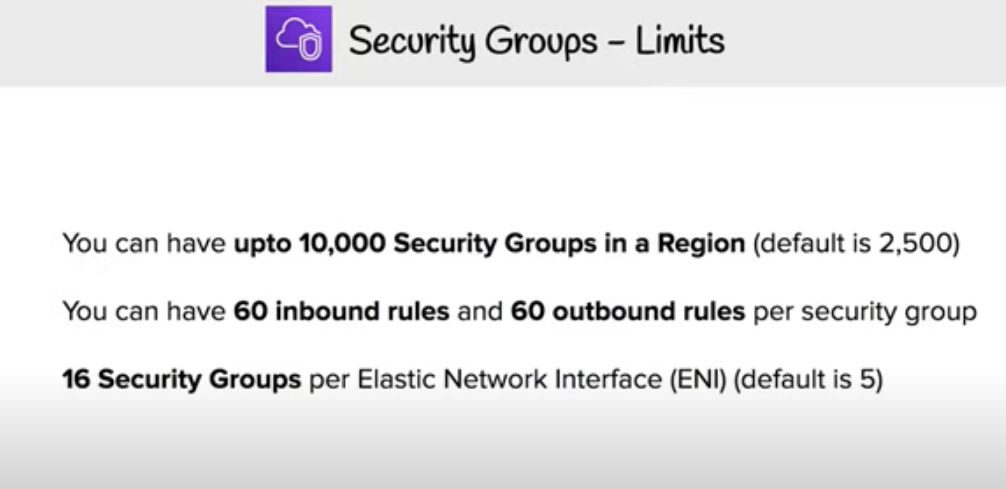
* In a VPC, both Security Groups and Network ACLs (NACLS) together help to build a layered network defense.
* **Security groups** – Act as a **virtual firewall** for **associated instances**, controlling both inbound and outbound traffic at the instance level
* **Network access control lists (NACLs)** – Act as a firewall for **associated subnets**, controlling both inbound and outbound traffic at the subnet level



