quiz

To save administration headaches, a consultant advises that you leave all security groups in web-facing subnets open on port 22 to 0.0.0.0/0 CIDR. That way, you can connect wherever you are in the world. Is this a good security design?

Yes

! NO

When peering VPCs, you may peer your VPC only with another VPC in your same AWS account.

True

! False

Which of the following are true for security groups?

! Security groups operate at the instance level and are associated with network interfaces.

Security groups process rules in number order when deciding whether to allow traffic.

Security groups operate at the subnet level.

Security groups support both "allow" and "deny" rules.

!Security groups support "allow" rules only.

!Security groups evaluate all rules before deciding whether to allow traffic.

You have five VPCs in a 'hub and spoke' configuration, with VPC 'A' in the center and individually peered with VPCs 'B', 'C', 'D', and 'E', which make up the spokes. There are no other VPC connections. Which of the following VPCs can VPC 'B' communicate with directly?

! VPC 'A'

VPCs 'C', 'D', and 'E'

VPCs 'A' and 'E'

VPCs 'A' and 'C'

When I create a new security group, all outbound traffic is allowed by default.

! True

False

Which of the following is true?

Both Security Groups and Network Access Control Lists are stateless.

Both security groups and Network Access Control Lists (NACLs) are stateful.

! Security groups are stateful and Network Access Control Lists (NACLs) are stateless.

Security groups are stateless and Network Access Control Lists (NACLs) are stateful.

Security groups act like a firewall at the instance level, whereas \_\_\_\_\_\_\_\_\_ are an additional layer of security that act at the subnet level. (Fill in the blank with the correct answer.)

!Network ACLs

Database Security Groups

Route Tables

VPC Security Groups

True or False: A subnet can span multiple Availability Zones.

True

! False

Which of the following offers the largest range of internal IP addresses?

/24

/28

! /16

/20

**From what services I can block incoming/outgoing IPs?**

Security Groups

ELB

DNS

VPC subnet

!NACL

**Which of the following statements describes network ACLs? (Choose 2 answers)**

Responses to allowed inbound traffic are allowed to flow outbound regardless of outbound rules, and vice versa (are stateless)

Using network ACLs, you can deny access from a specific IP range

Keep network ACL rules simple and use a security group to restrict application level access

NACLs are associated with a single Availability Zone (associated with Subnet)