Exam Session - Knowledge Check: Networking (SAA-C03) 1 of 2

cloudacademy.com/quiz/exam/3791952/results

#1

You are designing a VPC for a large insurance company. Because their data is highly sensitive, you plan to implement several security features including security groups, network access control lists (ACL), and server-side encryption. You first want to set up security groups for security at the instance level. Which statements regarding security group features are correct? (Choose 3 answers)

✓

You can specify allow rules but not deny rules.

✓

You can specify separate rules for inbound and outbound traffic.

✕

You can specify allow and deny rules.

✓

By default, new security groups include a rule allowing all outbound traffic.

Explanation

A *security group* acts as a virtual firewall for your instance to control inbound and outbound traffic. For each security group, you add *rules* that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic. You can specify allow rules, but not deny rules. You can specify separate rules for inbound and outbound traffic.

🔗

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

#2

You need to establish a site-to-site VPN connection from your on-premise network to the VPC. For this to work successfully, which of the following need to be configured? (Choose 2 answers)

✓

A public IP address on the customer gateway for the on-premise network

✗

A private IP address on the customer gateway for the on-premise network

✗

Both a private IP address on the customer gateway for the on-premise network and a Public/Elastic IP to a VPG

✓

A physical appliance or software application as your customer gateway

Explanation

You are taking information (the public IP) from the on-premises network and configuring it inside of the VPC . When you configure a VPN, you're configuring it from the VPC and from the on-premises network. To use Amazon VPC with a VPN connection, you or your network administrator must designate a physical appliance or software application as your customer gateway and configure it.

🔗http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html

Covered in this lecture

Amazon VPC IPSec Protocol Theory and Background

Course:Amazon VPC IPSec VPNs- Understanding, Building and Configuring

17m

#3

A(n) ______ connection creates a secure tunnel between your on-site networks and your AWS networks.

✓

VPN

✗

elastic

✗

VPC

✗

paired region

Explanation

You might also think about how you can connect your on-site networks with your networks within the cloud. This is also easily achievable and can be done using a VPN connection, which will create a secure tunnel between your on-premises environment and AWS.

🔗/course/connecting-networks-aws-transit-gateway-1579/connecting-networks-with-aws-transit-gateway/

#4

A customer has EC2 instances in two different VPCs and wants them to easily communicate with each other. VPC peering seems ideal without the need for a transit gateway, but there are some things you need to consider. Which two of the following do you need to ensure are correct for this to work? (Choose 2 answers)

✓

The VPCs are directly connected with a single peering connection.

✗

The VPCs' CIDR blocks need to be the same

✓

The VPCs' CIDR blocks cannot overlap.

✗

The VPCs both need to have EC2 instances with the same operating system

Explanation

To create a VPC peering connection with another VPC, you need to be aware of the following limitations and rules:

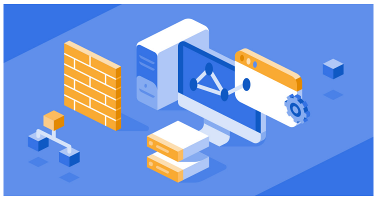
- You cannot create a VPC peering connection between VPCs that have matching or overlapping IPv4 or IPv6 CIDR blocks. Amazon always assigns your VPC a unique IPv6 CIDR block. If your IPv6 CIDR blocks are unique but your IPv4 blocks are not, you cannot create the peering connection.
- Transitive routing is not supported - that is you cannot route traffic through a intermediate (shared) VPC.

http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/vpc-peering-overview.html#vpc-peering-limitations

Covered in this lecture

Summary

Course:Introduction to VMware Cloud on AWS



10m

#5

Which of the following should be followed before connecting to Amazon Virtual Private Cloud (Amazon VPC) using AWS Direct Connect?

✗

Allocate a private IP address to your network in the 122.x.x.x range.

✗

Provide a public IP address for each Border Gateway Protocol (BGP) session.

✓

Create a virtual private gateway and attach it to your Virtual Private Cloud (VPC).

✗

Provide the public routes that you will advertise over Border Gateway Protocol (BGP).