## Security Groups





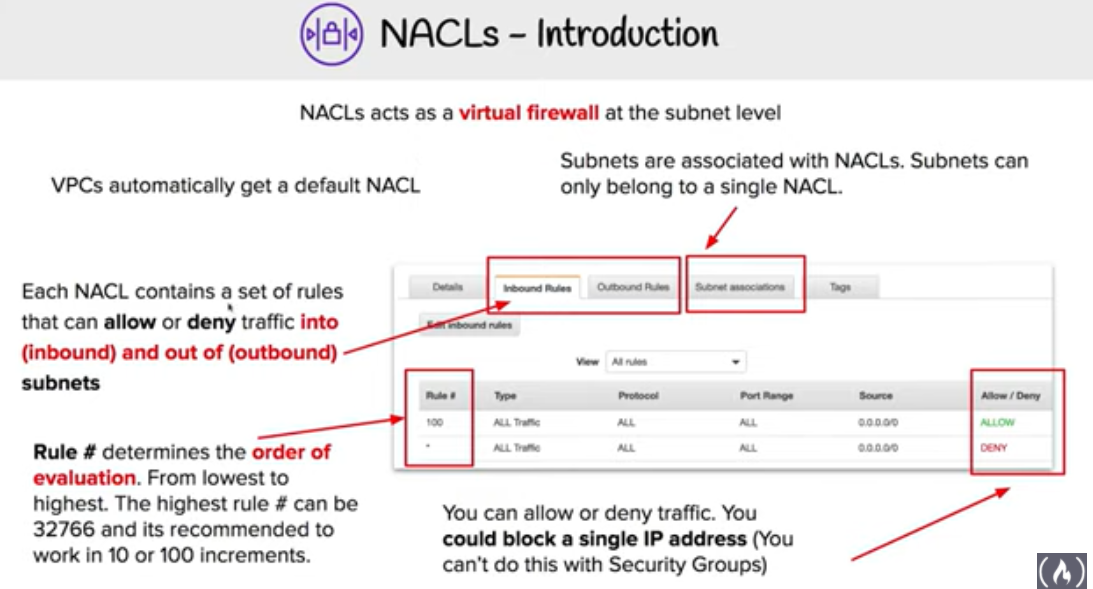


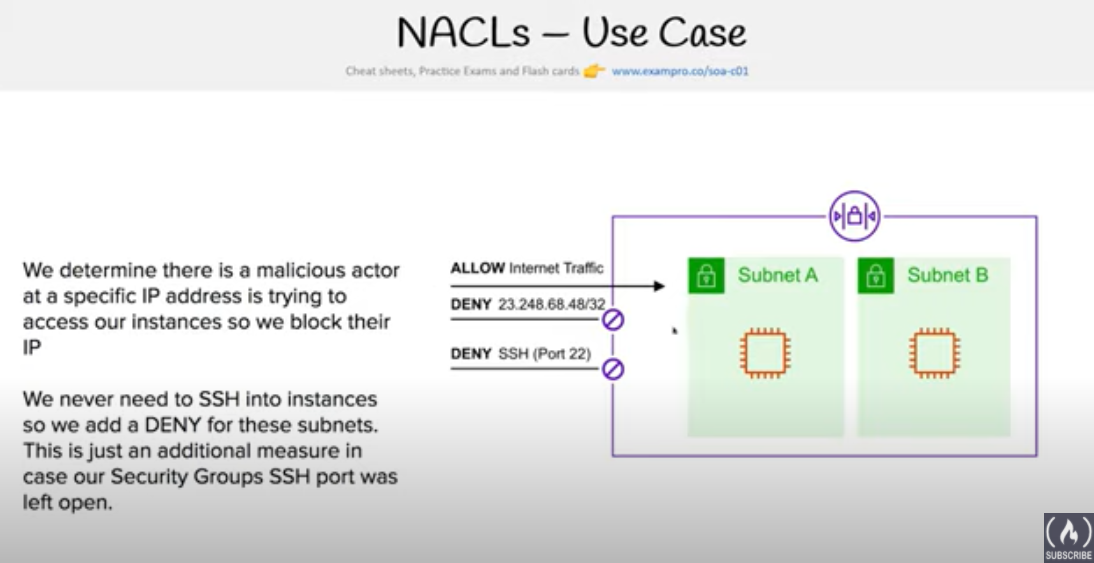
* Acts at an Instance level and not at the subnet level.
* Each instance within a subnet can be assigned a different set of Security groups
* An instance can be assigned 5 security groups with each security group having  60 rules
* allows separate rules for inbound and outbound traffic
* allows adding or removing rules (authorizing or revoking access) for both Inbound (ingress) and Outbound (egress) traffic to the instance
  + **Default** Security group allows **no external inbound traffic** but allows inbound traffic from instances with the same security group
  + **Default** Security group **allows all outbound traffic**
  + New Security groups start with only an outbound rule that allows all traffic to leave the instances
* can **specify only Allow rules, but not deny rules**
* **can grant access to a specific IP, CIDR range, or to another security group in the VPC or in a peer VPC (requires a VPC peering connection)**
* are **evaluated as a Whole or Cumulative bunch of rules** with the most permissive rule taking precedence for e.g. if you have a rule that allows access to TCP port 22 (SSH) from IP address 203.0.113.1 and another rule that allows access to TCP port 22 from everyone, everyone has access to TCP port 22.
* are **Stateful –**responses to allowed inbound traffic are allowed to flow outbound regardless of outbound rules, and vice versa. Hence an Outbound rule for the response is not needed
* Instances associated with a security group **can’t talk to each other** unless rules allowing the traffic are added.
* are associated with ENI (network interfaces).
* are associated with the instance and can be changed, which changes the security groups associated with the primary network interface (eth0) and the changes would be applicable immediately to all the instances associated with the Security group

