Netskope NSK200 NCCSI Practice Questions

Shared by Guthrie on 03-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Your organization has a homegrown cloud application. You are required to monitor the activities that users perform on this cloud application such as logins, views, and downloaded files. Unfortunately, it seems Netskope is unable to detect these activities by default.

How would you accomplish this goal?

Options:

A- Enable access to the application with Netskope Private Access.
B- Ensure that the cloud application is added as a steering exception.
C- Ensure that the application is added to the SSL decryption policy.
D- Create a new cloud application definition using the Chrome extension.

Answer:

D

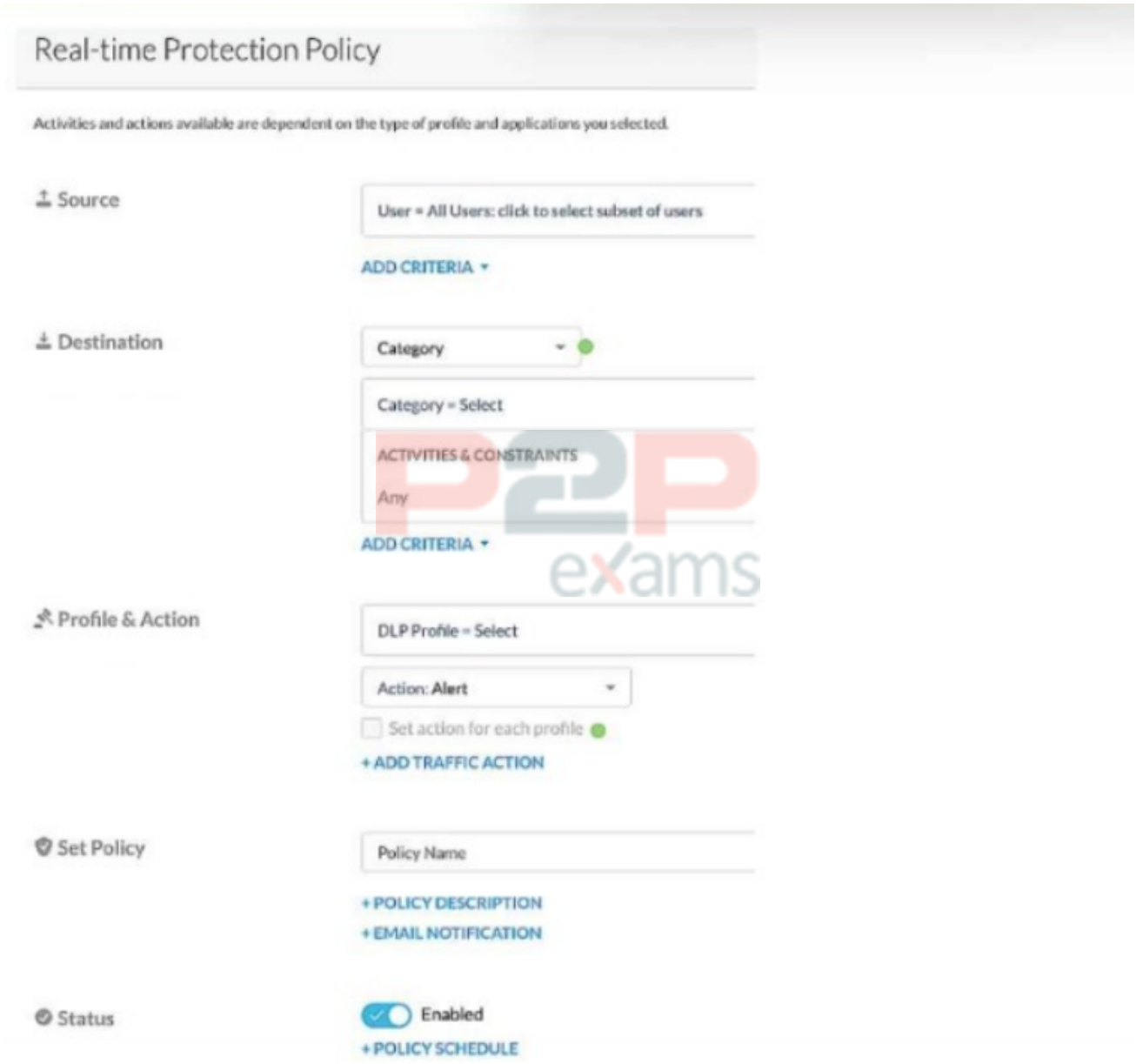
Explanation:

To monitor the activities that users perform on a homegrown cloud application, you need to create a new cloud application definition using the Chrome extension.The Chrome extension is a tool that allows you to record the traffic and activities of any web-based application and create a custom app definition that can be imported into your Netskope tenant1. This way, you can enable Netskope to detect and analyze the activities of your homegrown cloud application and apply policies accordingly. Therefore, option D is correct and the other options are incorrect.Reference:Creating a Cloud App Definition - Netskope Knowledge Portal

Question 2

Question Type: MultipleChoice

Review the exhibit.



Given the information shown below:

- for PCI data uploads, you want to provide no notification,

- for PHI data uploads, you want to allow users to proceed by clicking OK,

- for GDPR data uploads, you want to provide block notification,

- if none of the above matches, you want to provide no notification.

You want to reduce the number of policies by combining multiple DLP profiles Into one policy.

Referring to the exhibit, which two statements are true? (Select two.)

Options:

A- You must open a support ticket to enable the Advanced Policies feature.
B- You must check the 'set action for each profile' flag.

C- You can have only one action if you use multiple DLP profiles in the same policy.
D- You can apply a unique action to each profile In the same policy.

Answer:

B, D

Question 3

Question Type: MultipleChoice

Review the exhibit.

add log-upload syslogng parserconfig set log-upload syslogng parserconfig 0

logsource

You are asked to deploy a virtual appliance OPLP to accept syslog messages directly from the enterprise Palo Alto Networks firewall. You believe that you have configured the OPLP to accept the firewall logs, yet they are not appearing in Risk Insights. Referring to the exhibit, which parser name would be required to complete the new configuration?

Options:

A- panw-syslog
B- sfwder
C- custom-csv
D- squid

Answer:

A

Explanation:

The correct parser name to process syslog messages from Palo Alto Networks firewalls is 'panw-syslog.' Using the appropriate parser ensures that the logs are correctly interpreted and ingested by Netskope, making them available in Risk Insights.

Question 4

Question Type: MultipleChoice

While most Web and SaaS traffic is decrypted for inspection, you are asked to prevent a certain host on the network from SSL decryption for privacy purposes.

Options:

A- Create a steering exception for the host.
B- Create a Real-time Protection policy, select the host, and choose to block SSL decryption.
C- Create a Source Network Location for a Do Not Decrypt SSL policy.
D- Add the host to the certificate-pinned application list.

Answer:

A

Explanation:

Creating a steering exception for the host is the appropriate action to prevent SSL decryption on specific network traffic. Steering exceptions allow you to bypass decryption for designated hosts, which is useful for privacy-sensitive scenarios.

Question 5

Question Type: MultipleChoice

Your company has Microsoft Azure ADFS set up as the Identity Provider (idP). You need to deploy the Netskope client to all company users on Windows laptops without user intervention.

In this scenario, which two deployment options would you use? (Choose two.)

Options:

A- Deploy the Netskope client with SCCM.
B- Deploy the Netskope client with Microsoft GPO.
C- Deploy the Netskope client using IdP.
D- Deploy the Netskope client using an email Invitation.

Answer:

A, B

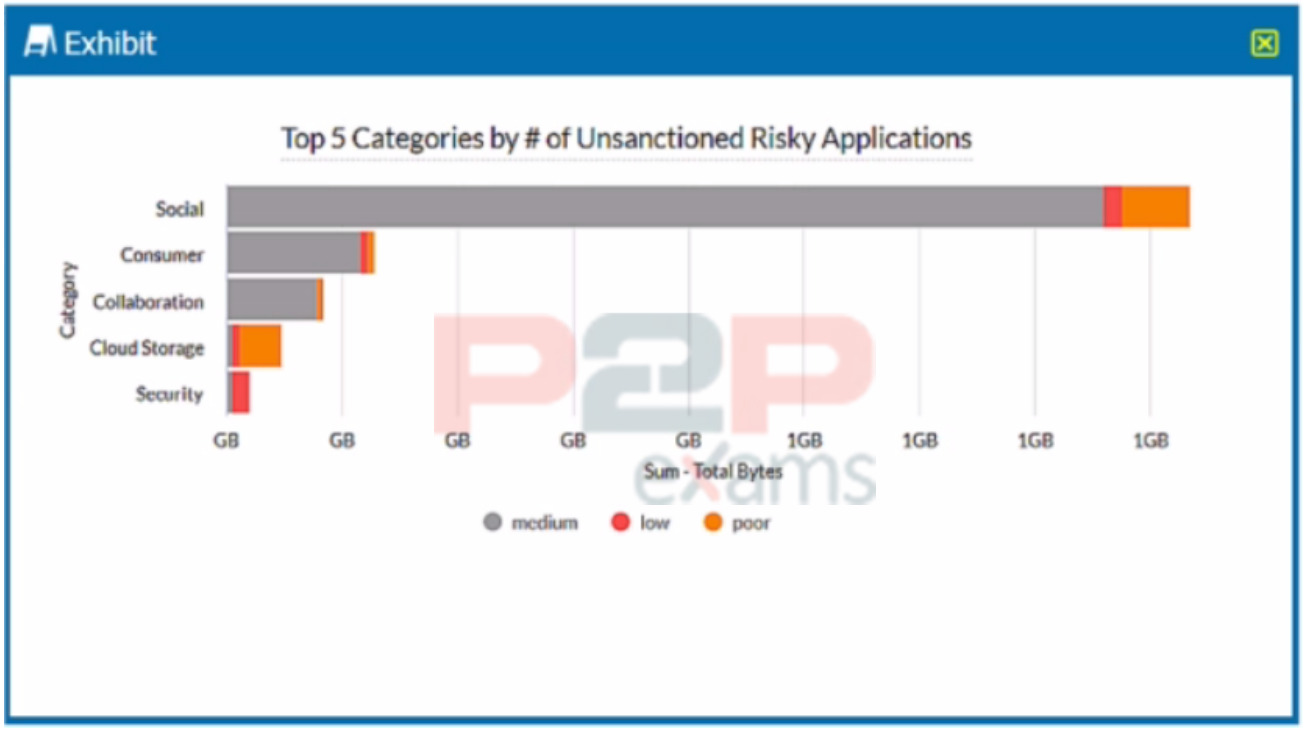
Explanation:

To deploy the Netskope client to all company users on Windows laptops without user intervention, you can use either SCCM or GPO.These are two methods of packaging the application and pushing it silently to the user's device using Microsoft tools4. These methods do not require the user to have local admin privileges or to initiate the installation themselves. They also allow enforcing the use of the client through company policy.The Netskope client can authenticate the user using Azure ADFS as the identity provider, as long as the UPN of the logged in user matches the directory5

Question 6

Question Type: MultipleChoice

Review the exhibit.



A security analyst needs to create a report to view the top five categories of unsanctioned applications accessed in the last 90 days. Referring to the exhibit, what are two data collections in Advanced Analytics that would be used to create this report? (Choose two.)

Options:

A- Alerts
B- Application Events
C- Page Events
D- Network Events

Answer:

B, D

Explanation:

To create a report to view the top five categories of unsanctioned applications accessed in the last 90 days, the security analyst would need to use two data collections in Advanced Analytics: Application Events and Network Events. Application Events provide information about the cloud applications and websites accessed by users, such as app name, app category, app risk score, app instance, app version, and more. Network Events provide information about the network traffic generated by users, such as source IP, destination IP, protocol, port, bytes sent, bytes received, and more. By combining these two data collections, the security analyst can filter the events by app category, app risk score, and time range to create a report that shows the top five categories of unsanctioned applications accessed in the last 90 days. Alerts and Page Events are not relevant for this report. Alerts provide information about the alerts triggered by Real-time Protection or API Data Protection policies, such as alert type, alert severity, alert status, alert description, and more.Page Events provide information about the web pages visited by users, such as page title, page URL, page category, page risk score, page content type, and more.Reference:Advanced Analytics

Question 7

Question Type: MultipleChoice

Your customer is migrating all of their applications over to Microsoft 365 and Azure. They have good practices and policies in place (or their inline traffic, but they want to continuously detect reconfigurations and enforce compliance standards.

Which two solutions would satisfy their requirements? (Choose two.)

