Netskope NSK300 Practice Questions

Shared by Shaw on 03-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You are already using Netskope CSPM to monitor your AWS accounts for compliance. Now you need to allow access from your company-managed devices running the Netskope Client to only Amazon S3 buckets owned by your organization. You must ensure that any current buckets and those created in the future will be allowed

Which configuration satisfies these requirements?

Options:

A- Steering: Cloud Apps Only, All Traffic Policy type: Real-time Protection
Constraint: Storage. Bucket Does Not Match -ALLAccounts Action: Block
B- Steering: Cloud Apps Only Policy type: Real-time Protection
Constraint: Storage. Bucket Does Not Match *@myorganization.com Action: Block
C- Steering: Cloud Apps Only. All Traffic Policy type: Real-time Protection Constraint: Storage. Bucket Does Match -ALLAccounts Action: Allow
D- Steering: All Web Traffic Policy type: API Data Protection
Constraint: Storage, Bucket Does Match *@myorganization.com Action: Allow

Answer:

C

Explanation:

To allow access from company-managed devices running the Netskope Client to only Amazon S3 buckets owned by the organization, the following configuration satisfies the requirements:

Steering Configuration:

Policy Type: Real-time Protection

Constraint: Storage

Bucket Condition: Bucket Does Match -ALLAccounts

Action: Allow

By configuring the policy to allow traffic from company-managed devices (Netskope Clients) to Amazon S3 buckets, the organization ensures that only buckets owned by the organization are accessible.

The-ALLAccountscondition ensures that both existing and future buckets are allowed.

This configuration aligns with the requirement to allow access to organization-owned buckets while blocking access to other buckets.

Netskope Cloud Security

Netskope Solution Brief

Netskope Community

Question 2

Question Type: MultipleChoice

You are currently designing a policy for AWS S3 bucket scans with a custom DLP profile Which policy action(s) are available for this policy?

Options:

A- Alert, Quarantine. Block, User Notification
B- Alert, User Notification
C- Alert only
D- Alert, Quarantine

Answer:

D

Explanation:

When designing a policy for AWS S3 bucket scans with a custom DLP profile in Netskope, the available policy actions are Alert and Quarantine. These actions allow you to be notified when a policy violation occurs and to quarantine sensitive data to prevent potential data loss or exposure. The Alert action will notify the designated personnel or system when a match to the DLP profile is found during the scan. The Quarantine action will move the offending file to a secure location where it can be reviewed and dealt with appropriately1.

Question 3

Question Type: MultipleChoice

You are asked to create a customized restricted administrator role in your Netskope tenant for a newly hired employee. Which two statements are correct in this scenario? (Choose two.)

Options:

A- An admin role prevents admins from downloading and viewing file content by default.
B- The scope of the data shown in the Ul can be restricted to specific events.
C- All role privileges default to Read Only for all functional areas.
D- Obfuscation can be applied to all functional areas.

Answer:

A, C

Explanation:

Admin Role and File Content Viewing: By default, an admin role doesnotprevent admins from downloading and viewing file content. Admins have access to view and download file content unless specific restrictions are applied.

Role Privileges Default to Read Only: All role privileges in Netskope default toRead Onlyfor all functional areas. This means that admins can view information but cannot make changes unless explicitly granted additional permissions.

Obfuscation: Obfuscation can be applied to specific functional areas, but it is not a default behavior for all areas.Reference:

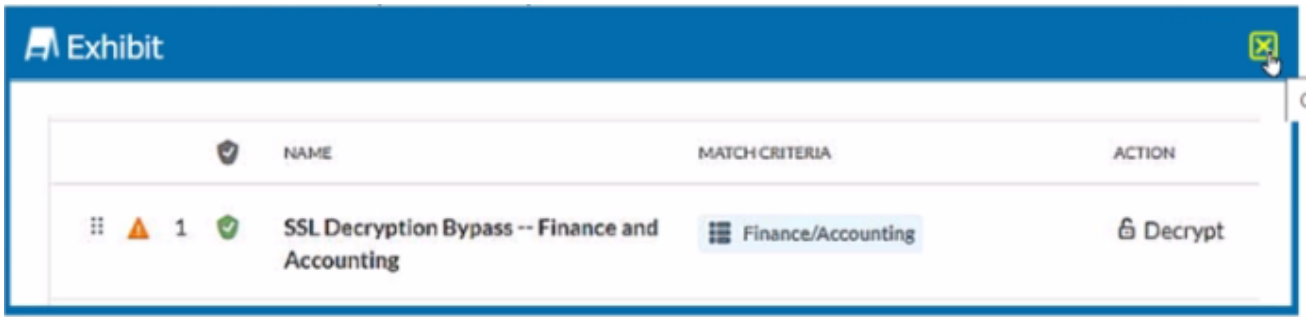
Netskope Security Cloud Introductory Online Technical Training

Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training

Question 4

Question Type: MultipleChoice

Review the exhibit.



You created an SSL decryption policy to bypass the inspection of financial and accounting Web categories. However, you still see banking websites being inspected.

Referring to the exhibit, what are two possible causes of this behavior? (Choose two.)

Options:

A- The policy is in a 'disabled' state.
B- An incorrect category has been selected
C- The policy is in a 'pending changes' state.
D- An incorrect action has been specified.

Answer:

B, D

Explanation:

The issue described in the exhibit is that banking websites are still being inspected despite creating an SSL decryption policy to bypass the inspection of financial and accounting web categories.

Possible Causes:

An incorrect category has been selected (Option B):

If the SSL decryption policy is configured to bypass the wrong category (e.g., not the actual financial and accounting category), it won't effectively exclude banking websites from inspection.

An incorrect action has been specified (Option D):

If the action specified in the policy is not set to ''Bypass,'' it won't achieve the desired behavior. The policy should explicitly bypass SSL inspection for the selected category.

Solution:

Verify that the correct category (financial and accounting) is selected in the policy, and ensure that the action is set to ''Bypass.''

Question 5

Question Type: MultipleChoice

Users in your network are attempting to reach a website that has a self-signed certificate using a GRE tunnel to Netskope. They are currently being blocked by Netskope with an SSL error. How would you allow this traffic?

Options:

A- Configure a Do Not Decrypt SSL Decryption rule to allow traffic to pass.
B- Configure a Real-time Protection policy with the action set to Allow.
C- Set the No SNI setting in Netskope to Bypass.
D- Ensure that the users add the self-signed certificate to their local certificate store.

Answer:

A

Explanation:

To allow traffic from a website with a self-signed certificate that is being blocked by Netskope with an SSL error, the correct action is to configure a Do Not Decrypt SSL Decryption rule. This rule will allow the traffic to pass without being decrypted, thus bypassing the SSL error caused by the self-signed certificate. This is a common practice for handling traffic from trusted internal applications or specific external sites that use self-signed certificates1.

Question 6

Question Type: MultipleChoice

You built a number of DLP profiles for different sensitive data types. If a file contains any of this sensitive data, you want to take the most restrictive policy action but also create incident details for all matching profiles.

Which statement is correct in this scenario?

Options:

A- Create a Real-time Protection policy for each DLP profile; each matched profile will generate a unique DLP incident.
B- Create a Real-time Protection policy for each DLP profile; all matched profiles will show up in a single DLP incident
C- Create a single Real-time Protection policy and include all of the DLP profiles; each matched profile will generate a unique DLP incident
D- Create a single Real-time Protection policy and include all of the DLP profiles; all matched profiles will show up in a single DLP incident.

Answer:

D

Explanation:

When configuring a Real-time Protection policy with multiple DLP profiles, if the content matches multiple profiles, the policy performs the most restrictive action associated with the DLP profiles that match for that policy. The resulting incident lists all the profiles that matched along with their corresponding forensic information.This means that even though the most restrictive action is taken, details for all matching profiles are created and included in a single DLP incident12.

Question 7

Question Type: MultipleChoice

You want to integrate with a third-party DLP engine that requires ICAP. In this scenario, which Netskope platform component must be configured?