### Connection Tracking

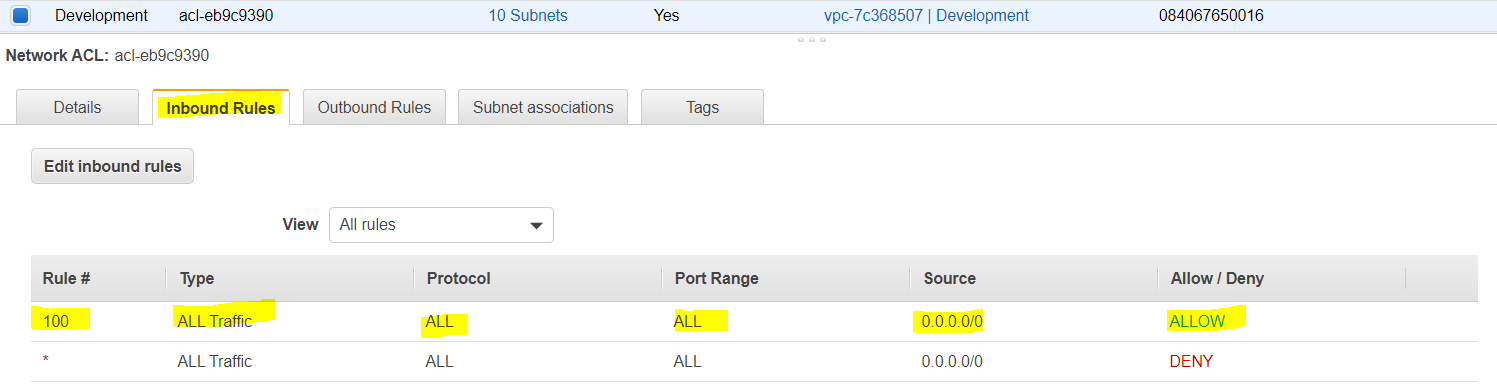
* **Security groups are Stateful as they use Connection tracking to track information about traffic to and from the instance.**
* **Responses to inbound traffic are allowed to flow out of the instance regardless of outbound security group rules, and vice versa.**
* Connection Tracking is maintained only if there is no explicit Outbound rule for an Inbound request (and vice versa)
* However, if there is an explicit Outbound rule for an Inbound request, the response traffic is allowed on the basis of the Outbound rule and not on the Tracking information
* **Tracking flow e.g.**
  + **If an instance (host A) initiates traffic to host B and uses a protocol other than TCP, UDP, or ICMP, the instance’s firewall only tracks the IP address & protocol number for the purpose of allowing response traffic from host B.**
  + If host B initiates traffic to the instance in a separate request within 600 seconds of the original request or response, the instance accepts it regardless of inbound security group rules, because it’s regarded as response traffic.
* **This can be controlled by modifying the security group’s outbound rules to permit only certain types of outbound traffic. Alternatively, Network ACLs (NACLs) can be used for the subnet, network ACLs are stateless and therefore do not automatically allow response traffic.**