Explanation

To connect to Amazon Virtual Private Cloud (Amazon VPC) by using AWS Direct Connect, you must first do the following:

- Provide a private Autonomous System Number (ASN) to identify your network on the Internet. Amazon then allocates a private IP address in the 169.x.x.x range to you.
- Create a virtual private gateway and attach it to your VPC.

http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

#6

To meet the needs of one of your on-premises applications, you decide to increase data transfer speeds from your site to AWS by implementing AWS Direct Connect. What are two components that you will need to properly implement AWS Direct Connect? (Choose 2 answers)

✓

a connection

✕

a virtual link

✕

a link parameters

✓

a virtual interface

Explanation

There are two key components that you will need to deploy AWS Direct Connect: a connection and a virtual interface. A connection in an AWS Direct Connect location establishes a network connection from your premises to an AWS region. Virtual interfaces enable access to AWS services. A public virtual interface enables access to public-facing services, such as Amazon S3, while a private virtual interface enables access to your VPC.

🔗http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

#7

Which statement about AWS Direct Connect is correct?

✕

AWS Direct Connect can be configured in minutes and are a good solution if you have an immediate need.

✕

AWS Direct Connect is a good solution if you have low to modest bandwidth requirements.

✓

AWS Direct Connect does not involve the Internet and uses dedicated, private network connections between your intranet and Amazon VPC.

✕

AWS Direct Connect is a good solution if you can tolerate the inherent variability in Internet-based connectivity.

Explanation

AWS Direct Connect is different from IPSec VPN Connection. A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet. VPN Connections can be configured in minutes and are a good solution if you have an immediate need, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity. AWS Direct Connect does not involve the Internet; instead, it uses dedicated, private network connections between your intranet and Amazon VPC.

🔗http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

#8

You are in charge of the VPC for your company. You are developing an overall architectural document for the VPC including specifics about the VPC, Internet Gateway, Network Access Control Lists, Security Groups, and EC2 instances. You want to provide details on public IP addresses and elastic IP addresses and when you might use one over the other. What can you detail about the benefits of Elastic IP addresses? (Choose 3 Answers)

✓

The Elastic IP address is not tied to the life of an EC2 instance.

✓

The Elastic IP address can be moved to a new instance in the case of instance failure.

✕

The Elastic IP address can be stretched across two EC2 instances at once.

✓

The loose coupling provided by the Elastic IP addresses is helpful in failover situations.

Explanation

An Elastic IP address is a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is associated with your AWS account. With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account.

An Elastic IP address is a public IPv4 address, which is reachable from the Internet. If your instance does not have a public IPv4 address, you can associate an Elastic IP address with your instance to enable communication with the Internet; for example, to connect to your instance from your local computer.

🔗http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html

#9

You want to allow an on-premises network to connect to multiple separate VPCs within your AWS network through a central network hub. What service would you need to provide the centralized network hub between multiple VPCs and your on-premises network?

✕

VPC peering

✕

AWS VPN

✕

AWS Direct Connect

✓

AWS Transit Gateway

Explanation

The central connection point or hub between the multiple VPCs and the hybrid connection to an on-premises network will be AWS Transit Gateway. The network suggested in this scenario would certainly include VPC peering connections and either VPNs or Direct Connect, but the component that connects them all is AWS Transit Gateway.

🔗https://docs.aws.amazon.com/vpc/latest/tgw/what-is-transit-gateway.html

#10

When you add a new VPC into an architecture that uses an AWS Transit Gateway, what must you do to enable it to communicate with your other VPCs?

✕

Simply update your subnet's route table with the new VPC.

✓

Connect the new VPC to the Transit Gateway and update your subnet’s route table.

✕

Create Transit Gateway peering connections between regions and assign an AWS account to each one.

✕

Create a Bastion Host in a private subnet, connect it to your backend instances, and then connect the new VPC to it.

Explanation

When you add a new VPC into an architecture that uses an AWS Transit Gateway, you only need to connect that VPC to the Transit Gateway and then update your subnet's route table for it to be able to communicate with your other VPCs.

