Netskope NSK101 NCCSA Practice Questions

Shared by Clay on 03-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What are two pillars of CASB? (Choose two.)

Options:

A- visibility
B- compliance
C- cloud native
D- SASE

P2P exams

Answer:

A, B

Explanation:

Two pillars of CASB are visibility and compliance. CASB stands for Cloud Access Security Broker, which is a solution that provides visibility and control over cloud services and web traffic, as well as data and threat protection for cloud users and devices. Visibility is the capability to identify all cloud services in use and assess their risk factors, such as security, auditability, business continuity, etc. Compliance is the capability to ensure that cloud services and data meet the regulatory standards and policies of the organization or industry, such as GDPR, HIPAA, PCI DSS, etc.Reference:What Is a Cloud Access Security Broker (CASB)? | MicrosoftCASB Guide: What are the 4 Pillars of CASB? - Security Service Edge

P2P exams

Question 2

Question Type: MultipleChoice

When would an administrator need to use a tombstone file?

Options:

A- You use a tombstone file when a policy causes a file download to be blocked.
B- You use a tombstone file when a policy causes a publicly shared file to be encrypted.
C- You use a tombstone file when the policy causes a file to be moved to quarantine.
D- You use a tombstone file when a policy causes a file to be moved to legal hold.

Answer:

C

Explanation:

A tombstone file is a placeholder file that replaces the original file when it is moved to quarantine by a Netskope policy. The tombstone file contains information about the original file, such as its name, size, type, owner, and the reason why it was quarantined. The tombstone file also provides a link to the Netskope UI where the administrator or the file owner can view more details about the incident and take appropriate actions, such as restoring or deleting the file. The purpose of using a tombstone file is to preserve the metadata and location of the original file, as well as to notify the users about the quarantine action and how to access the file if needed.Reference:Threat Protection - Netskope Knowledge PortalNetskope threat protection - Netskope

Question 3

Question Type: MultipleChoice

You want to block access to sites that use self-signed certificates. Which statement is true in this scenario?

Options:

A- Certificate-related settings apply globally to the entire customer tenant.
B- Certificate-related settings apply to each individual steering configuration level.
C- Certificate-related settings apply to each individual client configuration level.
D- Self-signed certificates must be changed to a publicly trusted CA signed certificate.

Answer:

B

Explanation:

The statement that is true in this scenario is: Certificate-related settings apply to each individual steering configuration level. Certificate-related settings are the options that allow you to configure how Netskope handles SSL/TLS certificates for encrypted web traffic. For example, you can choose whether to allow or block self-signed certificates, expired certificates, revoked

certificates, etc. You can also choose whether to enable SSL decryption for specific domains or categories. Certificate-related settings apply to each individual steering configuration level, which means that you can have different settings for different types of traffic or devices. For example, you can have one steering configuration for managed devices and another one for unmanaged devices, and apply different certificate-related settings for each one. This allows you to customize your security policies based on your needs and preferences.Reference:Netskope SSL DecryptionNetskope Steering Configuration

Question 4

Question Type: MultipleChoice

Which three components make up the Borderless SD-WAN solution? (Choose three)

Options:

A- Endpoint SD-WAN Client
B- SASE Orchestrator
C- NPA Publisher
D- SASE Gateway
E- On-Premises Log Parser

Answer:

A, B, D

Explanation:

The three components that make up the Borderless SD-WAN solution are:

Endpoint SD-WAN Client: This client is installed on endpoints (such as laptops and mobile devices) to ensure secure and optimized connectivity to the corporate network, even when users are remote. The Endpoint SD-WAN Client is a critical part of extending SD-WAN capabilities to individual users and devices, providing seamless connectivity and security.

SASE Orchestrator: The Secure Access Service Edge (SASE) Orchestrator is responsible for managing and orchestrating the various components of the SD-WAN solution. It ensures that policies are enforced consistently across the network, manages the deployment of network functions, and provides centralized control and visibility.

SASE Gateway: The SASE Gateway provides secure, optimized access to cloud applications and services. It combines SD-WAN capabilities with advanced security functions, such as firewalling, intrusion prevention, and secure web gateways, to protect data and users as they access

resources from different locations.

These components work together to provide a comprehensive SD-WAN solution that addresses the needs of modern, distributed workforces by combining networking and security functions in a unified architecture.

Netskope REST API v2 Overview.

Using the REST API v2 dataexport Iterator Endpoints.

Using the REST API v2 UCI Impact Endpoints.

Netskope SDK on PyPI.

Postman Collection for Netskope REST API.

