PassQueen
a.k.a dumpsqueen.com

Check Point Certified Cloud Specialist (CCCS)

Checkpoint 156-560

Version Demo

Total Demo Questions: 11

Total Premium Questions: 115

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, CloudGuard Network Security	77
Topic 2, CloudGuard Cloud Native Security	25
Topic 3, CloudGuard Workload Protection	2
Topic 4, Mix Questions	11
Total	115

QUESTION NO: 1

Which statements describe sound use of IAM for CloudGuard integrations with a public-cloud account? Select all that apply.

A. Use a dedicated identity for the integration

B. Grant only permissions required for enabled functions

C. Review role permissions and credentials periodically

D. Use unrestricted administrator permissions by default

E. Embed long-lived access keys in deployment templates

ANSWER: A B C

Explanation:

CloudGuard integrations should use a dedicated cloud identity, such as an IAM role or service account, with only the permissions needed for discovery, monitoring, and any explicitly enabled automation or remediation functions. Credentials and role assignments should be reviewed regularly, and audit logging should be enabled to provide traceability for cloud API activity.

Using broad administrative permissions permanently or embedding long-lived credentials in templates weakens the security posture and conflicts with least-privilege practices. AWS describes these practices in its IAM security best practices.

QUESTION NO: 2

Adaptive Security Policies allow the deployment of new cloud based resources without

A. Changing the cloud environment

B. Paying for new resources

C. Installing New Policies

D. Installing New Applications

ANSWER: C

Explanation:

Installing New Policies is correct because Check Point CloudGuard Adaptive Security Policies are designed to keep security controls aligned with dynamic cloud environments automatically. In cloud platforms, workloads, instances, and services can be created, removed, or scaled frequently. Adaptive policies use cloud context, such as resource metadata, tags, and logical grouping, to identify which workloads should receive a given security policy. As a result, a newly deployed resource that matches the policy's defined criteria can be protected automatically under the appropriate existing policy rather than requiring an administrator to manually create and install a separate policy for that resource.

This approach supports consistent enforcement while preserving the agility expected from cloud operations. Security administrators define policy intent once and allow CloudGuard to adapt enforcement as the cloud inventory changes. The policy therefore follows the relevant workload characteristics rather than relying only on static network addresses or manually maintained object membership. This is particularly useful for elastic environments in which IP addresses and instance populations change routinely. Check Point describes CloudGuard Network Security's cloud-native automation and policy-based protection capabilities in its CloudGuard Network Security overview. Additional CloudGuard cloud-security architecture and automation information is available in the CloudGuard overview.

QUESTION NO: 3

Which actions are required to use a CloudGuard Network Security Gateway as an Azure network virtual appliance for routed traffic inspection? Select all that apply.

A. Enable IP forwarding on the gateway NIC

B. Create routes using Virtual appliance as the next hop

C. Assign an Azure public IP to every spoke workload

D. Specify the gateway private IP as the virtual-appliance next hop

E. Disable all network security groups in the spoke

ANSWER: A B D

Explanation:

The gateway NIC must have **IP forwarding enabled**, because Azure otherwise rejects traffic that has a source or destination IP address different from the NIC's own address. The applicable workload subnets also need **user-defined routes with Virtual appliance as the next hop**, pointing to the gateway's private IP address. Together, these settings enable Azure to send matching traffic to the CloudGuard gateway and allow the gateway to forward it after inspection.

Network Security Groups can provide additional filtering but do not replace routing through the appliance. Azure documentation describes both IP forwarding on network interfaces and user-defined routes.

QUESTION NO: 4

In AWS, which CloudFormation stack state indicates that stack creation failed and CloudFormation successfully removed the resources it created during the failed operation?

A. CREATE_COMPLETE

B. ROLLBACK_COMPLETE

C. UPDATE_COMPLETE

D. DELETE_FAILED

ANSWER: B

Explanation:

ROLLBACK_COMPLETE indicates that stack creation failed and CloudFormation completed its rollback operation. During rollback, CloudFormation deletes resources that were created as part of the failed stack operation, when possible. The stack events identify the resource and error that caused the failure, such as insufficient IAM permissions, unavailable capacity, invalid parameters, or an unaccepted Marketplace subscription.

Administrators should inspect the Events tab or equivalent API output before redeploying. See the AWS CloudFormation stack status documentation.

QUESTION NO: 5

What is Reliability according to the Five Pillars?

A. The ability to use cloud resources efficiently for meeting system requirements, and maintaining that efficiency as demand changes and technologies evolve

B. The ability of a workload to function correctly and consistently when it is expected to.

C. The ability to support development and run workload effectively

D. In terms of the cloud, security is about architecting every workload to prevent.

ANSWER: B

Explanation:

The ability of a workload to function correctly and consistently when it is expected to is the Reliability pillar definition used by the AWS Well-Architected Framework. Reliability focuses on ensuring that a workload can recover from disruptions, dynamically obtain computing resources as demand changes, and mitigate failures or configuration issues. In practical cloud architecture, this means designing systems with resilient components, tested recovery procedures, monitoring, and automation so that the workload continues to deliver its intended business function under normal conditions and following faults. Reliability is not merely whether a service is available at one instant; it is the sustained capacity to meet expected behavior and restore service predictably when an incident occurs. This pillar is especially relevant when implementing cloud network-security architectures, because the supporting security controls and connectivity components must remain operational and recoverable as part of the overall workload. AWS defines Reliability and its design principles in the AWS Well-Architected Reliability Pillar. The full set of Well-Architected pillars, including Reliability, is also described in the AWS Well-Architected Framework documentation.

QUESTION NO: 6

What is the key component in securing and managing any environment?

