Free Questions for NSK101

Shared by Bonner on 16-04-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What are two primary advantages of Netskope's Secure Access Service Edge (SASE) architecture? (Choose two.

Options:

A- no on-premises hardware required for policy enforcement
B- Bayesian spam filtering
C- Endpoint Detection and Response (EDR)
D- single management console

Answer:

A, D

Explanation:

Two primary advantages of Netskope's Secure Access Service Edge (SASE) architecture are: no on-premises hardware required for policy enforcement and single management console. Netskope's SASE architecture delivers network and security services as cloud-based services that can be accessed from any location and device. This eliminates the need for on-premises hardware appliances such as firewalls, proxies, VPNs, etc., that are costly to maintain and scale. Netskope's SASE architecture also provides a single management console that allows administrators to configure and monitor all the network and security services from one place. This simplifies IT operations and reduces complexity and overhead.Reference:Netskope SASEWhat is SASE?

Question 2

Question Type: MultipleChoice

Which three status indicators does the NPA Troubleshooter Tool provide when run? (Select 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 3

Question Type: MultipleChoice

Click the Exhibit button.

Referring to the exhibit, which statement accurately describes the difference between Source IP (Egress) and Source IP (User) address?

Options:

A- Source IP (Egress) is the IP address of the destination Web server while Source IP (User) is the IP address assigned to your network.
B- Source IP (Egress) is the IP address assigned to the endpoint host IP address while Source IP (User) is the public IP address of your Internet edge router.
C- You must always leave the source IP fields blank and configure the user identity as a source criteria.
D- Source IP (Egress) is the public IP address of your Internet edge router while Source IP (User) is the address assigned to the endpoint.

Answer:

D

Explanation:

The statement that accurately describes the difference between Source IP (Egress) and Source IP (User) address is: Source IP (Egress) is the public IP address of your Internet edge router while Source IP (User) is the address assigned to the endpoint. Source IP (Egress) is the IP address that is visible to external networks when you send traffic from your network to the Internet. It is usually the IP address of your Internet edge router or gateway that performs NAT (Network Address Translation). Source IP (User) is the IP address that is assigned to your endpoint device, such as a laptop or a smartphone, within your network. It is usually a private IP address that is not routable on the Internet. You can use these two criteria to filter traffic based on where it originates from within your network or outside your network.Reference:Source Address / Source Port vs Destination Address / Destination PortHow to explain Source IP Address, Destination IP Address & Service in easy way

Question 4

Question Type: MultipleChoice

When comparing data in motion with data at rest, which statement is correct?

Options:

A- Data at rest cannot be scanned for malware until a user opens the file.
B- Data in motion requires API integration.
C- Data in motion requires the Netskope client.
D- Data at rest requires API integration.

Answer:

C, D

Explanation:

When comparing data in motion with data at rest, the following statements are correct:

Data in motion requires the Netskope client: To inspect and enforce policies on data as it is being transmitted across the network (data in motion), the Netskope client is required. The client steers the traffic through the Netskope cloud where it is analyzed and policies are applied in real-time.

Data at rest requires API integration: To scan and enforce policies on data stored in cloud applications (data at rest), API integration is required. This allows Netskope to directly interact with cloud services and perform actions such as scanning for malware, applying DLP policies, and ensuring compliance.

Netskope documentation on data protection strategies, including data in motion and data at rest.

Best practices for implementing API integrations for data at rest and using the Netskope client for data in motion.

Question 5

Question Type: MultipleChoice

You need to locate events for specific activities such as "edit" or "login successful" in a cloud application.

In which SkopeIT Events & Alerts page would this information be found?

Options:

A- Endpoint Events
B- Page Events
C- Application Events
D- Websites

Answer:

C

Explanation:

The Application Events page in the SkopeIT Events & Alerts section is where you can find logs and events related to specific activities within cloud applications, such as 'edit' or 'login successful'. This section provides a detailed audit trail of user activities and application usage, which is essential for monitoring, security, and compliance purposes.

This answer is validated by the event categorization provided in the Netskope documentation, where application-specific events are logged under the Application Events section for easier tracking and analysis.

========

REST API v2 Overview - Netskope Knowledge Portal

Using the REST API v2 UCI Impact Endpoints - Netskope Knowledge Portal

Postman Collection for Netskope API

Question 6

Question Type: MultipleChoice

Your company asks you to obtain a detailed list of all events from the last 24 hours for a specific user. In this scenario, what are two methods to accomplish this task? (Select two.)

