**Security**

1. Your server logs are full of what appear to be application-layer attacks, so you deploy AWS Web Application Firewall. Which of the following conditions may you set when configuring AWS WAF? [Select 3]
   1. IP match constraints.
   2. String match constraints.
   3. Size constraints.
   4. SQL rejection match conditions.
   5. Termination Conditions.
   6. URL match conditions.
2. With SAML-enabled single sign-on, \_\_\_\_\_\_\_\_. [Select 2]
   1. After the client browser posts the SAML assertion, AWS sends the siginurl as a redirect and the client browser is redirected to the console.
   2. The portal first verifies the user’s identity in your organization then generates a SAML authentication response.
   3. The client browser is immediately directed to the AWS console.
   4. The portal acknowledges a SAML authentication response, then verifies the user’s identity in your organization.
3. AWS provides a number of security-related managed services. From the options below, select which AWS service is related to protecting your infrastructure from which security issue. [Select 4]
   1. AWS WAF blocks IP addresses based on the rules.
   2. Amazon macie uses ML to protect sensitive data.
   3. AWS WAF protects from CSS attacks.
   4. AWS Shield protects from Distributed Denial-of-Service attacks.
   5. AWS Shield protects from SQL injection attacks.
4. Security Groups are stateful and updates are applied immediately.
5. You are a solutions architect working for a large anti-virus company and your job is to secure your company’s production AWS environment. A new policy dictates that a particular public-facing subnet needs to allow RDP on port 3389 at the network ACL layer. You create an inbound rule allowing traffic to port 3389 on the ACL level. However, users complain that they still cannot connect. Which of the following answers may represent the root cause of the connectivity issues? [Select 2]
   1. NACL are stateful
   2. Updates to NACL can take time to propagate.
   3. NACL are stateless.
   4. You need to create an outbound rule allowing RDP response traffic to go back out again.
6. A solutions architect is designing a two-tier web application The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet Security is a high priority for the company How should security groups be configured in this situation? (Select TWO )
   1. Configure the security group for the web tier to allow inbound traffic on port 443 from 0 0 0 0/0
   2. Configure the security group for the web tier to allow outbound traffic on port 443 from 0 0 0 0/0
   3. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier
   4. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier
   5. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier
7. A company’s security team requires that all data stored in the cloud be encrypted at rest at all times using encryption keys stored on-premises.Which encryption options meettheserequirements? (Select TWO.)
   1. Use Server-Side Encryption with Amazon S3Managed Keys (SSE-S3).
   2. Use Server-Side Encryption with AWS KMS Managed Keys (SSE-KMS).
   3. Use Server-Side Encryption with Customer Provided Keys (SSE-C).
   4. Use client-side encryption to provide at-rest encryption.
   5. Use an AWS Lambda function triggered by Amazon S3 events to encrypt the data using the customer’s keys.
8. An organization has created an application which is hosted on the AWS EC2 instance. The application stores images to S3 when the end user uploads to it. The organization does not want to store the AWS secure credentials required to access the S3 inside the instance. Which of the below mentioned options is a possible solution to avoid any security threat?

A. Use the IAM based single sign between the AWS resources and the organization application.

B. Use the IAM role and assign it to the instance.

C. Since the application is hosted on EC2, it does not need credentials to access S3.

D. Use the X.509 certificates instead of the access and the secret access key

1. A user has created an application which will be hosted on EC2. The application makes calls to DynamoDB to fetch certain data. The application is using the DynamoDB SDK to connect with from the EC2 instance. Which of the below mentioned statements is true with respect to the best practice for security in this scenario?

A. The user should create an IAM user with DynamoDB access and use its credentials within the application to connect with DynamoDB

B. The user should attach an IAM role with DynamoDB access to the EC2 instance

C. The user should create an IAM role, which has EC2 access so that it will allow deploying the application

D. The user should create an IAM user with DynamoDB and EC2 acces

E. Attach the user with the application so that it does not use the root account credentials

1. Your manager has asked you to set up a public subnet with instances that can send and receive internet traffic, and a private subnet that can't receive traffic directly from the internet, but can initiate traffic to the internet (and receive responses) through a NAT instance in the public subnet. Hence, the following 3 rules need to be allowed:

Inbound SSH traffic.

Web sewers in the public subnet to read and write to MS SQL servers in the private subnet Inbound RDP traffic from the Microsoft Terminal Services gateway in the public private subnet What are the respective ports that need to be opened for this?

A. Ports 22,1433,3389

B. Ports 21,1433,3389

C. Ports 25,1433,3389

D. Ports 22,1343,3999

1. You log in to IAM on your AWS console and notice the following message. "Delete your root access keys." Why do you think IAM is requesting this?