/course/networking-vpc-sap-aws-2713/network-and-vpc-architectures-for-sap-on-aws/

#11

Your development team did not create a new security group when it deployed three EC2 instances, so the instances are associated with the default security group. The default security group is unchanged, so what rules does the default security group enforce? (Choose 3 answers)

✓

No inbound traffic is allowed from resources outside the security group.

✗

No outbound traffic will be allowed from the EC2 instances.

✓

The EC2 instances will be able to communicate with each other.

✓

All outbound traffic from the EC2 instances will be allowed.

Explanation

Your VPC automatically comes with a default security group. Each EC2 instance that you launch in your VPC is automatically associated with the default security group if you don't specify a different security group when you launch the instance. The default security group disallows all inbound traffic and allows all outbound traffic. The default security group does allow communication between resources associated with the same default security group. However, the rules for a default security group can be changed.

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

#12

How does AWS Direct Connect differ from a VPN Connection?

✗

AWS Direct Connect can be configured in minutes.

✓

AWS Direct Connect uses dedicated, private network connections between your intranet and Amazon VPC.

✗

AWS Direct Connect can tolerate the inherent variability in Internet-based connectivity.

✗

AWS Direct Connect utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet.

Explanation

A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet. VPN Connections can be configured in minutes and are a good solution if you have an immediate need, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity.

AWS Direct Connect does not involve the Internet; instead, it uses dedicated, private network connections between your intranet and Amazon VPC.

http://aws.amazon.com/directconnect/faqs/

#13

You want to connect a single VPC network with a company's on-premises network. You will encrypt the network traffic that travels over the public internet between the two destinations. Which AWS network connection method would meet your needs?

✓

A Virtual Private Network (VPN)

✗

AWS Direct Connect

✗

VPC Peering connections

✕

AWS Transit Gateway

Explanation

A VPN is the best choice because it can provide a hybrid connection and encrypt network traffic over the public internet. VPC peering connections can connect two VPCs. AWS Transit Gateway can create a hub between multiple VPCs and an on-premise network, but this case only requires connecting two networks so a central hub is not necessary. Direct Connect would provide a private network connection, which is also not necessary.

🔗/course/saa-networking/vpc-vpn-direct-connect/

#14

What does a local route within a route table enable?

✓

It enables communication between VPC subnets.

✕

It enables communication only within each VPC subnet, not between subnets.

✕

It enables communication between a VPC and external public IP addresses.

✕

It enables an administrator to SSH directly into any VPC resource.

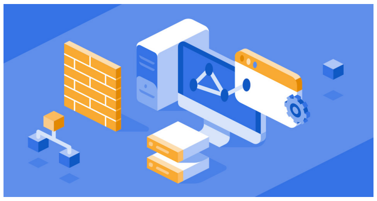
Explanation

Now, by default, when your subnet's created, it will have a default route in it, and this is a local route. Let's take a look. Now, your route table will contain a destination field and also a target field. Now, the destination field is the destination address that you're trying to get to. The target essentially specifies the route to that destination. Now, within every route table that's created, there will be this local route here. Now, what this enables your subnets to do is simply talk to each other. So any subnet within your VPC is able to communicate with each other without you having to configure any routes. It's there by default. Every route table has this local route. It can't be deleted, and it simply allows all subnets within your VPC to communicate with each other.

🔗/course/amazon-vpc-networking/vpc-subnets/

Covered in this lecture

Routing: VPC Peering
Course:AWS Virtual Private Cloud: Subnets and Routing



5m

#15

You want to implement SSH forwarding to access EC2 instances. What descriptions of SSH agent forwarding are correct? (Choose 2 answers)

✓

You use it to access instances through a bastion host.

✗

It allows you to access private keys stored on the bastion host.

✓

It stores EC2 private keys on the local client.

✗

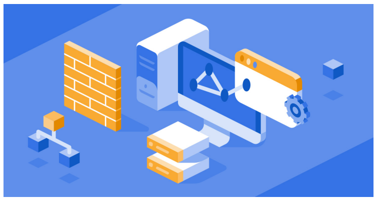
You use it to access instances through a virtual private gateway.

