PassQueen
a.k.a dumpsqueen.com

Netskope Certified Cloud Security Integrator (NCCSI)

Netskope NSK200

Version Demo

Total Demo Questions: 11

Total Premium Questions: 116

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Netskope Platform	44
Topic 2, Cloud Security	15
Topic 3, Web Security	16
Topic 4, Private Access	5
Topic 5, Data Protection	24
Topic 6, Threat Protection	12
Total	116

QUESTION NO: 1

You are testing policies using the DLP predefined identifier " Card Numbers (Major Networks; all). " No DLP policy hits are observed.

A. You must use Netskope API protection.

B. Your data must have valid credit card numbers.

C. You must normalize credit card numbers to 16-digit consecutive numbers.

D. You must use the Netskope client to perform advanced DLP and optical character recognition.

ANSWER: B

Explanation:

Your data must have valid credit card numbers. The Netskope predefined identifier named “Card Numbers (Major Networks; all)” is intended to identify payment-card account numbers for the supported major card networks, rather than merely any sequence of digits that resembles a card number. During a policy test, the sample value must satisfy the identifier’s validation requirements, including the expected characteristics of a genuine card number. In practice, this means using an appropriate test PAN for a supported network that passes the relevant checksum validation; a random 16-digit value is not a reliable test input. The data must also be present in the traffic or content channel being inspected by the policy and match the rule’s configured scope. When validating a DLP policy, use approved non-production payment-card test numbers and send the test through the same application, activity, and policy path that the rule covers. Netskope’s DLP documentation describes predefined identifiers as the content-detection building blocks used in DLP rules, while PCI guidance explains requirements for protecting payment-card data. See Netskope Documentation and the PCI DSS document library.

QUESTION NO: 2

A customer wants to use Netskope to prevent PCI data from leaving the corporate sanctioned OneDrive instance. In this scenario. which two solutions would assist in preventing data exfiltration? (Choose two.)

A. API Data Protection

B. Cloud Firewall (CFW)

C. SaaS Security Posture Management (SSPM)

D. Real-time Protection

ANSWER: A D

Explanation:

API Data Protection and Real-time Protection work together to protect PCI data in a sanctioned OneDrive environment. API Data Protection provides out-of-band inspection of content already stored in OneDrive through the Microsoft API integration. It can discover and classify sensitive files using PCI-oriented DLP rules, identify risky sharing states such as public links or external collaborators, and apply remediation actions. This is important because sensitive content may already exist in the tenant before a policy is deployed or may become exposed through later sharing changes.

Real-time Protection applies inline controls to user activity as it occurs. Netskope can inspect uploads, downloads, sharing-related activity, and other supported OneDrive transactions against DLP profiles that detect payment-card data. Policies can then enforce an appropriate protective action, such as blocking a transfer, alerting, or applying another configured response. Inline inspection prevents a user from moving detected PCI data outside the sanctioned OneDrive workflow at the point of attempted exfiltration, while API scanning continues to govern data at rest. Together, these controls provide coverage for both existing cloud content and data in motion. See the Netskope API Data Protection documentation and Netskope Real-time Protection documentation.

QUESTION NO: 3

You want to allow both the user identities and groups to be imported in the Netskope platform. Which two methods would satisfy this requirement? (Choose two.)

A. Use System for Cross-domain Identity Management (SCIM).

B. Use Manual Entries.

C. Use Directory Importer.

D. Use Bulk Upload with a CSV file.

ANSWER: A D

Explanation:

Use System for Cross-domain Identity Management (SCIM) and Use Bulk Upload with a CSV file. SCIM is a standards-based provisioning mechanism that enables an identity provider to create and maintain identity objects in Netskope through automated synchronization. When group provisioning is configured, the identity provider can send both user records and group membership information, allowing Netskope policies to use current user and group context. This is especially useful when lifecycle changes, such as onboarding, offboarding, or group-membership updates, should be reflected automatically.

Bulk Upload with a CSV file is also suitable when identities and group associations need to be loaded from a prepared data file. An administrator can supply the required user information and group data in the supported CSV structure, enabling Netskope to populate the identity and group context needed for policy enforcement. This approach is useful for an initial population or for environments where automated provisioning is not required. Netskope documents its identity and provisioning capabilities in the Netskope Documentation portal; the underlying SCIM provisioning model is defined by the SCIM Protocol specification.