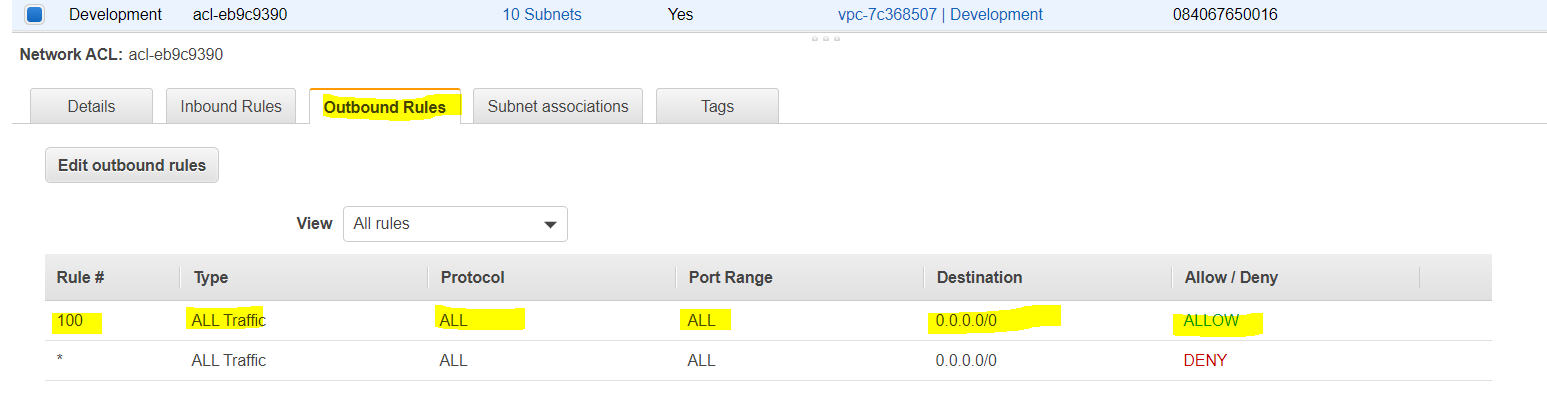
## Network Access Control Lists – NACLs



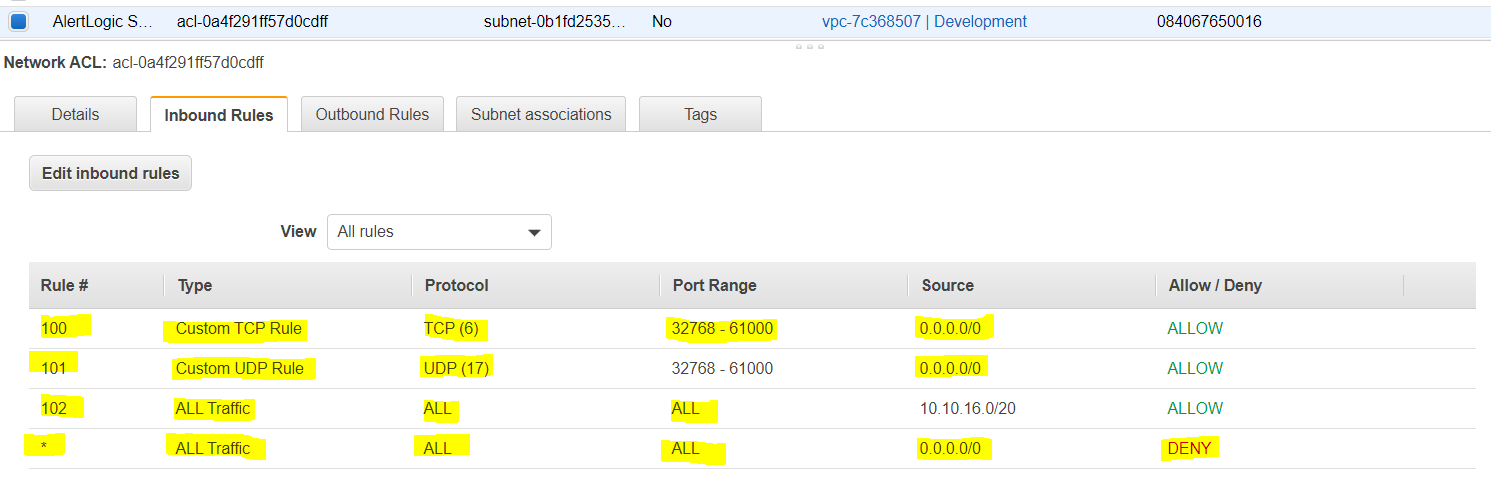


* A Network ACLs (NACLs) is an optional layer of security for the VPC that acts as a **firewall for controlling traffic in and out of one or more subnets**.
* are not for granular control and are assigned at a Subnet level and is **applicable to all the instances in that Subnet**
* has separate inbound and outbound rules, and each rule can either **allow or deny traffic.**
  + **Default ACL allows all inbound and outbound traffic.**