Explanation

SSH agent forwarding is a process that allows you to access private instances through a bastion host without storing the private key within the bastion host, which could be a security risk. Instead, through SSH agent forwarding you store the private keys on your local machine.

/course/amazon-vpc-networking/vpc-bastion-hosts/

Covered in this lecture
Bastion Hosts
Course:Working with AWS Networking and Amazon VPC



8m

#16

Which of the following services can improve instance network performance to speeds of up to 100 Gbps and is available at no cost?

✗

AWS Global Accelerator

✗

Amazon CloudFront

✓

Elastic Network Adapter (ENA)

✗

Elastic Network Interface (ENI)

Explanation

If you are looking to enable enhanced networking features to reach speeds of up to 100 Gbps for your Linux compute instances, then you can do so using an ENA. However, ENAs are only supported on a limited number of instances as shown below, and by instances running kernel versions 2.6.32 and 3.2 and above.

In addition to 100 Gbps speeds, enhanced networking offers higher bandwidth with increased packet per second (PPS) performance, and a big bonus of enhanced networking is that it is offered at no extra cost. In fact, when launching an instance using Amazon Linux 2 or with the latest version of the Amazon Linux AMI, then the instance will have enhanced networking enabled by default, providing its provisioned with one of the supported instance types mentioned earlier.

🔗/course/saa-networking/ec2-enhanced-networking-with-the-enhanced-network-adaptor-ena/

#17

AWS provides two features that you can use to increase security in your VPC: security groups and network ACLs (NACLs). Which of the following statements are true in relation to security groups and NACLs in your VPC? (Choose 2 answers)

✓

Security groups control inbound and outbound traffic for your instances

✗

Security groups control inbound and outbound traffic for your instances and for your subnets.

✗

Network ACLs control inbound and outbound traffic for your subnets and outbound traffic for your instances

✓

NACLs control inbound and outbound traffic for your subnets.

Explanation

AWS provides two features that you can use to increase security in your VPC: *security groups* and *network ACLs*. Security groups control inbound and outbound traffic for your instances, and network ACLs control inbound and outbound traffic for your subnets. In most cases, security groups can meet your needs; however, you can also use network ACLs if you want an additional layer of security for your VPC.

🔗http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

#18

A client wants a connection between their VPC and other AWS services including Amazon S3 and DynamoDB without availability concerns or bandwidth constraints.They do not want a VPN connection because of bandwidth limitations and do not want to incur the expense of Direct Connect. What AWS solution will meet the client's requirements?

✕

NAT Gateways

✕

Network Load Balancers

✕

Transit Gateways

✓

VPC Endpoints

Explanation

A VPC endpoint enables you to create a private connection between your VPC and another AWS service without requiring access over the Internet, through a NAT device, a VPN connection, or AWS Direct Connect. Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and AWS services without imposing availability risks or bandwidth constraints on your network traffic.

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html

#19

You can allow the instances in your private subnets in an Amazon VPC to have outbound access to the Internet by placing ______ inside of a public subnet and then configuring a route from your private subnet to it.

✗

an AWS Transit Hub

✗

VPC peering

✓

a NAT gateway

✗

AWS Direct Connect

Explanation

You can still allow the instances in your private subnets to have outbound access to the Internet by placing a NAT gateway inside of a public subnet and then configuring a route from your private subnet to the NAT gateway.

/course/networking-vpc-sap-aws-2713/network-and-vpc-architectures-for-sap-on-aws/

#20

Which of the following EC2 instances cannot initiate outbound traffic to the public internet?

✗

An instance with an assigned public IP address in a public subnet.

✗

An instance with an assigned Elastic IP address in a public subnet.

✗

An instance with an assigned private IP address **only** in a private subnet with a route to a NAT Gateway.

✓

An instance with an assigned private IP address **only** in a private subnet with no route to a NAT Gateway.

Explanation

The only EC2 instance from the four choices above that cannot initiate outbound traffic to the public internet is an Amazon EC2 instance with an assigned private IP address in a private subnet.

An instance with an assigned public IP or EIP address in a public subnet is about as ready as you can be to send and receive traffic from the public internet.