QUESTION NO: 4

You have deployed an NPA Publisher and created a private application for an internal source-code repository. Users with the Netskope Client are still attempting direct connections to the repository, and no authorized users can establish private application access.

Which two configuration steps are needed to provide the intended access? (Choose two.)

A. Enable traffic steering for private applications.

B. Create a Real-time Protection policy that allows the intended users to access the private application.

C. Create an inbound Internet firewall rule that permits traffic to the Publisher.

D. Create an application instance for the source-code repository in Skope IT.

E. Configure an API Data Protection policy for the repository.

ANSWER: A B

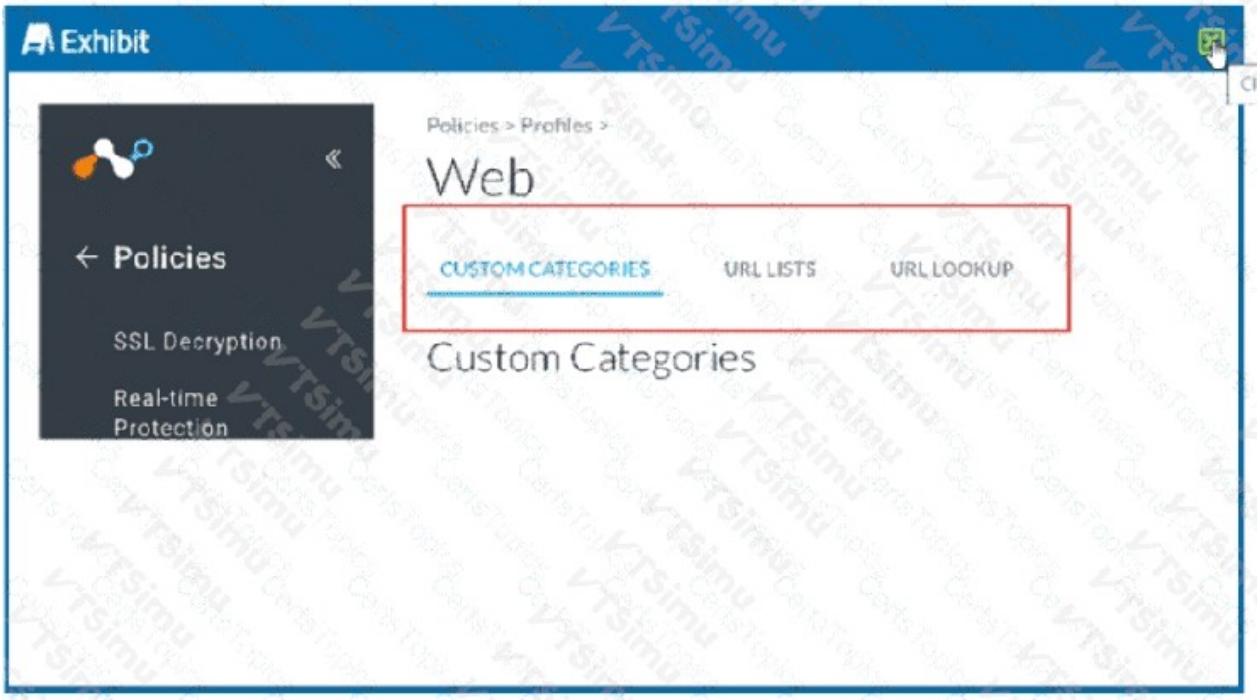
Explanation:

Traffic steering for private applications must be enabled so that the Client identifies and directs repository traffic to Netskope Private Access. A Real-time Protection policy must also authorize the intended users or groups to access the published private application.

An inbound Internet firewall rule is not required because the Publisher establishes outbound connectivity to Netskope. Application instances are used for cloud-application identification and do not grant access to an NPA private application.

QUESTION NO: 5

Review the exhibit.



You want to create a custom URL category to apply a secure Web gateway policy combining your own list of URLs and Netskope predefined categories.

In this scenario, which task must be completed?

