

Netskope Certified Security Associate (NSK101)

1. You investigate a suspected malware incident and confirm that it was a false alarm.

A. In this scenario, how would you prevent the same file from triggering another incident?

B. Quarantine the file. Look up the hash at the VirusTotal website.

C. Export the packet capture to a pcap file.

D. Add the hash to the file filter.

Answer(s): D

2. 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(s): B C

3. You have applied a DLP Profile to block all Personally Identifiable Information data uploads to Microsoft 365 OneDrive. DLP Alerts are not displayed and no OneDrive-related activities are displayed in the Skope IT App Events table.

In this scenario, what are two possible reasons for this issue? (Choose two.)

- A. The Cloud Storage category is in the Steering Configuration as an exception.
- B. The destination domain is excluded from decryption in the decryption policy.
- C. A Netskope POP is not in your local country and therefore DLP policies cannot be applied.
- D. DLP policies do not apply when using IPsec as a steering option.

Answer(s): A B

4. A customer changes CCI scoring from the default objective score to another score. In this scenario, what would be a valid reason for making this change?

- A. The customer has discovered a new SaaS application that is not yet rated in the CCI database.
- B. The customer's organization places a higher business risk weight on vendors that claim ownership of their data.
- C. The customer wants to punish an application vendor for providing poor customer service.
- D. The customer's organization uses a SaaS application that is currently listed as "under research".

Answer(s): B

5. What are two use cases for Netskope's DLP solution? (Choose two.)

- A. to stop unintentional data movement
- B. to detect malware in files before they are uploaded to a cloud application
- C. to detect sensitive data in password protected files
- D. to ensure regulatory compliance

Answer(s): A D

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

A. as an endpoint for Netskope Private Access (NPA)

B. as a local reverse-proxy to secure a SaaS application

C. as a log parser to discover in-use cloud applications

D. as a Secure Forwarder to steer traffic

Answer(s): A D

7. You are working with a large retail chain and have concerns about their customer data

A. 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?

B. SOC 3

C. PCI-DSS

D. AES-256

E. ISO 27001

Answer(s): B

8. You need to block all users from uploading data files into risky collaboration applications. Which element must you configure within Netskope's CASB to accomplish this task?

A. DLP Rule

B. real-time policy

C. DLP Profile

D. block notification

Answer(s): B

9. Which three security controls are offered by the Netskope Cloud platform? (Choose three.)

A. identity lifecycle management

B. data loss prevention for SMTP

C. cloud security posture management

D. endpoint anti-malware

E. threat protection

Answer(s): B C E

10. You want to use an out-of-band API connection into your sanctioned Microsoft 365 OneDrive for Business application to find sensitive content, enforce near real-time policy controls, and quarantine malware.

In this scenario, which primary function in the Netskope platform would you use to connect your application to Netskope?

A. DLP forensics

B. Risk Insights

C. IaaS API-enabled Protection

D. SaaS API-enabled Protection

Answer(s): D

11. You need to create a service request ticket for a client-related issue using the Netskope client UI. In this scenario, you generate the client logs by right-clicking on the system tray icon and choosing.

A. Save logs

B. Configuration

C. Troubleshoot

D. Help

Answer(s): C

12. What are two characteristics of Netskope's Private Access Solution? (Choose two.)

A. It provides protection for private applications.

B. It provides access to private applications.

C. It acts as a cloud-based firewall.

D. It requires on-premises hardware.

Answer(s): A B

13. You are required to mitigate malicious scripts from being downloaded into your corporate devices every time a user goes to a website. Users need to access websites from a variety of categories, including new websites.

Which two actions would help you accomplish this task while allowing the user to work? (Choose two.)

A. Allow the user to browse uncategorized domains but restrict edit activities.

B. Block malware detected on download activity for all remaining categories.

C. Block known bad websites and enable RBI to uncategorized domains.

D. Allow a limited amount of domains and block everything else.

Answer(s): B C

14. 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(s): B

15. A company is attempting to steer traffic to Netskope using GRE tunnels. They notice that after the initial configuration, users cannot access external websites from their browsers.

What are three probable causes for this issue? (Choose three.)

A. The pre-shared key for the GRE tunnel is incorrect.

B. The configured GRE peer in the Netskope platform is incorrect.

C. The corporate firewall might be blocking GRE traffic.

D. The route map was applied to the wrong router interface.

E. Netskope does not support GRE tunnels.

Answer(s): B C D

16. What are two fundamental differences between the inline and API implementation of the Netskope platform? (Choose two.)

A. The API implementation can be used with both sanctioned and unsanctioned applications.

B. The API implementation can only be used with sanctioned applications.

C. The inline implementation can effectively block a transaction in both sanctioned and unsanctioned applications.

D. The inline implementation can only effectively block a transaction in sanctioned applications.

Answer(s): B C

17. 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? (Choose two.)

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(s): B C

18. Why would you want to define an App Instance?

A. to create an API Data Protection Policy for a personal Box instance

B. to differentiate between an enterprise Google Drive instance vs. a personal Google Drive instance

C. to enable the instance_id attribute in the advanced search field when using query mode

D. to differentiate between an enterprise Google Drive instance vs. an enterprise Box instance

Answer(s): B

19. You want to enable Netskope to gain visibility into your users' cloud application activities in an inline mode.

In this scenario, which two deployment methods would match your inline use case? (Choose two.)

A. Use a forward proxy.

B. Use an API connector

C. Use a log parser.

D. Use a reverse proxy.

Answer(s): A D

20. Which two cloud security and infrastructure enablement technologies does Secure Access Service Edge (SASE) combine into its unified platform? (Choose two.)

A. Distributed Denial of Service Protection (DDoS)

B. Zero Trust Network Access (ZTNA)

C. Cloud Access Security Broker (CASB)

D. Unified Threat Management (UTM)

Answer(s): B C