An instance with an assigned private IP address only, in a private subnet with a route to a NAT Gateway, can initiate outbound traffic to the public internet.

🔗/course/design-multi-tier-architectures/saa-d1-connectivity/
Covered in this lecture
Connectivity Within The VPC
Course:Designing Multi-Tier Architectures

3m
🔖
#21

Which choice correctly describes the differences between security groups and Network Access Control Lists (NACLs)? (Choose 2 answers)

✓

Security Groups operate at the instance level, are stateful, and support allow rules only.

✗

Security Groups operate at the subnet level, and they support allow rules only.

✗

NACLs operate at the subnet level and support deny rules only.

✓

NACLs operate at the subnet level, are stateless, and support allow and deny rules.

Explanation

You can secure your VPC instances using only security groups; however, you can add NACLs as a second layer of defense. Security groups are stateful and — Act as a firewall for associated Amazon EC2 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 are stateful and support allow rules only while Network Access Control Lists are stateless and support allow and deny rules.

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html

#22

Which statement regarding VPC peering is correct?

✗

VPC-A can communicate with VPC-B through their peering connections with VPC-C.

✗

VPCs with overlapping CIDR block ranges can establish a peering connection.

✓

VPC-A and VPC-B have identical CIDR block ranges. VPC-C can establish peering connections with both VPC-A and VPC-B.

✗

VPCs with identical CIDR block ranges can establish a peering connection.

Explanation

The connectivity between the VPCs is implemented through the existing AWS network infrastructure, and so it is highly available with no bandwidth bottleneck. As peered connections operate as if they were part of the same network, there are restrictions when it comes to your CIDR block ranges that can be used.

Of the choices below, the only possible option is connecting two separate VPCs with identical CIDR blocks to the same separate VPC. The other choices, which involve duplicate or overlapping CIDR ranges, or daisy-chain connections between VPC peer connections, are not possible.

https://docs.aws.amazon.com/vpc/latest/peering/peering-configurations-partial-access.html#one-to-two-vpcs-simple-hub

#23

With a(n) ______ , you can mask the failure of an instance by rapidly remapping the address to another instance in your VPC.

✓

Elastic IP address

✗

Private IP address

✗

Public IP address

✗

Reserved IP address

Explanation

With an Elastic IP address, you can mask the failure of an instance by rapidly remapping the address to another instance in your VPC. You can associate an Elastic IP address with any instance or network interface for your VPC.

🔗http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html

#24

What features of VPC security groups are correct? (Choose 2 answers)

✓

Instances associated with the same security group can not talk to each other unless rules are added specifically allowing communication.

✗

You can specify only deny rules, not allow rules.

✗

Security Groups are stateless.

✓

You can change the security group that an instance is associated with after launch and the changes will take effect immediately.

Explanation

Instances associated with a security group can't talk to each other unless you add rules allowing it (exception: the default security group has these rules by default). By default, a security group includes an outbound rule that allows all outbound traffic. You can remove the rule and add outbound rules that allow specific outbound traffic only. If your security group has no outbound rules, no outbound traffic is allowed.

🔗
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html
#25

All statements regarding VPC peering connections below are correct except:

✕
You can configure a peering connection between VPCs in separate regions.

✓
Peering connections are established using virtual private networks (VPN).

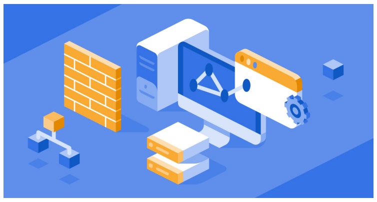
✕
Peering connections establish a one-to-one connection only.

✕
Peering connections are not possible between VPCs with an IP address overlap.

Explanation

VPC peering connects two separate VPCs, either in the same region or different regions. That connection is a one-to-one connection only, and cannot be established between VPCs with an IP address overlap. The connection is made over AWS infrastructure, not through a Direct Connect co-location or a virtual private network (VPN). This offers high availability, and avoids a bandwidth bottleneck.

🔗/course/amazon-vpc-networking/vpc-vpc-peering/
Covered in this lecture
VPC Peering
Course:Working with AWS Networking and Amazon VPC



7m