P2P exams

Question 5

Question Type: MultipleChoice

You need to create a service request ticket for a client-related issue using the Netskope client Ul. In this scenario, you generate the client logs by right-clicking on the system tray icon and choosing

Options:

A- Save logs
B- Configuration
C- Troubleshoot
D- Help

P2P exams

Answer:

C

Explanation:

To create a service request ticket for a client-related issue using the Netskope client UI, you need to generate the client logs by right-clicking on the system tray icon and choosing Troubleshoot. This will open a window where you can select the option to Save Logs, which will create a zip file containing the client logs. You can then attach this file to your service request ticket and provide any relevant details about the issue. Choosing Save logs, Configuration, or Help will not generate the client logs, as they perform different functions, such as saving the

current configuration, opening the settings menu, or opening the help page.Reference:[Netskope Client Troubleshooting].

Question 6

Question Type: MultipleChoice

You want to take into account some recent adjustments to CCI scoring that were made in your Netskope tenant.

In this scenario, which two CCI aspects in the Ul would be used in a real-time protection policy? (Choose two.)

Options:

A- App Tag
B- CCL
C- App Score
D- GDPR Readiness

Answer:

A, C

Explanation:

To take into account some recent adjustments to CCI scoring that were made in your Netskope tenant, you can use the App Tag and App Score aspects in the UI to create a real-time protection policy. The App Tag is a label that indicates the level of enterprise readiness of a cloud app based on its CCI score. The App Score is a numerical value that represents the CCI score of a cloud app based on various criteria such as security, auditability, and business continuity. You can use these aspects to filter cloud apps by their CCI ratings and apply policies accordingly. For example, you can create a policy that blocks access to cloud apps with an App Tag of Poor or an App Score below 50.Reference:Netskope Cloud Confidence IndexCreating Real-Time Policies for Cloud Applications

Question 7

Question Type: MultipleChoice

How do you protect your data at rest intellectual property (IP), such as source code or product designs, stored in Microsoft 365 SharePoint?

Options:

A- by configuring Netskope Explicit Proxy in the user's browser
B- by steering SharePoint traffic over GRE or IPsec to a Netskope cloud proxy
C- by using Netskope's API-enabled Protection for SharePoint
D- by steering SharePoint traffic using the Netskope Client

Answer:

C

Explanation:

Protecting Data at Rest in SharePoint:

Protecting intellectual property stored in Microsoft 365 SharePoint requires a solution that can monitor and control data access and usage.

Netskope's API-enabled Protection integrates directly with Microsoft 365 to provide comprehensive security for data at rest.

API-enabled Protection:

Netskope's API-enabled Protection allows direct integration with SharePoint, enabling continuous monitoring and enforcement of security policies.

It ensures that data such as source code or product designs are protected from unauthorized access and potential data breaches.

Configuration:

Configure API-enabled Protection by navigating to the Netskope admin console.

Set up the necessary API integrations with Microsoft 365 SharePoint.

Define security policies to monitor and control access to sensitive data stored in SharePoint.