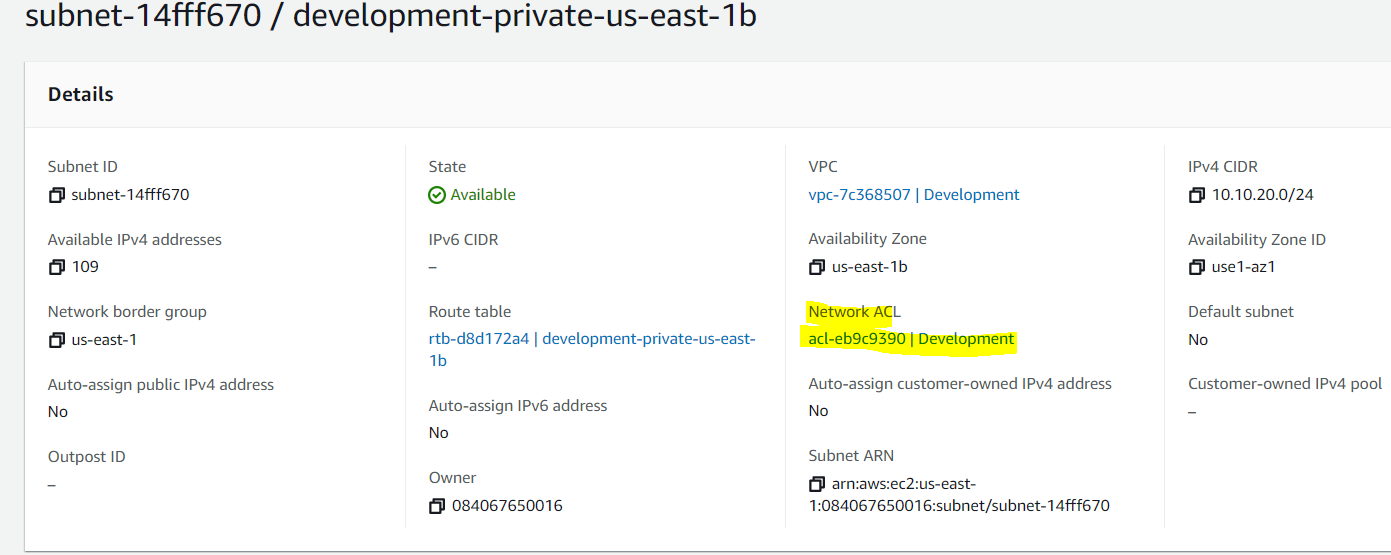




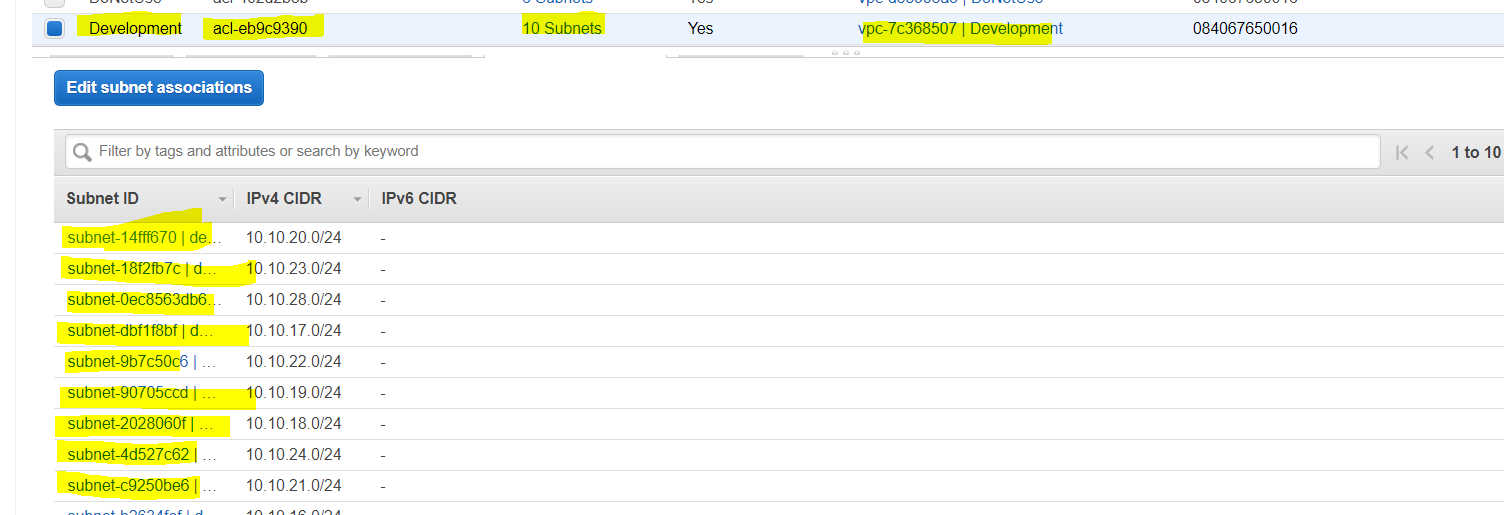
* + **Newly created ACL denies all inbound and outbound traffic**



