DUMPSBOSS.

Netskope Certified Cloud Security Administrator (NCCSA)

Netskope NSK101

Version Demo

Total Demo Questions: 15

Total Premium Questions: 151

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Which two functions are available for both inline and API protection? (Choose two.)

A. multi-factor authentication

B. threat protection

C. DLP

D. Cloud Security Posture Management (CSPM)

ANSWER: B C

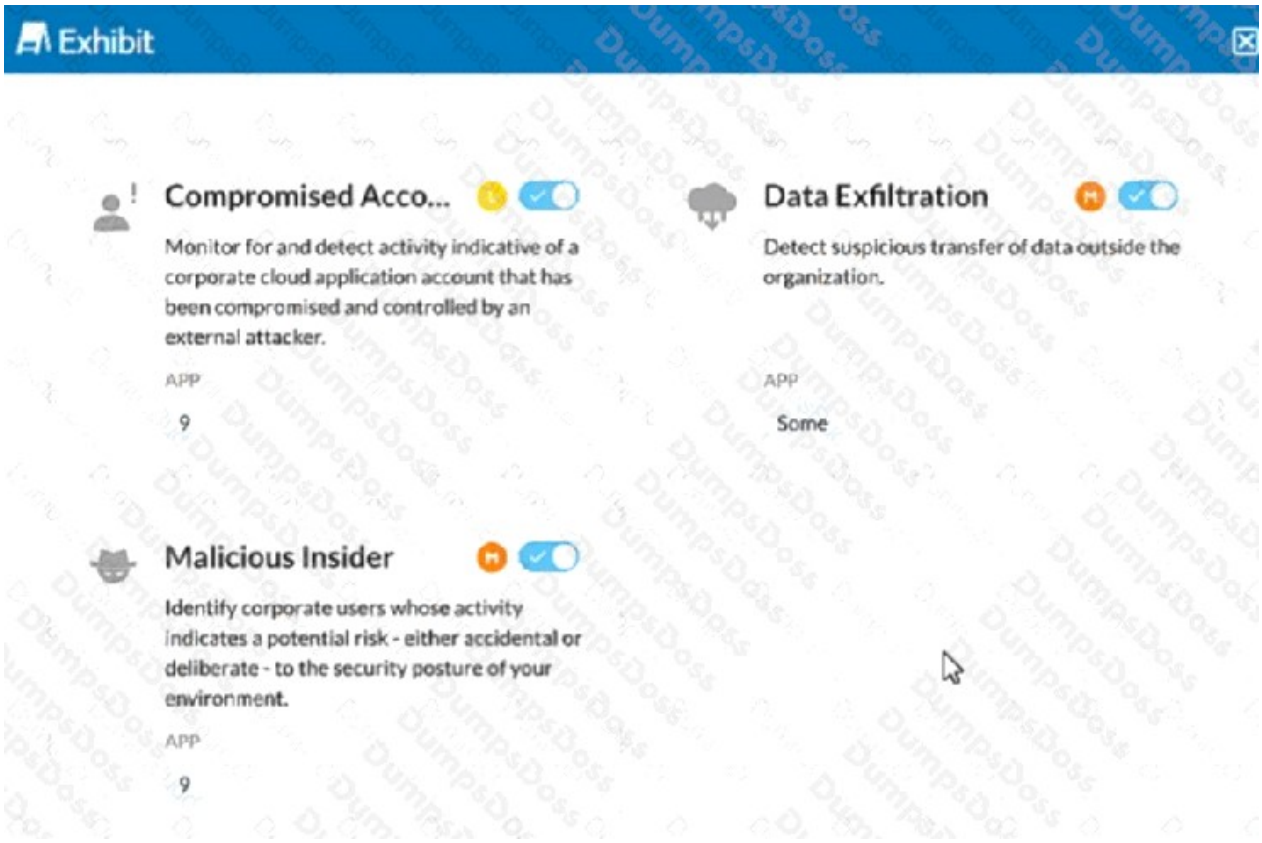
Explanation:

threat protection and **DLP** are available through both Netskope inline and API-based protection. Inline protection evaluates traffic in real time as users interact with sanctioned and unsanctioned cloud applications or websites. This enables policy enforcement during the transaction, including inspection for sensitive content and malicious files. API protection connects to supported SaaS applications to inspect data that already resides in those applications, providing out-of-band discovery and remediation for existing files and objects.