Options:

A- On-Premises Log Parser (OPLP)
B- Secure Forwarder
C- Netskope Cloud Exchange
D- Netskope Adapter

Answer:

D

Explanation:

When integrating a third-party Data Loss Prevention (DLP) engine that requires ICAP, the Netskope platform component that must be configured is theNetskope Adapter. The Netskope Adapter is designed to facilitate the integration of Netskope with various third-party tools and services, including DLP engines that use ICAP for communication. By configuring the Netskope Adapter, you can ensure that the third-party DLP engine can communicate effectively with the Netskope platform to provide comprehensive data protection.

Question 8

Question Type: MultipleChoice

You want customers to configure Real-time Protection policies. In which order should the policies be placed in this scenario?

Options:

A- Threat, CASB, RBI, Web
B- RBI, CASB, Web, Threat
C- Threat, RBI, CASB, Web
D- CASB, RBI, Threat, Web

Answer:

B

Explanation:

When configuring Real-time Protection policies in Netskope, the recommended order is as follows:

RBI (Risk-Based Index) Policies: These policies focus on risk assessment and prioritize actions based on risk scores. They help identify high-risk activities and users.

CASB (Cloud Access Security Broker) Policies: These policies address cloud-specific security requirements, such as controlling access to cloud applications, enforcing data loss prevention (DLP) rules, and managing shadow IT.

Web Policies: These policies deal with web traffic, including URL filtering, web categories, and threat prevention.

Threat Policies: These policies focus on detecting and preventing threats, such as malware, phishing, and malicious URLs.

Placing the policies in this order ensures that risk assessment and cloud-specific controls are applied before addressing web and threat-related issues.Reference:

Netskope Security Cloud Introductory Online Technical Training

Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training

Netskope Certification Description

Netskope Architectural Advantage Features

Question 9

Question Type: MultipleChoice

You are already using Netskope CSPM to monitor your AWS accounts for compliance. Now you need to allow access from your company-managed devices running the Netskope Client to only Amazon S3 buckets owned by your organization. You must ensure that any current buckets and those created in the future will be allowed

Which configuration satisfies these requirements?

Options:

A- Steering: Cloud Apps Only, All Traffic Policy type: Real-time Protection Constraint: Storage. Bucket Does Not Match -ALLAccounts Action: Block
B- Steering: Cloud Apps Only Policy type: Real-time Protection Constraint: Storage. Bucket Does Not Match *@myorganization.com Action: Block
C- Steering: Cloud Apps Only. All Traffic Policy type: Real-time Protection Constraint: Storage. Bucket Does Match -ALLAccounts Action: Allow
D- Steering: All Web Traffic Policy type: API Data Protection Constraint: Storage, Bucket Does Match *@myorganization.com Action: Allow

Answer:

C

Explanation:

To allow access from company-managed devices running the Netskope Client to only Amazon S3 buckets owned by the organization, the following configuration satisfies the requirements:

Steering Configuration:

Policy Type: Real-time Protection

Constraint: Storage

Bucket Condition: Bucket Does Match -ALLAccounts

Action: Allow

By configuring the policy to allow traffic from company-managed devices (Netskope Clients) to Amazon S3 buckets, the organization ensures that only buckets owned by the organization are accessible.

The-ALLAccountscondition ensures that both existing and future buckets are allowed.

This configuration aligns with the requirement to allow access to organization-owned buckets while blocking access to other buckets.

Netskope Cloud Security

Netskope Solution Brief

Netskope Community

Question 10

Question Type: MultipleChoice

Review the exhibit.