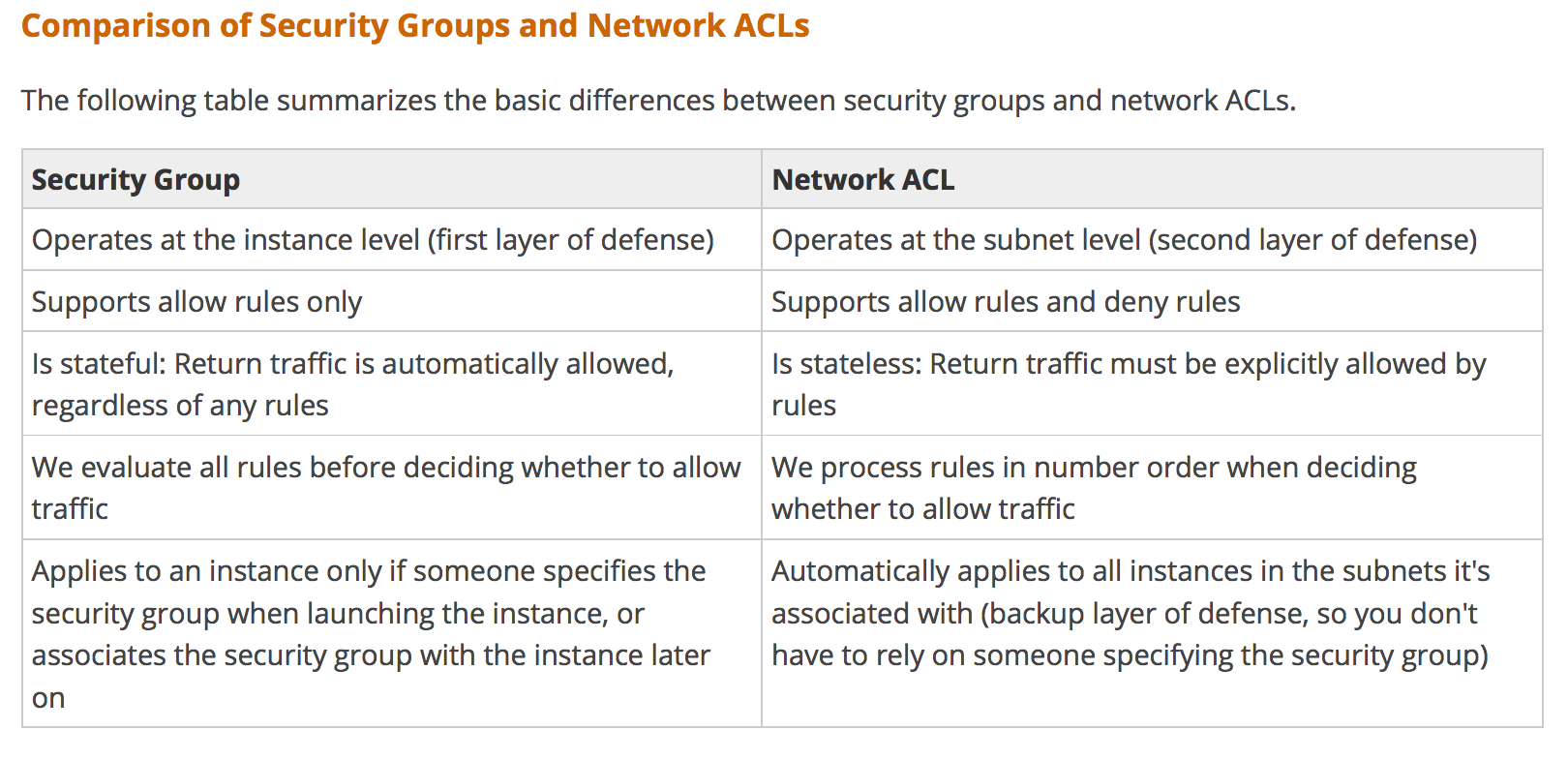
* **A Subnet can be assigned only 1 NACLs** and if not associated explicitly would be associated implicitly with the default NACL.