Netskope DLP policies can be applied in both deployment models to identify sensitive information using predefined or custom data identifiers, then enforce the configured protection action. Threat protection likewise supports both models: inline inspection can prevent malicious content from reaching users or cloud services, while API scanning can identify malware in content already stored in connected SaaS tenants. Using both methods provides coverage for data in motion and data at rest, allowing consistent data and threat controls across cloud usage. Netskope describes these complementary capabilities in its Cloud Access Security Broker overview and Data Loss Prevention overview.

QUESTION NO: 2

Click the Exhibit button.



The exhibit shows security rules that are part of which component of the Netskope platform?

A. Real-time Protection

B. Advanced Malware Protection

C. Security Posture

D. Behavior Analytics

ANSWER: D

Explanation:

Behavior Analytics is the Netskope platform component that provides detections and rules focused on risky or anomalous user activity, including indicators associated with compromised accounts, suspicious data movement or exfiltration, and potential insider threats. It applies user and entity behavior analytics principles to establish activity patterns and identify deviations that merit investigation. These detections help security teams prioritize events by connecting actions to user behavior, access context, applications, and data activity rather than evaluating each event in isolation.

In the Netskope tenant, Behavior Analytics is therefore the appropriate area for rules designed to identify behavioral risk scenarios. It supports investigation workflows by surfacing unusual activity that can indicate account takeover, misuse of authorized access, or data handling behavior inconsistent with an established baseline. This is particularly valuable for cloud applications and web activity, where valid credentials alone do not establish that a session or action is trustworthy. Netskope describes its UEBA capabilities as identifying anomalous behavior and insider-risk activity through analytics-driven detection. See the Netskope User Behavior Analytics product overview and the Netskope Behavior Analytics documentation.

QUESTION NO: 3

You added a new private app definition and created a Real-time Protection policy to allow access for all users. You have a user who reports that they are unable to access the application but all other applications work fine.

Which statement correctly describes how to troubleshoot this issue using the Netskope Web UI?

A. You can verify the user's policy, steering configuration, client status and other relevant details using the Advanced Debugging tools in the Netskope Client.

B. You can verify the user's policy, steering configuration, client status and other relevant details using the App Discovery dashboard.

C. You can verify the user's policy, steering configuration, client status and other relevant details using DEM.

D. You can verify the user's policy, steering configuration, client status and other relevant details using the NPA Troubleshooter tool.

ANSWER: D

Explanation:

You can verify the user's policy, steering configuration, client status and other relevant details using the NPA Troubleshooter tool. This is the purpose-built Web UI workflow for diagnosing a user’s access to a Netskope Private Access application. It helps an administrator evaluate the access path for the affected user and private application, including whether the user matches an applicable Real-time Protection policy, whether traffic is being steered to Netskope, and whether the endpoint client and private-app connectivity components are in an appropriate state. Because the problem is isolated to one newly defined private application while other applications continue to work, examining the application-specific access decision and connectivity path is especially valuable. The troubleshooter consolidates the relevant diagnostic context rather than requiring the administrator to infer the cause from general dashboards or endpoint-only diagnostics. It can therefore identify whether the access request is reaching the Netskope platform, being evaluated against the intended policy, and being routed toward the configured private application resources. Netskope Private Access provides application-level, identity-aware connectivity, so validation of the user, policy, app definition, steering, and client path is central to resolving this type of issue. See the Netskope Private Access documentation and the Netskope documentation portal.

QUESTION NO: 4

A cloud security team needs to continuously identify risky configuration settings in its public-cloud environment, such as overly permissive storage access and missing security controls. The team also needs prioritized posture findings for remediation.

Which Netskope capability addresses this requirement?

A. Cloud Security Posture Management (CSPM)

B. Data Loss Prevention (DLP)

C. Threat Protection

D. Cloud Confidence Index (CCI)

ANSWER: A

Explanation:

Cloud Security Posture Management (CSPM) is the appropriate capability because it evaluates public-cloud configurations against security and compliance requirements, identifies configuration risks, and helps prioritize remediation. CSPM focuses on the security posture of cloud infrastructure and services.

DLP identifies sensitive data, while Threat Protection focuses on malicious content and activity. Cloud Confidence Index ratings assess cloud application risk and enterprise readiness rather than an organization's own public-cloud configuration posture.

QUESTION NO: 5

You are working with a large retail chain and have concerns about their customer data. You want to protect customer credit card data so that it is never exposed in transit or at rest. In this scenario, which regulatory compliance standard should be used to govern this data?