1

SOURCE	DESTINATION	PROFILE	ACTION
Any	Microsoft Office 365 Suite:AcmeCorp	None	Allow
Any	Microsoft Office 365 OneDrive for Business, Microsoft OneDrive, MS GCC Office 365 OneDrive for Business Create, Post, Share, Upload	None	Block Default Template
Any	Microsoft Office 365 OneDrive for Business:AcmeCorp	None	Allow
Any	Microsoft Office 365 Suite	None	Block Default Template

2

SOURCE	DESTINATION	PROFILE	ACTION
Any	Microsoft Office 365 Suite:AcmeCorp	None	Allow
Any	Microsoft Office 365 Suite	None	Block Default Template
Any	Microsoft Office 365 OneDrive for Business, Microsoft OneDrive, MS GCC Office 365 OneDrive for Business	None	Allow

3

SOURCE	DESTINATION	PROFILE	ACTION
Any	Microsoft Office 365 Suite:AcmeCorp	None	Allow
Any	Microsoft Office 365 Suite	None	Block Default Template

4

SOURCE	DESTINATION	PROFILE	ACTION
Any	Microsoft Office 365 OneDrive for Business, Microsoft OneDrive, MS GCC Office 365 OneDrive for Business Create, Post, Share, Upload	None	Block Default Template
Any	Microsoft Office 365 OneDrive for Business:AcmeCorp	None	Allow

AcmeCorp has recently begun using Microsoft 365. The organization is concerned that employees will start using third-party non-AcmeCorp OneDrive instances to store company dat

a. The CISO asks you to use Netskope to create a policy that ensures that no data is being uploaded to non-AcmeCorp instances of OneDrive.

Referring to the exhibit, which two policies would accomplish this posture? (Choose two.)

Options:

A- 4
B- 3
C- 2
D- 1

Answer:

B, C

Explanation:

To ensure that no data is uploaded to non-AcmeCorp instances of OneDrive, the policies that would accomplish this are:

Policy B: This policy allows traffic only for AcmeCorp's OneDrive and blocks all other Microsoft 365 Suite traffic. It ensures that data is not uploaded to non-AcmeCorp OneDrive instances by restricting access to only the corporate instance of OneDrive.

Policy C: This policy allows traffic for AcmeCorp's Microsoft 365 Suite but blocks all other OneDrive for Business traffic. It achieves the same outcome by permitting corporate suite usage while preventing uploads to any OneDrive for Business instances that are not part of AcmeCorp.

These policies are designed to provide granular control over the data flow, ensuring that company data remains within the corporate environment and is not transferred to external or personal storage solutions.

Question 11

Question Type: MultipleChoice

You created a Real-time Protection policy that blocks all activities to non-corporate S3 buckets, but determine that the policy is too restrictive. Specifically, users are complaining that normal websites have stopped rendering properly.

How would you solve this problem?

Options:

A- Create a Real-time Protection policy to allow the Browse activity to the Amazon S3 application.
B- Create a Real-time Protection policy to allow the Browse activity to the Cloud Storage category
C- Create a Real-time Protection policy to allow the Download activity to the Cloud Storage category
D- Create a Real-time Protection policy to allow the Download activity to the Amazon S3 application

Answer:

B

Explanation:

To solve the problem of normal websites not rendering properly due to a Real-time Protection policy that blocks all activities to non-corporate S3 buckets, the best solution is tocreate a Real-time Protection policy to allow the Browse activity to the Cloud Storage category. This approach will enable users to view content from various cloud storage services, including Amazon S3, without allowing full access to non-corporate S3 buckets.It's a more granular and less restrictive policy that allows necessary browsing activities while still maintaining control over the upload and download activities to non-corporate buckets1.

Question 12

Question Type: MultipleChoice

Your Netskope Client tunnel has connected to Netskope; however, the user is not receiving any steering or client configuration updates What would cause this issue?

Options:

A- The client is unable to establish communication to add-on-[tenantl.goskope.com.
B- The client is unable to establish communication to gateway-(tenant|.goskope.com.
C- The Netskope Client service is not running.
D- An invalid steering exception was created in the tenant

Answer:

C

Explanation:

When the Netskope Client service is not running, it cannot execute the necessary processes to receive steering or client configuration updates. The service must be active to establish communication with the Netskope cloud and apply the configurations and policies defined by the administrator.

P2P exams

P2P exams

To Get Premium Files for NSK300 Visit

https://www.p2pexams.com/products/nsk300

For More Free Questions Visit

https://www.p2pexams.com/netskope/pdf/nsk300

