Free Questions for NSK101 by certsdeals

Shared by Bennett on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company user cannot open a sports news site. You want to review the category of the website and see how the rules are applied even though this category is allowed. In this scenario, which action will accomplish this task?

Options:

A- Use the Forensic profile

B- Use www.netskope.com/url-lookup.

C- Use the URL Lookup page in the dashboard.

D- Verify with your own computer and use Advanced Debugging.

Answer:

C

Explanation:

To review the category of a website and understand how the rules are applied, the following action can be taken:

Use the URL Lookup page in the dashboard: The URL Lookup page in the Netskope dashboard allows administrators to enter a URL and view its categorization. This tool provides information on how the website is classified and which policies apply to it. It helps in troubleshooting why a user might be unable to access a specific site, even if the category is generally allowed.

Netskope documentation on using the URL Lookup tool to review website categories and policy applications.

Guidelines for troubleshooting web access issues using the Netskope dashboard tools.

Question 2

Question Type: **MultipleChoice**

An administrator wants to determine to which data plane a user is traversing. In this scenario, what are two ways to accomplish this task? (Choose two.)

Options:

A- Settings -> Security Cloud Platform -> Devices

B- Settings -> Security Cloud Platform -> Client Configuration

C- SkopeIT -> Alerts -> View Details

D- System Tray -> Configuration

Answer:

B, C

Explanation:

To determine which data plane a user is traversing, an administrator can use the following methods:

Settings -> Security Cloud Platform -> Client Configuration: This section provides details about the client configurations and the data planes assigned to different users or groups. By reviewing the client configuration, administrators can determine the data plane a user is connected to.

SkopeIT -> Alerts -> View Details: In the SkopeIT alerts, administrators can view detailed information about user activities, including the data plane through which the user traffic is being routed. This provides real-time insights into the user's path through the Netskope infrastructure.

Netskope documentation on configuring and managing the Security Cloud Platform and client configurations.

Guides on using SkopeIT to monitor user activities and view detailed alert information.

Question 3

Question Type: MultipleChoice

What are two valid use cases for the Cloud Confidence Index (CCI)? (Choose two.)

Options:

A- To recategorize cloud applications in the database

B- To delete cloud applications from the database

C- To identify the activities that Netskope supports for cloud applications

D- To compare similar cloud applications

Answer:

C, D

Explanation:

The Cloud Confidence Index (CCI) has several use cases, including:

To identify the activities that Netskope supports for cloud applications: The CCI helps administrators understand which activities are supported and monitored by Netskope for various cloud applications. This includes knowing the types of data that can be protected and the actions that can be controlled within those applications.

To compare similar cloud applications: The CCI provides a comparative assessment of cloud applications based on their security and compliance postures. This allows organizations to make informed decisions about which applications to approve or restrict based on their confidence levels.

These use cases help organizations enhance their security posture by using the CCI to guide application usage policies and ensure compliance with internal standards.

Netskope documentation on Cloud Confidence Index and its applications in policy creation and management.

Guides on using CCI to assess and compare cloud applications for better security and compliance.

Question 4

Question Type: **MultipleChoice**

You are required to provide an additional pop-up warning to users before allowing them to proceed to Web applications categorized as "low" or "poor" by Netskope's Cloud Confidence Index. Which action would allow you to accomplish this task?

Options:

A- Enable RBI on the uncategorized domains

B- Create a policy limiting usage of generative AI.

C- Redirect the user to the company banner page for the Web usage policy.

D- Enable real-time user coaching based on CCL.

Answer:

D

Explanation:

To provide an additional pop-up warning to users before allowing them to proceed to web applications categorized as 'low' or 'poor' by Netskope's Cloud Confidence Index (CCI), you can:

Enable real-time user coaching based on CCL: This feature allows administrators to create policies that provide real-time guidance and warnings to users when they attempt to access web applications with low or poor confidence levels. This helps in educating users about the potential risks and ensures that they proceed with caution.

Netskope documentation on configuring real-time user coaching and leveraging the Cloud Confidence Index for policy enforcement.

Best practices for using CCL to guide user behavior and enhance security awareness.

Question 5

Question Type: MultipleChoice

Which three status indicators does the NPA Troubleshooter Tool provide when run? (Choose three)

Options:

A- Steering configuration

B- Client configuration timestamp

C- Publisher connectivity

D- Client version

E- Reachability of the private app

Answer:

A, C, E

Explanation:

The NPA (Netskope Private Access) Troubleshooter Tool provides the following status indicators when run:

Steering configuration: This indicates whether the traffic is being correctly steered through the Netskope infrastructure according to the defined policies.

Publisher connectivity: This status shows whether the Netskope Publisher is correctly connected and able to communicate with the Netskope cloud. It ensures that the Publisher, which acts as a gateway, is functioning correctly.

Reachability of the private app: This status verifies if the private application is reachable from the Netskope infrastructure, ensuring that users can access the necessary internal resources.

These indicators help administrators troubleshoot and ensure that the NPA setup is working correctly, providing secure and reliable access to private applications.

Netskope documentation on using the NPA Troubleshooter Tool and the status indicators it provides.

Best practices for troubleshooting NPA connectivity and performance issues.

Question 6

Question Type: **MultipleChoice**

When designing an architecture with Netskope Private Access, which element guarantees connectivity between the Netskope cloud and the private application?

Options:

A- Netskope Publisher

B- API connector

C- Third-party router with GRE/IPsec support

D- Netskope Client

Answer:

A

Explanation:

When designing an architecture with Netskope Private Access, the Netskope Publisher is the element that guarantees connectivity between the Netskope cloud and the private application. The Publisher acts as a gateway, securely connecting users to private applications hosted on-premises or in data centers.

Netskope Publisher: This component facilitates secure access to private applications by connecting the Netskope cloud with the internal network. It ensures that users can access private applications seamlessly while maintaining security and compliance.

Netskope documentation on Private Access and the role of the Publisher.

Best practices for configuring and deploying Netskope Publisher to ensure secure connectivity to private applications.

Question 7

Question Type: MultipleChoice

API-enabled Protection traffic is sent to which Netskope component?

Options:

A- Netskope Publisher

B- Netskope Management Plane

C- Netskope Data Plane

D- Netskope Reverse Proxy

Answer:

C

Explanation:

API-enabled Protection traffic is sent to the Netskope Data Plane. The Netskope Data Plane is responsible for processing and inspecting data in real-time, applying security policies, and ensuring that the traffic conforms to organizational policies.

Netskope Data Plane: This component handles the inline inspection and enforcement of security policies, including API-enabled protection. It ensures that all traffic is securely processed and monitored according to the defined policies.

Netskope architecture documentation describing the roles of different components.

Detailed guides on how API-enabled protection integrates with the Netskope Data Plane for real-time traffic inspection.