A. Because the root access keys will expire as soon as you log out.

B. Because the root access keys expire after 1 week.

C. Because the root access keys are the same for all users.

D. Because they provide unrestricted access to your AWS resource

1. Your Security Manager has hired a security contractor to audit your firewall implementation. When the consultant asks for the login details for the firewall appliance, which of the following might you do? [Select 2]
   1. Create a IAM Role with a policy that can read SG and NACL settings.
   2. Create a IAM user with a policy than can read SG and NACL settings.
   3. Create a IAM user with a policy than can read SG and Route settings.
   4. Create a IAM Role with a policy that can read SG and Route settings.
   5. Explain that AWS implements network security differently and that there is no such thing as a firewall appliance.
2. Which of the following are true for Security Groups? [Select 3]
   1. Operate at instance level
   2. Support both “allow” and “deny” rules.
   3. Process rules in number order when deciding whether to allow traffic.
   4. Operate at the subnet level.
   5. Evaluate all rules before deciding whether to allow traffic.
   6. Support “allow” rules only.
3. You are signed in as root user on your account but there is an Amazon S3 bucket under your account that you cannot access. What is a possible reason for this?

A. An IAM user assigned a bucket policy to an Amazon S3 bucket and didn't specify the root user as a principal

B. The S3 bucket is full.

C. The S3 bucket has reached the maximum number of objects allowed.

D. You are in the wrong availability zone

|  |  |  |
| --- | --- | --- |
| No | Answer | Explanation |
| 1 | A,B,C |  |
| 2 | A,B |  |
| 3 | A, B, C, D | AWS provides various services to cope with many security related issues and because of this, there are a number of options which are correct. AWS Shield has two options listed above, but only one is correct. AWS Shield operates on layer 3 and 4 of the ISO network model and its primary purpose is to protect against DDoS attacks. It does not have any affect against SQL Injection attacks which are dealt with by AWS WAF. WAF also protects against Cross Site Scripting and can block traffic from IP addresses based on rules and therefore these options are also correct. Finally, Amazon Macie tackles a different problem related to Data Loss Prevention and protects sensitive data and so this answer is also correct. |
| 5 | C, D | Network Access Control Lists are stateless; updates are applied near instantaneously. |
| 6 | A, C |  |
| 7 | C, D | Server-Side Encryption with Customer-Provided Keys (SSE-C)enables Amazon S3 to encrypt objects serverside using an encryption key provided in the PUT request. The same key must be provided in GET requests for Amazon S3 to decrypt the object. Customers also have the option to encrypt data clientside before uploading it toAmazonS3 and decrypting it after downloading it. AWS SDKs provide an S3encryption client that streamlines the process. |
| 8 | B | The AWS IAM role uses temporary security credentials to access AWS services. Once the role is assigned to an instance, it will not need any security credentials to be stored on the instance. |
| 9 | B | With AWS IAM a user is creating an application which runs on an EC2 instance and makes requests to  AWS, such as DynamoDB or S3 calls. Here it is recommended that the user should not create an IAM user and pass the user's credentials to the application or embed those credentials inside the application. Instead, the user should use roles for EC2 and give that role access to DynamoDB /S3. When the roles are attached to EC2, it will give temporary security credentials to the application hosted on that EC2, to connect with DynamoDB / S3 |
| 10 | A | A network access control list (ACL) is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.  The following ports are recommended by AWS for a single subnet with instances that can receive and send Internet traffic and a private subnet that can't receive traffic directly from the Internet. However, it can initiate traffic to the Internet (and receive responses) through a NAT instance in the public subnet. Inbound SSH traffic. Port 22  Web sewers in the public subnet to read and write to MS SQL sewers in the private subnet. Port 1433 Inbound RDP traffic from the Microsoft Terminal Sewices gateway in the public private subnet. Port 3389 |
| 11 | D | In AWS an access key is required in order to sign requests that you make using the command-line interface (CLI), using the AWS SDKs, or using direct API calls. Anyone who has the access key for your root account has unrestricted access to all the resources in your account, including billing information.  One of the best ways to protect your account is to not have an access key for your root account. We recommend that unless you must have a root access key (this is very rare), that you do not generate one. Instead, AWS best practice is to create one or more AWS Identity and Access Management (IAM) users, give them the necessary permissions, and use IAM users for everyday interaction with AWS. |
| 12 | B, E | AWS has removed the Firewall appliance from the hub of the network and implemented the firewall functionality as stateful Security Groups, and stateless subnet NACLs. This is not a new concept in networking, but rarely implemented at this scale. In this case an IAM role by itself will not be enough to gain access to the AWS infrastructure - an IAM user will also be required. |
| 13 | A, E, F | Security Groups operate at the instance level, they support "allow" rules only, and they evaluate all rules before deciding whether to allow traffic. |
| 14 | A | With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.  In some cases, you might have an IAM user with full access to IAM and Amazon S3. If the IAM user assigns a bucket policy to an Amazon S3 bucket and doesn't specify the root user as a principal, the root user is denied access to that bucket. However, as the root user, you can still access the bucket by modifying the bucket policy to allow root user access. |