A. Add the URL list to the Client configuration.

B. Add the URL list to a Custom category.

C. Add the URL list to a Steering configuration.

D. Add the URL list to a Real-time Protection policy.

ANSWER: B

Explanation:

Add the URL list to a Custom category. Netskope Custom Categories are designed to provide a single reusable URL-category object that can combine administrator-defined URL entries with Netskope's predefined URL categories. The custom category can contain URL lists and selected predefined categories, allowing the organization to express a broader business or security classification in one place. After the custom category is saved, it can be selected as the category match condition in a Web Real-time Protection policy, where the policy defines the enforcement action.

This approach also makes administration more consistent: updates to the organization's URL list or category composition are made in the Custom Category definition and are then reflected wherever that category is used. It supports the stated requirement to combine private URL intelligence with Netskope-maintained category coverage, rather than treating the URLs solely as a traffic-steering input. Netskope documents Custom Categories as the mechanism for creating organization-specific URL classifications for policy use. See the Netskope Documentation portal for the current administration guidance and the Netskope Next Gen Secure Web Gateway overview for the policy-enforcement context.

QUESTION NO: 6

A Netskope Client deployment is operating in an office where endpoints are prohibited from connecting directly to the Internet. The Client must establish its secure connection to a Netskope gateway through the organization's existing explicit proxy.

What must be configured to support this connectivity?

A. Set up an HTTP proxy server to tunnel the SSL connection to the Netskope gateway.

B. Install the proxy decryption certificate into every browser profile.

C. Configure a Do Not Decrypt policy for all Netskope gateway domains.

D. Create a GRE tunnel from each endpoint to the Netskope gateway.

ANSWER: A

Explanation:

An HTTP proxy must be available to tunnel the SSL connection to the Netskope gateway. In an explicit-proxy environment, the proxy provides the permitted egress path and can establish the required CONNECT tunnel for the Client's secure connection.

Installing a proxy-decryption certificate does not create the required tunnel path. A PAC file may direct browser traffic, but it is not the mechanism that enables the Client's gateway connection in this scenario.

QUESTION NO: 7

To which three event types does Netskope ' s REST API v2 provide access? (Choose three.)

A. application

B. alert

C. client

D. infrastructure

E. user

ANSWER: A B D

Explanation:

The correct event types are **application**, **alert**, and **infrastructure**. Netskope REST API v2 exposes event-query endpoints that enable an authorized integration to retrieve security telemetry generated by the Netskope platform. Application events provide visibility into activities involving cloud applications, including the application context and actions evaluated by Netskope. Alert events expose alert records created when activity matches policy or risk conditions, allowing external systems such as SIEM and SOAR platforms to collect, correlate, and act on Netskope detections. Infrastructure events provide telemetry related to infrastructure-related traffic and activity, extending the event data available for operational monitoring and investigation.

These event categories are specified as supported event types in the REST API v2 event retrieval path. An integration supplies the appropriate tenant URL, API token, event type, and query parameters such as time boundaries or pagination controls to collect the desired records. This REST interface is commonly used to export Netskope events for centralized monitoring, reporting, and incident-response workflows. See Netskope's REST API v2 overview and the REST API v2 Get Events documentation for the event API structure and supported event data.

QUESTION NO: 8

Your customer implements Netskope Secure Web Gateway to secure all Web traffic. While they have created policies to block certain categories, there are many new sites available dally that are not yet categorized. The customer ' s users need quick access and cannot wait to put in a request to gain access requiring a policy change or have the site ' s category changed.

To solve this problem, which Netskope feature would provide quick, safe access to these types of sites?

A. Netskope Cloud Firewall (CFW)

B. Netskope Remote Browser Isolation (RBI)

C. Netskope Continuous Security Assessment (CSA)

D. Netskope SaaS Security Posture Management (SSPM)

ANSWER: B

Explanation:

Netskope Remote Browser Isolation (RBI) provides a practical way to give users immediate access to newly discovered or uncategorized websites without waiting for URL categorization or a conventional allow-policy update. Rather than allowing the user's endpoint to interact directly with potentially unknown web content, RBI opens the site in an isolated remote browser session and safely renders the resulting content to the user. This approach reduces exposure to browser-based threats, malicious scripts, drive-by downloads, and risky active content that may be associated with sites whose reputation or category is not yet established.

In a Secure Web Gateway deployment, administrators can use an isolation action for traffic matching criteria such as uncategorized URLs, newly registered domains, or other risk-based web classifications. Users retain fast access to the information they need, while the organization maintains a security control appropriate for destinations that have not yet been fully assessed. Netskope documents RBI as a cloud-delivered isolation capability that separates web browsing activity from the endpoint and supports secure access to potentially risky web destinations. See the Netskope Browser Isolation documentation and Netskope's Remote Browser Isolation product overview.