A. Security Management Server

B. Security Gateway

C. Security Policy

D. Security Access

ANSWER: A

Explanation:

The **Security Management Server** is the key component because it provides the centralized management plane for a Check Point deployment. Administrators use it to define, administer, install, and maintain the security policy that governs protected networks and cloud resources. It also centrally manages gateway objects and configurations, administrator access and roles, logs, monitoring data, and event information. This centralization is essential in any environment because it gives security teams a consistent policy lifecycle and a single authoritative place to manage enforcement across one or many Security Gateways. In Check Point terminology, the management server hosts the management services and databases used by SmartConsole and related management tools, while gateways receive and enforce the policy that management creates and installs. Central management therefore enables a scalable, auditable operational model: changes can be reviewed and applied consistently, and operational visibility can be retained in one place. Check Point describes the Security Management Server as the component used to manage security policies and Security Gateways in its Security Management Administration Guide. The relationship between centralized management, policy installation, and gateway enforcement is also covered in Check Point's Quantum Security Gateway overview.

QUESTION NO: 7

Which characteristics are benefits of deploying CloudGuard Network Security Gateways behind a cloud load balancer in a scalable architecture?

A. It can distribute traffic among healthy gateway instances.

B. It can use health checks when selecting targets.

C. It can support elastic gateway capacity with an autoscaling design.

D. It replaces the Check Point Security Policy.

E. It independently performs Threat Prevention inspection.

ANSWER: A B C

Explanation:

A load balancer can distribute eligible traffic among multiple healthy gateway instances and use health checks to avoid sending new traffic to unhealthy instances. Combined with an autoscaling mechanism and CME-based lifecycle automation, this supports elastic gateway capacity. A load balancer does not itself author Check Point Security Policy or replace gateway Threat Prevention inspection.

For cloud load-balancing concepts, see AWS Elastic Load Balancing documentation. For CloudGuard lifecycle automation, see the CME overview.

QUESTION NO: 8

Once the Deployment finishes, Cloud Security Posture Management applies default network security posture that does what?

A. Minimizes the risk of external threats by blocking access to high risk sites and external users

B. Minimizes the risk of external threats by blocking accessed to the internet

C. Minimizes the risk of external threats by blocking access to all internal resources

D. Minimizes the risks of external threats by blocking access to services and ports

ANSWER: D

Explanation:

Cloud Security Posture Management applies a default network security posture that minimizes exposure to external threats by blocking access to services and ports. This baseline approach addresses a core cloud-security concern: publicly reachable network services can create an attack surface when inbound access is broader than the workload requires. By identifying and restricting unnecessarily exposed ports and services, the posture helps enforce least-privilege network access from the start of the deployment. The control is intended to establish a secure default state while still allowing administrators to review business requirements and explicitly permit the connectivity needed for approved applications. In practice, this means the organization begins with reduced external exposure rather than relying on every individual cloud resource to have been manually configured securely. Check Point describes CloudGuard Posture Management as helping organizations continuously assess cloud environments and remediate misconfigurations that increase risk, including network-exposure issues. This default posture aligns with Check Point's cloud-native security model of reducing attack surface through automated governance and configuration controls. See the Check Point CloudGuard Posture Management overview and the CloudGuard platform overview.

QUESTION NO: 9

Which two statements correctly describe the use of Data Center Objects in a CloudGuard adaptive security policy?

A. They can represent cloud resources selected by tags.

B. They can dynamically represent discovered hosts and subnets.

C. They require a static IP address for every member.

D. They automatically create cloud-provider route tables.

E. They can be used as source or destination objects in policy rules.

ANSWER: A B E

Explanation:

Data Center Objects obtain cloud inventory and context through a configured Data Center Server integration. They can represent dynamically discovered cloud assets, including hosts, subnets, and tag-based groups. When cloud membership changes, the dynamic object information can be updated for gateways without administrators manually changing every affected IP address.

Data Center Objects are not limited to static addresses, and they do not replace cloud-provider route tables, which are used for traffic steering. See the Check Point Data Center Objects documentation.

QUESTION NO: 10

Which practices support the AWS Well-Architected Security Pillar for a cloud workload protected by CloudGuard?

A. Apply least-privilege IAM permissions.

B. Collect and monitor security-relevant logs.

C. Encrypt sensitive data appropriately.

D. Share a long-lived administrator access key among operators.

E. Use automation to apply security controls consistently.

ANSWER: A B C E

Explanation:

The Security Pillar emphasizes strong identity foundations, traceability, protection of data, and security automation. Applying least privilege to IAM identities, collecting and monitoring logs, and encrypting sensitive data are aligned with these principles. Sharing long-lived administrator credentials is contrary to secure identity management.

See the AWS Well-Architected Security Pillar and the AWS IAM best practices.

QUESTION NO: 11

A CloudGuard Network gateway is deployed in a hub VPC to inspect traffic from a spoke VPC to on-premises networks. Besides an appropriate Security Policy, what is required for the spoke traffic to reach the gateway for inspection?

A. A spoke route that directs the destination prefix to the gateway inspection path

B. A new policy installation on each spoke workload

C. A public IP address on every workload instance

D. A load balancer target group for the on-premises network

ANSWER: A

Explanation:

The spoke route table needs a route for the on-premises destination prefix whose target sends traffic to the inspection path through the **CloudGuard gateway**. Security policy cannot inspect traffic that is never routed to the Security Gateway. In cloud designs, route tables and the gateway policy work together: routing steers the packet to the enforcement point, and the gateway then evaluates it against the installed policy.

The exact AWS route target depends on the selected topology and interface design, but the key requirement is explicit traffic steering through the security appliance. See the AWS VPC route table documentation.