* can associate a **network ACL with multiple subnets**



* **is a numbered list of rules that are evaluated 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 for e.g. if you have a Rule No. 100 with Allow All and 110 with Deny All, the Allow All would take precedence and all the traffic will be allowed**
* are **Stateless**; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa) for e.g. if you enable Inbound SSH on port 22 from the specific IP address, you would need to add an Outbound rule for the response as well.



## AWS Certification Exam Practice Questions

1. Instance A and instance B are running in two different subnets A and B of a VPC. Instance A is not able to ping instance B. What are two possible reasons for this? (Pick 2 correct answers)
   1. The routing table of subnet A has no target route to subnet B
   2. **The security group attached to instance B does not allow inbound ICMP traffic**
   3. The policy linked to the IAM role on instance A is not configured correctly
   4. **The NACL on subnet B does not allow outbound ICMP traffic**
2. An instance is launched into a VPC subnet with the network ACL configured to allow all inbound traffic and deny all outbound traffic. The instance’s security group is configured to allow SSH from any IP address and deny all outbound traffic. What changes need to be made to allow SSH access to the instance?
   1. The outbound security group needs to be modified to allow outbound traffic.
   2. **The outbound network ACL needs to be modified to allow outbound traffic.**
   3. Nothing, it can be accessed from any IP address using SSH.
   4. Both the outbound security group and outbound network ACL need to be modified to allow outbound traffic.
3. From what services I can block incoming/outgoing IPs?
   1. Security Groups
   2. DNS
   3. ELB
   4. VPC subnet
   5. IGW
   6. **NACL**
4. What is the difference between a security group in VPC and a network ACL in VPC (chose 3 correct answers)
   1. Security group restricts access to a Subnet while ACL restricts traffic to EC2
   2. **Security group restricts access to EC2 while ACL restricts traffic to a subnet**
   3. Security group can work outside the VPC also while ACL only works within a VPC
   4. **Network ACL performs stateless filtering and Security group provides stateful filtering**
   5. **Security group can only set Allow rule, while ACL can set Deny rule also**
5. You are currently hosting multiple applications in a VPC and have logged numerous port scans coming in from a specific IP address block. Your security team has requested that all access from the offending IP address block be denied for the next 24 hours. Which of the following is the best method to quickly and temporarily deny access from the specified IP address block?
   1. Create an AD policy to modify Windows Firewall settings on all hosts in the VPC to deny access from the IP address block
   2. **Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP address block**
   3. Add a rule to all of the VPC 5 Security Groups to deny access from the IP address block
   4. Modify the Windows Firewall settings on all Amazon Machine Images (AMIs) that your organization uses in that VPC to deny access from the IP address block
6. You have two Elastic Compute Cloud (EC2) instances inside a Virtual Private Cloud (VPC) in the same Availability Zone (AZ) but in different subnets. One instance is running a database and the other instance an application that will interface with the database. You want to confirm that they can talk to each other for your application to work properly. Which two things do we need to confirm in the VPC settings so that these EC2 instances can communicate inside the VPC? Choose 2 answers
   1. **A network ACL that allows communication between the two subnets.**
   2. Both instances are the same instance class and using the same Key-pair.
   3. That the default route is set to a NAT instance or Internet Gateway (IGW) for them to communicate.
   4. **Security groups are set to allow the application host to talk to the database on the right port/protocol**
7. A benefits enrollment company is hosting a 3-tier web application running in a VPC on AWS, which includes a NAT (Network Address Translation) instance in the public Web tier. There is enough provisioned capacity for the expected workload tor the new fiscal year benefit enrollment period plus some extra overhead Enrollment proceeds nicely for two days and then the web tier becomes unresponsive, upon investigation using CloudWatch and other monitoring tools it is discovered that there is an extremely large and unanticipated amount of inbound traffic coming from a set of 15 specific IP addresses over port 80 from a country where the benefits company has no customers. The web tier instances are so overloaded that benefit enrollment administrators cannot even SSH into them. Which activity would be useful in defending against this attack?
   1. Create a custom route table associated with the web tier and block the attacking IP addresses from the IGW (internet Gateway)
   2. Change the EIP (Elastic IP Address) of the NAT instance in the web tier subnet and update the Main Route Table with the new EIP
   3. Create 15 Security Group rules to block the attacking IP addresses over port 80
   4. **Create an inbound NACL (Network Access control list) associated with the web tier subnet with deny rules to block the attacking IP addresses**