A. SOC 3

B. PCI-DSS

C. AES-256

D. ISO 27001

ANSWER: B

Explanation:

PCI-DSS is the appropriate standard because it is specifically designed to protect payment account data handled by merchants, processors, service providers, and other entities in the payment-card ecosystem. Its requirements apply to cardholder data and sensitive authentication data throughout the cardholder data environment, including when data is stored, processed, or transmitted. PCI DSS requires organizations to protect stored account data, use strong cryptography and security protocols when transmitting account data over open or public networks, restrict access according to business need, monitor systems, and maintain security policies and incident-response processes. For a retail chain handling customer credit-card information, PCI DSS therefore provides the directly relevant compliance framework for establishing the required safeguards and validating their implementation. The current PCI DSS standard is maintained by the PCI Security Standards Council; version 4.0.1 is the active version and clarifies the baseline technical and operational controls expected for payment-card data protection. See the PCI Security Standards Council PCI DSS overview and the PCI SSC Document Library for the official standard and supporting resources.

QUESTION NO: 6

You are working with traffic from applications with pinned certificates. In this scenario, which statement is correct?

A. An exception should be added to the steering configuration.

B. The domains used by certificate-pinned applications should be added to the authentication bypass list.

C. Traffic with pinned certificates should be blocked.

D. The domains used by applications with pinned certificates should be allowed in an inline policy.

ANSWER: A

Explanation:

An exception should be added to the steering configuration. Certificate-pinned applications validate the server certificate or public-key information against an expected value embedded in the application. When inline TLS decryption is applied, the security service must present a substitute certificate to inspect the encrypted session. That certificate does not match the certificate or key the application has pinned, so the application can reject the connection and its traffic may fail. A steering exception prevents the affected destination traffic from being sent through the inline inspection path, allowing the application to establish its end-to-end TLS session with the original destination certificate intact. The exception should be scoped as narrowly as practical to the required domains, hosts, or traffic so that only the certificate-pinned application traffic bypasses the relevant steering path. This is a traffic-handling requirement rather than an authentication decision or an inline-policy allowance. Netskope's documentation portal contains the configuration guidance for traffic steering and client behavior at Netskope Documentation; additional product configuration resources are available through the Netskope Support portal.

QUESTION NO: 7

Which two common security frameworks are used today to assess and validate a vendor ' s security practices? (Choose two.)

A. Data Science Council of America

B. Building Security in Maturity Model

C. ISO 27001

D. NIST Cybersecurity Framework

ANSWER: B C

Explanation:

Building Security in Maturity Model and **ISO 27001** are appropriate frameworks for evaluating a vendor's security maturity and security-management practices. BSIMM is a data-driven maturity model for assessing software security initiatives. It organizes observed software-security activities into practices and allows an organization to compare the breadth and maturity of its program with those observed across participating organizations. In a vendor-review context, this can help assess whether a software supplier has repeatable secure-development, governance, testing, and vulnerability-management practices.

ISO 27001 is an internationally recognized standard for an information security management system (ISMS). An organization may be independently certified against ISO 27001, giving customers a commonly understood way to validate that the vendor operates a structured, risk-based program to establish, maintain, and continually improve information-security controls. Vendor due-diligence processes frequently use ISO 27001 certification and related ISMS evidence as assurance inputs. BSIMM details are available from BSIMM, and ISO describes the standard at ISO/IEC 27001.

QUESTION NO: 8

Your organization allows employees to upload approved documents to its managed Google Drive tenant but must block uploads of sensitive customer data to personal Google Drive accounts.

Which two configuration actions support this requirement? (Choose two.)

A. Define the managed Google Drive tenant as an App Instance.

B. Create a Real-time Protection policy that uses the instance and DLP context.

C. Create an allow policy for all Google Drive instances.

D. Use API-enabled Protection for the personal Google Drive account.

ANSWER: A B

Explanation:

Defining the managed Google Drive tenant as an App Instance gives Netskope the destination context needed to distinguish the enterprise-owned tenant from personal Google Drive usage. Without instance awareness, both destinations can appear as the same cloud application.

A Real-time Protection policy can then use the application-instance context together with a DLP profile to block sensitive uploads to personal or unmanaged instances while allowing the approved activity in the managed enterprise instance. A broad Google Drive allow policy would remove the required distinction, and API-enabled Protection is intended for authorized sanctioned SaaS tenants and data at rest rather than inline control of a personal account upload.