QUESTION NO: 9

Review the exhibit.

You receive a service request from a user who indicates that their Netskope client is in a disabled state. The exhibit shows an excerpt (rom the affected client nsdebuglog.log.

What is the problem in this scenario?

A. User authentication failed during IdP-based enrollment.

B. The Netskope client connection is being decrypted.

C. Custom installation parameters are incorrectly specified

D. The user ' s account has not been provisioned into Netskope.

ANSWER: B

Explanation:

The Netskope client connection is being decrypted. The relevant nsdebuglog.log error, *"SSL certificate verification failed: self signed certificate in certificate chain,"* indicates that the client received a certificate chain that it cannot validate against its expected trusted certificate authorities. In this scenario, the usual cause is TLS/SSL inspection by an upstream security device, secure web gateway, firewall, or proxy. That device terminates the original TLS session, creates a replacement certificate for the requested Netskope service, and then re-encrypts the traffic. Unless the resulting certificate chain is trusted appropriately and the required Netskope traffic is excluded from inspection, the client cannot establish the secure connection it needs to retrieve configuration and maintain service connectivity. A client that cannot complete these communications can enter or remain in a disabled state. The appropriate remediation is to identify the decrypting network path and configure a no-decrypt/TLS-inspection bypass for the Netskope Client's required service endpoints, following the organization's Netskope deployment guidance. Netskope's client documentation and deployment resources describe client connectivity requirements and operational considerations: Netskope Client documentation and Netskope deployment resources.

QUESTION NO: 10

You are given an MD5 hash of a file suspected to be malware by your security incident response team. They ask you to offer insight into who has encountered this file and from where was the threat initiated. In which two Skope IT events tables would you search to find the answers to these questions? (Choose two.)

A. Application Events

B. Network Events

C. Alerts

D. Page Events

ANSWER: A C

Explanation:

Application Events is the appropriate Skope IT table for investigating user interaction with a file in cloud applications. Its event records include file and transaction context that can be filtered or pivoted on file attributes such as an MD5 hash. This enables the incident responder to identify the affected users, the relevant cloud application or instance, and the activity associated with the file, such as a download or upload. That activity context helps establish where the suspicious file entered or was encountered within sanctioned cloud traffic.

Alerts provides the security-policy and detection context for the same investigation. Alert records capture events generated by Netskope security controls, including threat protection detections and their enforcement outcome. Searching alerts using the file hash can show whether Netskope identified the file as malicious or suspicious, which user and activity were associated with the detection, and the action applied by policy. Correlating the application activity with the alert supplies both the user-facing event trail and the threat-detection trail needed for incident response. See Netskope's Skope IT documentation and malware protection documentation for the event-investigation and threat-context workflow.

QUESTION NO: 11

You want the ability to perform automated remediation of misconfigurations on GitHub, Microsoft 365, Salesforce, ServiceNow, and Zoom.

A. Netskope Infrastructure as a Service

B. Netskope Remote Browser Isolation

C. Netskope Cloud Firewall

D. Netskope SaaS Security Posture Management

ANSWER: D

Explanation:

Netskope SaaS Security Posture Management is the appropriate solution because it continuously assesses SaaS configurations against security best practices and enables remediation workflows for configuration issues. Its purpose is to provide centralized visibility into the security posture of connected SaaS tenants, identify risky settings, and help security teams reduce exposure caused by misconfigurations. For supported applications such as GitHub, Microsoft 365, Salesforce, ServiceNow, and Zoom, SSPM uses API-based integrations to evaluate configuration settings and detect deviations from recommended controls. Where remediation is supported, administrators can use remediation actions and workflows to correct settings efficiently rather than relying solely on manual reviews across separate application consoles. This makes SSPM particularly suitable when the requirement is consistent, scalable posture management across a portfolio of business-critical SaaS services. Netskope describes SSPM as providing continuous monitoring, assessment, and remediation of SaaS security posture, while its documentation lists supported SaaS applications and integration capabilities. See the Netskope SSPM overview and the Netskope SSPM documentation for product capabilities and supported-app guidance.