8. Which of the following statements describes network ACLs? (Choose 2 answers)
   1. Responses to allowed inbound traffic are allowed to flow outbound regardless of outbound rules, and vice versa (are stateless)
   2. **Using network ACLs, you can deny access from a specific IP range**
   3. **Keep network ACL rules simple and use a security group to restrict application level access**
   4. NACLs are associated with a single Availability Zone (associated with Subnet)
9. You are designing security inside your VPC. You are considering the options for establishing separate security zones and enforcing network traffic rules across different zone to limit Instances can communications.  How would you accomplish these requirements? Choose 2 answers
   1. Configure a security group for every zone. Configure a default allow all rule. Configure explicit deny rules for the zones that shouldn’t be able to communicate with one another (Security group does not allow deny rules)
   2. **Configure you instances to use pre-set IP addresses with an IP address range every security zone. Configure NACL to explicitly allow or deny communication between the different IP address ranges, as required for interzone communication**
   3. **Configure a security group for every zone. Configure allow rules only between zone that need to be able to communicate with one another. Use implicit deny all rule to block any other traffic**
   4. Configure multiple subnets in your VPC, one for each zone. Configure routing within your VPC in such a way that each subnet only has routes to other subnets with which it needs to communicate, and doesn’t have routes to subnets with which it shouldn’t be able to communicate. (default routes are unmodifiable)
10. Your entire AWS infrastructure lives inside of one Amazon VPC. You have an Infrastructure monitoring application running on an Amazon instance in Availability Zone (AZ) A of the region, and another application instance running in AZ B. The monitoring application needs to make use of ICMP ping to confirm network reachability of the instance hosting the application. Can you configure the security groups for these instances to only allow the ICMP ping to pass from the monitoring instance to the application instance and nothing else” If so how?
    1. No Two instances in two different AZ’s can’t talk directly to each other via ICMP ping as that protocol is not allowed across subnet (i.e. broadcast) boundaries (Can communicate)
    2. Yes Both the monitoring instance and the application instance have to be a part of the same security group, and that security group needs to allow inbound ICMP (Need not have to be part of same security group)
    3. **Yes, The security group for the monitoring instance needs to allow outbound ICMP and the application instance’s security group needs to allow Inbound ICMP**(is stateful, so just allow outbound ICMP from monitoring and inbound ICMP on monitored instance)
    4. Yes, Both the monitoring instance’s security group and the application instance’s security group need to allow both inbound and outbound ICMP ping packets since ICMP is not a connection-oriented protocol (Security groups are stateful)
11. A user has configured a VPC with a new subnet. The user has created a security group. The user wants to configure that instances of the same subnet communicate with each other. How can the user configure this with the security group?
    1. There is no need for a security group modification as all the instances can communicate with each other inside the same subnet
    2. Configure the subnet as the source in the security group and allow traffic on all the protocols and ports
    3. **Configure the security group itself as the source and allow traffic on all the protocols and ports**
    4. The user has to use VPC peering to configure this
12. You are designing a data leak prevention solution for your VPC environment. You want your VPC Instances to be able to access software depots and distributions on the Internet for product updates. The depots and distributions are accessible via third party CDNs by their URLs. You want to explicitly deny any other outbound connections from your VPC instances to hosts on the Internet. Which of the following options would you consider?
    1. **Configure a web proxy server in your VPC and enforce URL-based rules for outbound access Remove default routes.**(Security group and NACL cannot have URLs in the rules nor does the route)
    2. Implement security groups and configure outbound rules to only permit traffic to software depots.
    3. Move all your instances into private VPC subnets remove default routes from all routing tables and add specific routes to the software depots and distributions only.
    4. Implement network access control lists to all specific destinations, with an Implicit deny as a rule.
13. You have an EC2 Security Group with several running EC2 instances. You change the Security Group rules to allow inbound traffic on a new port and protocol, and launch several new instances in the same Security Group. The new rules apply:
    1. **Immediately to all instances in the security group.**
    2. Immediately to the new instances only.
    3. Immediately to the new instances, but old instances must be stopped and restarted before the new rules apply.
    4. To all instances, but it may take several minutes for old instances to see the changes.