Options:

A- Netskope SaaS Security Posture Management
B- Netskope Cloud Confidence Index
C- Netskope Risk Insights

D- Netskope Continuous Security Assessment

Answer:

A, D

Explanation:

To continuously detect and enforce compliance standards for their Microsoft 365 and Azure applications, the customer needs to use Netskope SaaS Security Posture Management (SSPM) and Netskope Continuous Security Assessment (CSA). Netskope SSPM allows the customer to monitor, assess, and act on security, permission, and access related issues in their SaaS environment, such as Microsoft 365. Netskope SSPM continuously checks security posture by comparing SaaS app settings with security policies and industry benchmarks (CIS, PCI-DSS, NIST, HIPAA, CSA, GDPR, AIPCA, ISO, and more).It also provides visibility and control over third-party apps that are connected to the managed apps1. Netskope CSA allows the customer to discover, audit, and remediate misconfigurations in their IaaS environment, such as Azure. Netskope CSA continuously monitors and audits cloud configurations against industry standards, CIS benchmarks, and regulatory frameworks.It also provides real-time inline protection to secure public clouds from threats and data loss2. Therefore, options A and D are correct and the other options are incorrect.Reference:SaaS Security Posture Management - Netskope,Public Cloud Security Solutions - Netskope

Question 8

Question Type: MultipleChoice

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.)

Options:

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:

To allow both the user identities and groups to be imported in the Netskope platform, you can use either the System for Cross-domain Identity Management (SCIM) method or the Bulk Upload with a CSV file method. Both of these methods allow for the import of user identities and groups from different identity providers (IdPs) that support SCIM or CSV formats. The SCIM method is recommended for large-scale deployments, as it automates the exchange of user identity information across apps for user provisioning. The CSV method is recommended for small-scale deployments, as it allows for manual upload of user details in a comma-separated values file. The other methods are not suitable for this requirement. The Manual Entries method does not allow for the import of groups, only user emails. The Directory Importer method does not import users and groups directly into the Netskope platform, but rather connects to an Active Directory or LDAP server and periodically fetches user and group information.

P2P exams

Question 9

Question Type: MultipleChoice

Your company asks you to use Netskope to integrate with Endpoint Detection and Response (EDR) vendors such as CrowdStrike. In this scenario, what is a requirement for a successful Integration and sharing of threat data?

Options:

A- API Client ID
B- device classification
C- custom log parser
D- user endpoint

P2P exams

Answer:

A

Explanation:

To integrate Netskope with EDR vendors such as CrowdStrike and share threat data, a requirement for a successful integration is A. API Client ID. An API Client ID is a unique identifier that is used to authenticate and authorize requests to the EDR vendor's API. You need to obtain an API Client ID from the EDR vendor and enter it in the Netskope tenant settings under Threat Protection > Integration.This will allow Netskope to communicate with the EDR vendor and exchange threat intelligence and remediation actions1. Therefore, option A is correct and the other options are incorrect.Reference:Integrating CrowdStrike for EDR -

Netskope Knowledge Portal

Question 10

Question Type: MultipleChoice

Review the exhibit.



While diagnosing an NPA connectivity issue, you notice an error message in the Netskope client logs.

Referring to the exhibit, what does this error represent?

Options:

A- The Netskope client has been load-balanced to a different data center.
B- The primary publisher is unavailable or cannot be reached.
C- There Is an EDNS or LDNS resolution error.
D- There Is an upstream device trying to intercept the NPA TLS connection.

Answer:

D

Explanation:

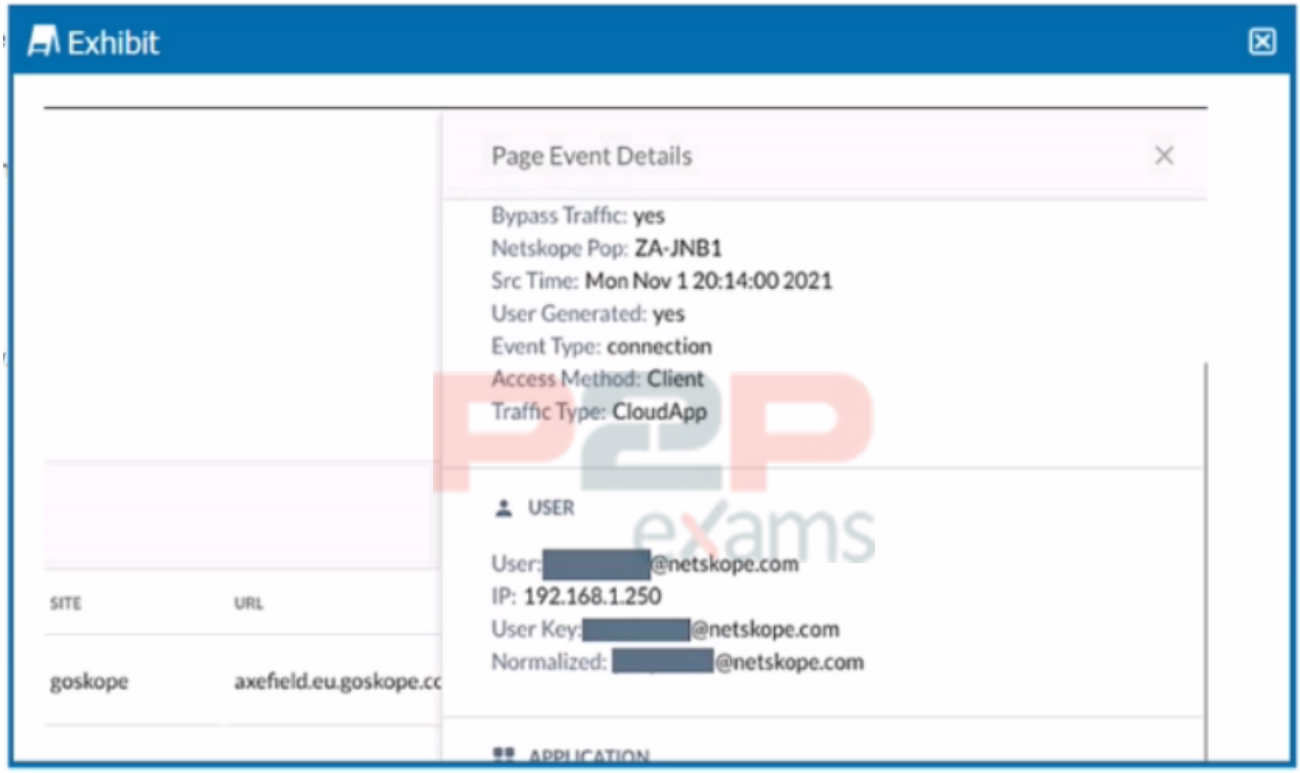
The error message in the exhibit represents that there is an upstream device trying to intercept the NPA TLS connection. The error message is ''ERROR SSL certificate verification failed: self signed certificate in certificate chain''. This means that the Netskope client is receiving a certificate that is not issued by Netskope, but by a device that is intercepting and decrypting the traffic between the client and the Netskope cloud.This can cause the client to fail to establish a secure connection to the NPA service and access the private applications4.To solve this problem, you need to either bypass or trust the upstream device that is performing SSL decryption, such as a firewall or proxy5. Therefore, option D is correct and the other options are incorrect.Reference:Troubleshooting Netskope Client - Netskope Knowledge Portal,Netskope Client Troubleshooting Guide - The Netskope Community

P2P exams

Question 11

Question Type: MultipleChoice

Review the exhibit.



You are asked to restrict users from accessing YouTube content tagged as Sport. You created the required real-time policy; however, users can still access the content

Referring to the exhibit, What is the problem?

Options:

A- The website is in a steering policy exception.
B- The policy changes have not been applied.
C- The YouTube content cannot be controlled.
D- The traffic matched a Do Not Decrypt policy

Answer:

D

Explanation:

The problem in this scenario is that the traffic matched a Do Not Decrypt policy.A Do Not Decrypt policy is a rule that specifies the traffic that you want to leave encrypted and not further analyzed by Netskope via the Real-time Protection policies1. In the exhibit, we can see that the traffic from the user to YouTube has a ''Bypass Traffic'' value of ''yes'' and a ''Netskope'' value of ''yes''.This means that the traffic was steered to Netskope but not decrypted or inspected2. Therefore, the real-time policy that was created to restrict users from accessing YouTube content tagged as Sport did not apply, and users could still access the content.To solve this problem, you need to either remove or modify the Do Not Decrypt policy that matches the traffic to YouTube, or create an exception for the Sport category in the policy3. Therefore, option D is correct and the other options are incorrect.Reference:Page Events - Netskope Knowledge Portal,Add a Policy for SSL Decryption - Netskope Knowledge Portal,YouTube Content Control - Netskope Knowledge Portal

To Get Premium Files for NSK200 Visit

https://www.p2pexams.com/products/nsk200

For More Free Questions Visit

https://www.p2pexams.com/netskope/pdf/nsk200