QUESTION NO: 9

A customer is reviewing cloud applications using the default Cloud Confidence Index score. Its legal team considers a provider's data-ownership terms substantially more important than the default scoring model does.

What is a valid reason for the customer to customize the CCI scoring?

A. To apply greater risk weight to the provider's data-ownership terms

B. To create a CCI rating for an application that is not yet researched

C. To reduce a vendor's score because of poor customer service

D. To change an Under Research application into a sanctioned application

ANSWER: A

Explanation:

The customer can customize CCI scoring to apply a higher business-risk weight to data-ownership criteria. The default CCI score provides a broadly applicable assessment, but organizations can have different legal, regulatory, operational, and risk-management priorities. Adjusting the weighting allows the application score to reflect this customer's specific governance requirements.

Custom scoring does not create a CCI rating for an application that has not yet been researched, and it is not intended to penalize a vendor for unrelated service-quality concerns. It also does not change the underlying application inventory merely because an application is marked Under Research.

QUESTION NO: 10

A branch network contains printers, servers, and other devices that cannot run the Netskope Client. The organization needs to steer the branch traffic to the Netskope Security Cloud for inspection and policy enforcement.

Which Netskope Virtual Appliance deployment role should be used?

A. Secure Forwarder

B. NPA Publisher

C. On-Premises Log Parser

D. Exact Data Match hash generator

ANSWER: A

Explanation:

Deploy the Netskope Virtual Appliance as a Secure Forwarder. A Secure Forwarder is used to forward traffic from network-based sources, including sites and devices that cannot run the Netskope Client, to the Netskope Security Cloud for inspection and policy enforcement.

A Publisher provides NPA connectivity to private applications, and a log parser ingests network logs for cloud-application discovery. Neither role performs the required inline traffic-forwarding function for the branch devices.

QUESTION NO: 11

Your organization wants to restrict access to the Netskope Admin UI to administrators connecting from approved public egress addresses. It also requires an organization-specific legal notice to appear after an administrator successfully authenticates.

Which two actions should be configured? (Choose two.)

A. Add the approved public addresses to the IP Allow List.

B. Configure and enable the Privacy Notice.

C. Add the approved public addresses to a Network Location.

D. Configure a User Notification Template for the legal notice.

ANSWER: A B

Explanation:

Add the approved public source addresses to the IP Allow List. This restricts access to the Netskope administrative interface to requests originating from trusted IP addresses, adding a network-based control to privileged access.

Configure and enable the Privacy Notice to display the legal notice after authentication. The Privacy Notice is intended for organization-specific administrative, privacy, legal, or acceptable-use messaging. A Network Location is used for traffic and policy context, not to restrict Admin UI source access, while a user notification template is used for policy-related notifications rather than the post-authentication Admin UI notice.

QUESTION NO: 12

Your company started deploying the latest version of the Netskope Client and you want to track the progress and device count using Netskope.

Which two statements are correct in this scenario? (Choose two.)

A. Use Netskope Digital Experience Management to monitor the status.

B. Use the Devices page under Settings to view and filter the required data.

C. Review the Group definitions under Settings to determine the number of deployed clients.

D. Review the Steering Configuration to determine the number of deployed clients.

ANSWER: A B

Explanation:

Use Netskope Digital Experience Management to monitor the status. Netskope Digital Experience Management provides endpoint-focused visibility that helps administrators assess client health and connectivity experience during a rollout. This visibility is useful for monitoring whether endpoints are reporting normally and for identifying deployment-related experience issues that may need operational follow-up. DEM complements deployment management by providing ongoing telemetry from managed devices rather than relying only on endpoint-management tooling.

Use the Devices page under Settings to view and filter the required data. The Devices page is the appropriate Netskope-console inventory view for examining enrolled endpoints. Administrators can filter the device inventory and inspect client-related attributes, including installed client version information, to determine how broadly a target version has been deployed and which devices still require attention. Using the inventory filters also supports an accurate device count for the rollout population, allowing progress to be tracked directly in the tenant. Together, DEM status visibility and the device inventory provide both operational health context and version-based deployment progress tracking. See the Netskope Help documentation and Netskope's Digital Experience Management overview.

QUESTION NO: 13

A customer asks you to create several real-time policies. Policy A generates alerts when any user downloads, uploads, or shares files on a cloud storage application. Policy B blocks users from downloading files from any operating system (OS) other than Mac or Windows for cloud storage. In this case, policy A is least restrictive and policy B is more restrictive.

