DUMPSARENA

FCSSPublic Cloud Security 7.6 Architect

Fortinet FCSS_CDS_AR-7.6

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Public Cloud Security Architecture	5
Topic 2, Public Cloud Security Deployment	14
Topic 3, Public Cloud Security Operations	4
Total	23

QUESTION NO: 1

An AWS application environment uses Auto Scaling groups. New application instances are tagged with *Role=Web*, and the security team wants FortiGate policies to allow administrative access only to the private IP addresses of instances carrying that tag.

The policy must automatically adapt when instances are launched, terminated, or assigned new private IP addresses.

Which FortiGate capability best meets this requirement?

A. Configure an AWS Fabric Connector and use a tag-based dynamic address object.

B. Create a static FortiGate address group containing the current instance IP addresses.

C. Enable VPC Flow Logs and use the log records as the firewall policy source.

D. Create an AWS security group that contains the current FortiGate private IP addresses.

ANSWER: A

Explanation:

Configure an AWS Fabric Connector and use a dynamic address object that resolves EC2 instances according to the required AWS tag. FortiGate can update the object membership as the cloud environment changes, allowing a firewall policy to reference the dynamic group rather than manually maintained IP addresses.

A static address group requires ongoing manual updates and is unsuitable for an Auto Scaling environment. A VPC Flow Log records traffic metadata but cannot populate a firewall address object. An AWS security group can control traffic at the instance interface, but it does not create a FortiGate policy object that dynamically tracks tagged cloud resources.

QUESTION NO: 2

An organization uses AWS CloudFormation to deploy a FortiGate-VM Auto Scaling environment. An administrator made an emergency change directly to a security group in the AWS console. The organization wants to identify configuration differences between the running environment and the declared CloudFormation template before the next update.

What should the administrator use?

A. A CloudFormation change set

B. CloudFormation stack drift detection

C. CloudFormation stack events

D. An AWS Config resource timeline

ANSWER: B

Explanation:

The administrator should run CloudFormation drift detection on the stack. Drift detection compares the actual properties of supported provisioned resources with the properties expected by the stack template and identifies resources that have drifted.

A change set previews the effect of a proposed stack update; it does not detect manual changes already made outside CloudFormation. Stack events show deployment activity, and AWS Config records configuration history but does not perform the template-to-resource comparison provided by CloudFormation drift detection.