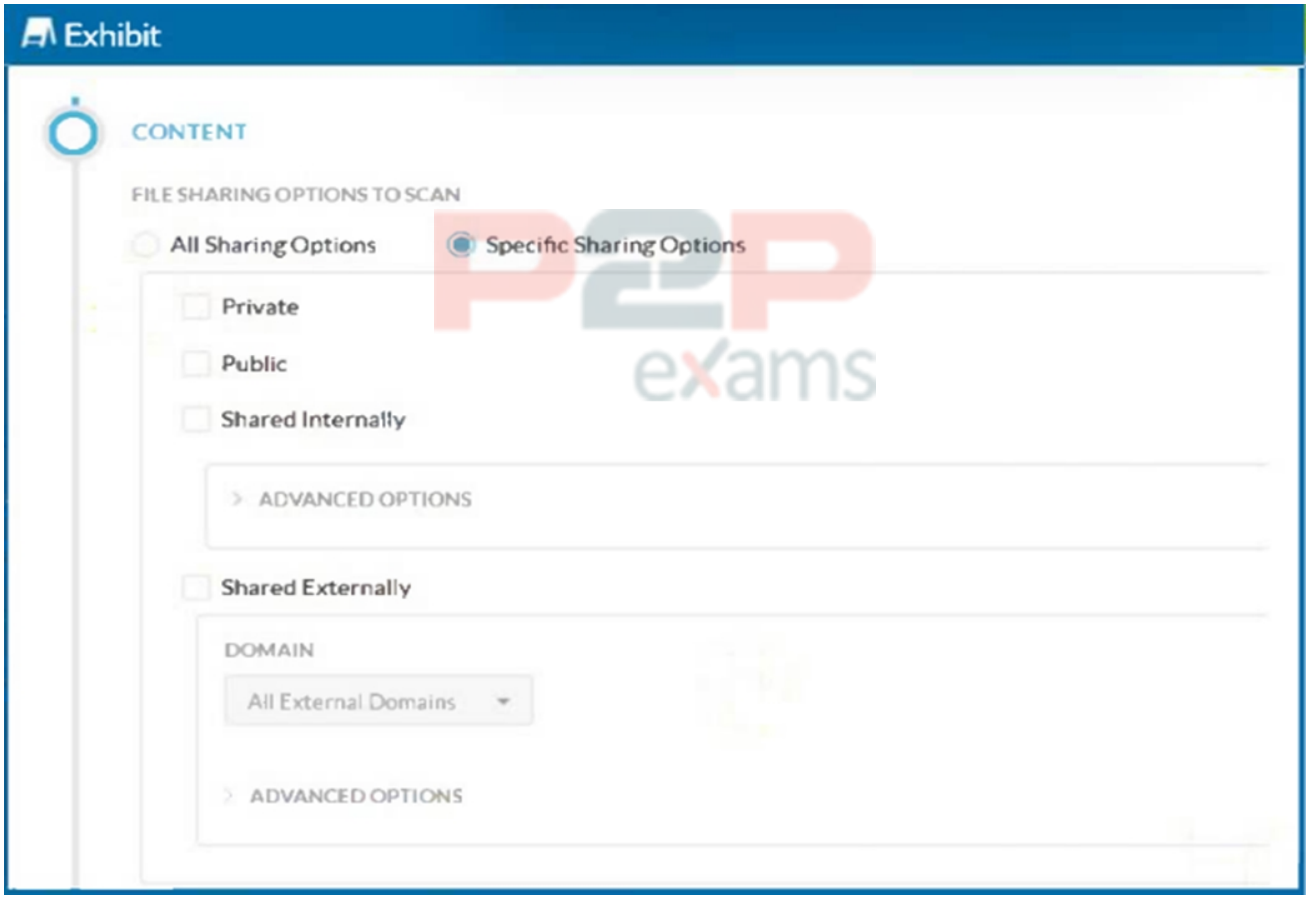
Reference:

For more details on setting up and configuring API-enabled Protection for SharePoint, refer to the Netskope documentation on API-enabled protection solutions.

Question 8

Question Type: MultipleChoice

Click the Exhibit button.



A customer has created a CASB API-enabled Protection policy to detect files containing sensitive data that are shared outside of their organization.

Referring to the exhibit, which statement is correct?

Options:

A- The administrator needs to use Shared Externally as the only shared option.
B- The administrator needs to use Shared Externally and Public as the shared options.
C- The administrator must select Private as the only shared option.
D- The administrator needs to use Public as the only shared option.

Answer:

B

Explanation:

To detect files containing sensitive data that are shared outside of the organization, the administrator should select both 'Shared Externally' and 'Public' sharing options. These settings ensure that any files shared externally (outside the organization) or publicly are scanned for sensitive data. This comprehensive approach covers all potential scenarios where data could be exposed outside the organization.

Step-by-Step Configuration:

Select Specific Sharing Options:

Navigate to the CASB API-enabled Protection policy configuration page.

Choose the option for 'Specific Sharing Options' to limit the scan to files shared under certain conditions.

Enable Shared Externally and Public:

Check both 'Shared Externally' and 'Public' options. This setting ensures that files shared either publicly or with external domains are included in the scan.

Configure Advanced Options:

For further granularity, configure the advanced options under each sharing type if needed (e.g., specifying particular external domains).

This configuration aligns with the best practices for CASB policies and ensures that all files potentially leaving the organization are scanned for sensitive data.

Netskope CASB Policy Configuration Documentation

Question 9

Question Type: MultipleChoice

What are two benefits of creating a policy group as a logical collection of Real-time Protection policies? (Choose two.)

Options:

A- To split up policies by region or business unit.
B- To enable Alert and Continue policies.
C- To simplify workflow, allowing exact access to a specific set of policies.
D- To provide additional actions based on policy match criteria.

Answer:

A, C

Explanation:

Creating a policy group as a logical collection of Real-time Protection policies provides several benefits:

To split up policies by region or business unit: This allows for more granular control and management of policies based on organizational structure. Each region or business unit can have its own set of policies tailored to its specific needs and compliance requirements.

To simplify workflow, allowing exact access to a specific set of policies: Policy groups help streamline the management process by grouping related policies together. This simplifies the workflow for administrators by providing them with access to only the relevant policies they need to manage, reducing complexity and potential for errors.

Netskope documentation on creating and managing policy groups.

Best practices for organizing policies to enhance manageability and operational efficiency.

To Get Premium Files for NSK101 Visit

https://www.p2pexams.com/products/nsk101

For More Free Questions Visit

https://www.p2pexams.com/netskope/pdf/nsk101