Options:

A- Use the Netskope reporting engine.
B- Export the data from Skope IT Application Events.
C- Use the Netskope REST API.
D- Export the data from Skope IT Alerts.

Answer:

B, C

Explanation:

In this scenario, there are two methods to obtain a detailed list of all events from the last 24 hours for a specific user. One method is to export the data from Skope IT Application Events, which is a feature in the Netskope platform that allows you to view and analyze all the activities

performed by users on cloud applications. You can use filters to narrow down your search by user name, time range, application, activity, and other criteria. You can then export the data to a CSV or JSON file for further analysis or reporting. Another method is to use the Netskope REST API, which is a programmatic interface that allows you to access and manipulate data from the Netskope platform using HTTP requests. You can use the API to query for events by user name, time range, application, activity, and other parameters. You can then retrieve the data in JSON format for further analysis or integration with other tools. Using the Netskope reporting engine or exporting the data from Skope IT Alerts are not methods to obtain a detailed list of all events from the last 24 hours for a specific user, as they are more suited for generating summary reports or alerts based on predefined criteria or thresholds, rather than granular event data.Reference:[Netskope Skope IT Application Events], [Netskope REST API].

Question 7

Question Type: MultipleChoice

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.)

Options:

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:

To track the progress and device count of the latest Netskope Client deployment, you can use the following methods:

Use Netskope Digital Experience Management to monitor the status:

Netskope Digital Experience Management (DEM) provides visibility into the performance and status of applications and devices. You can use this tool to monitor the deployment status and ensure that the new client version is being deployed correctly across the organization.

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

The Devices page in the Netskope console provides detailed information about all devices managed by Netskope. You can filter this data to view the specific deployment status of the latest Netskope Client version, helping you track the progress and identify any issues.

Netskope Knowledge Portal: Digital Experience Management

Netskope Knowledge Portal: Devices Page

Question 8

Question Type: MultipleChoice

As an administrator, you need to configure the Netskope Admin UI to be accessible by specific IP addresses and to display a custom message after the admin users have been authenticated.

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

Options:

A- Add the specific IP addresses on the IP Allow List.
B- Configure and enable the Privacy Notice to display the custom message.
C- Add the specific IP addresses on the Network Location.
D- Enable and set the User Notification Template to display the custom message.

Answer:

A, D

Explanation:

Add the specific IP addresses on the IP Allow List (A): To restrict access to the Netskope Admin UI to specific IP addresses, administrators need to add these IP addresses to the IP Allow List. This ensures that only connections from these specified IP addresses are allowed access to the Admin UI. This configuration is crucial for enhancing security by limiting access to trusted IP addresses only.

Enable and set the User Notification Template to display the custom message (D): To display a custom message to admin users after they have authenticated, administrators need to enable and configure the User Notification Template. This template allows the customization of messages that are shown to users, including after login. This feature is useful for displaying

privacy notices, welcome messages, or other important information to users upon successful authentication.

These steps are verified based on the configuration options available within the Netskope Admin UI settings. For more detailed steps and configuration, you can refer to the respective sections in the Netskope documentation.

Question 9

Question Type: MultipleChoice

What are two uses for deploying a Netskope Virtual Appliance? (Choose two.)

Options:

A- to use as a log parser to discover in-use cloud applications
B- to use as a local reverse proxy to secure a SaaS application
C- to use as an endpoint for Netskope Private Access (NPA)
D- to use as a secure way to generate Exact Data Match hashes

Answer:

A, C

Explanation:

Deploying a Netskope Virtual Appliance (NPA) can serve multiple purposes within an organization's security infrastructure. Two key uses are:

To use as a log parser to discover in-use cloud applications:

The Netskope Virtual Appliance can be deployed to parse logs from various sources, including firewalls, proxies, and other network devices. By analyzing these logs, the appliance can discover and identify cloud applications that are being used within the network. This provides visibility into shadow IT and helps in managing and securing cloud application usage.

To use as an endpoint for Netskope Private Access (NPA):

The virtual appliance can act as an endpoint for Netskope Private Access, enabling secure access to private applications hosted in data centers or public clouds. It facilitates the establishment of secure, direct connections between users and the applications they need to access, without exposing the applications to the public internet.

Netskope Knowledge Portal: Deploying Virtual Appliances

Netskope Private Access Overview