Which statement is correct in this scenario?

A. Policy A is implemented before policy B.

B. Policy B is implemented before policy A.

C. The policy order is not important; policies are independent of each other.

D. These two policies would actually not work together.

ANSWER: B

Explanation:

Policy B is implemented before policy A. Real-time protection policy order is significant because Netskope evaluates policies in their configured order. A policy with a restrictive enforcement action should be placed above a broader policy that matches the same activity. Here, the blocking policy targets downloads to cloud-storage applications when the device OS is not macOS or Windows. It must be evaluated first so that the download is stopped for the affected devices. The alerting policy is broader: it covers downloads, uploads, and sharing activity for all users on cloud-storage applications. Positioning that broad policy below the blocking rule preserves the intended enforcement priority while allowing it to provide visibility for relevant activity that is not handled by the higher-priority block rule. This ordering follows the general best practice of placing narrower, more restrictive real-time policies before broader, less restrictive monitoring policies. Administrators can manage and reorder real-time protection rules in the Netskope tenant's policy configuration. See the Netskope Documentation portal and Netskope's Cloud Security product documentation and resources for policy-management guidance.

QUESTION NO: 14

All users are going through Netskope ' s Next Gen SWG. Your CISO requests a monthly report of all users who are accessing cloud applications with a " Low " or a " Poor " CCL, where the activity is either " Edit " or " Upload " .

Using the Advanced Analytics interface, which two statements describe which actions must be performed in this scenario? (Choose two.)

A. Create a report using the Data Collection " Page Events " , filtering on the activities " Edit " and " Upload " for cloud apps with CCL values of " Low " or " Poor " .

B. Schedule a report with a monthly recurrence to be sent by e-mail with the attached PDF document at the end of each month.

C. Create a report using the Data Collection " Application Events " filtering on the activities " Edit " and " Upload " for cloud apps with CCL values of " Low " or " Poor " .

D. Schedule a report with a monthly recurrence to be sent by SMS with the attached PDF document at the end of each month.

ANSWER: B C

Explanation:

Creating a report using the Data Collection " Application Events " and filtering on the activities " Edit " and " Upload " for cloud apps with CCL values of " Low " or " Poor " is required because Application Events records user activity performed within discovered cloud applications. This data collection supplies the application-specific activity information needed to identify edits and uploads, along with cloud-application attributes such as Cloud Confidence Level. The report can therefore be scoped to the requested activity values and CCL ratings, while including user-related fields in the report output to identify the users for the CISO.

Scheduling a report with a monthly recurrence to be sent by e-mail with the attached PDF document at the end of each month is also required to meet the request for a recurring monthly deliverable. Advanced Analytics reports can be scheduled and distributed to designated recipients, allowing the report to be generated consistently without manual intervention. The report author should select the desired monthly schedule, configure the CISO as a recipient, and choose the appropriate attachment/output settings supported by the report schedule. Netskope's documentation describes Advanced Analytics reporting and the event data used for analytics at Netskope Advanced Analytics documentation and provides the documentation portal at Netskope Documentation.

QUESTION NO: 15

What are two CASB inline interception use cases? (Choose two.)

A. blocking file uploads to a personal Box account

B. running a retroactive scan for data at rest in Google Drive

C. using the Netskope steering client to provide user alerts when sensitive information is posted in Slack

D. scanning Dropbox for credit card information

ANSWER: A C

Explanation:

blocking file uploads to a personal Box account is an inline CASB use case because Netskope can proxy and inspect a user's cloud traffic in real time, identify the specific Box instance involved, and enforce a policy before an upload is completed. This allows organizations to prevent sensitive information from being transferred to unmanaged or personal cloud-storage accounts at the point of attempted exfiltration.

using the Netskope steering client to provide user alerts when sensitive information is posted in Slack is also an inline interception use case. The Netskope steering client directs applicable user traffic to the Netskope Security Cloud, where the inline CASB can inspect Slack activity as it occurs. Netskope DLP policies can detect sensitive data patterns and trigger a coaching or alert action immediately, helping users correct risky sharing behavior before or while the content is submitted. Inline controls are intended for real-time visibility and enforcement over sanctioned cloud-app activity, including granular actions based on application, app instance, user, content, and data classification. See Netskope's CASB overview and Data Loss Prevention overview.