Vendor: Netskope

Exam Code: NSK101

Exam Name: Netskope Certified Cloud Security Administrator Exam

Version: DEMO

QUESTION 1

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: BCE

Explanation:

Three security controls that are offered by the Netskope Cloud platform are: C. cloud security posture management, E. threat protection, and B. data loss prevention for SMTP. Cloud security posture management is a service that provides continuous assessment and remediation of public cloud deployments for risks, threats, and compliance issues. Netskope CSPM leverages the APIs available from cloud service providers such as AWS, Azure, and GCP to scan the cloud infrastructure for misconfigurations, such as insecure permissions, open ports, unencrypted data, etc. Netskope CSPM also provides security posture policies, profiles, and rules that can be customized to match the security standards and best practices of the organization or industry.

Threat protection is a capability to detect and block malware, ransomware, phishing, and other cyber threats that may compromise cloud data or users. Netskope threat protection uses advanced techniques such as machine learning, sandboxing, threat intelligence, and behavioral analysis to identify and prevent malicious activities in real time. Netskope threat protection also integrates with third-party solutions such as antivirus engines, firewalls, SIEMs, etc., to provide comprehensive defense across the cloud and web.

Data loss prevention for SMTP is a feature that allows you to protect sensitive data that is sent or received via email. Netskope DLP for SMTP can scan email messages and attachments for predefined or custom data patterns, such as credit card numbers, social security numbers, health records, etc., and apply appropriate actions, such as block, quarantine, encrypt, notify, etc., based on the DLP policies. Netskope DLP for SMTP can also support multiple email domains and routing rules for different groups of users.

QUESTION 2

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. laaS API-enabled Protection
D. SaaS API-enabled Protection

Answer: D

Explanation:

SaaS API-enabled Protection is a primary function in the Netskope platform that allows customers to connect their sanctioned SaaS applications to Netskope using out-of-band API connections. This enables customers to find sensitive content, enforce near real-time policy controls, and quarantine malware in their SaaS applications without affecting user experience or performance. If you want to use an out-of-band API connection into your sanctioned Microsoft 365 OneDrive for Business application to achieve these goals, you should use SaaS API-enabled Protection as the primary function in the Netskope platform. DLP forensics, Risk Insights, and

IaaS API-enabled Protection are not primary functions in the Netskope platform that can be used to connect your application to Netskope.

QUESTION 3
You need to create a service request ticket for a client-related issue using the Netskope client Ul. 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: C
Explanation:
To create a service request ticket for a client-related issue using the Netskope client UI, you need to generate the client logs by right-clicking on the system tray icon and choosing Troubleshoot. This will open a window where you can select the option to Save Logs, which will create a zip file containing the client logs. You can then attach this file to your service request ticket and provide any relevant details about the issue. Choosing Save logs, Configuration, or Help will not generate the client logs, as they perform different functions, such as saving the current configuration, opening the settings menu, or opening the help page.

QUESTION 4
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: BC
Explanation:
Secure Access Service Edge (SASE) is a cloud-based architecture that combines various cloud security and infrastructure enablement technologies into a unified platform that delivers security and networking services from the edge of the network. Two of these technologies are Zero Trust Network Access (ZTNA) and Cloud Access Security Broker (CASB). ZTNA is a technology that provides secure access to private applications without exposing them to the internet or using VPNs. It uses identity- based policies and encryption to grant granular access to authorized users and devices, regardless of their location or network. CASB is a technology that provides visibility and control over cloud applications (SaaS) used by users and devices. It uses API connections or inline proxies to inspect and enforce policies on data and activities in cloud applications, such as data loss prevention, threat protection, or compliance. Distributed Denial of Service Protection (DDoS) and Unified Threat Management (UTM) are not technologies that SASE combines into its unified platform, although they may be related or integrated with some of its components.

QUESTION 5
In the Skope IT interface, which two event tables would be used to label a cloud application instance? (Choose two.)

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

Answer: BC
Explanation:
In the Skope IT interface, which is a feature in the Netskope platform that allows you to view and analyze all the activities performed by users on cloud applications, there are two event tables that would be used to label a cloud application instance: Page Events and Application Events. Page Events are events that capture the URL and category of the web pages visited by users, as well as the time spent and the bytes transferred on each page. Application Events are events that capture the details of the actions performed by users on cloud applications, such as upload, download, share, edit, delete, etc. You can use these event tables to label a cloud application instance by applying filters based on the domain name or URL of the instance, such as drive.google.com/a/yourcompany.com or slack.com/yourteam. You can then assign a custom label to the filtered events and use it for reporting or policy enforcement. Network Events and Alerts are not event tables that would be used to label a cloud application instance, as they are more related to network traffic or policy violations, rather than cloud application activities.

QUESTION 6
Your department is asked to report on GDPR data publicly exposed in Microsoft 365, Salesforce. and Slack-sanctioned cloud applications. Which deployment model would you use to discover this data?

A. reverse proxy
B. on-premises appliance
C. API-enabled protection
D. inline protection

Answer: C
Explanation:
To discover GDPR data publicly exposed in Microsoft 365, Salesforce, and Slack-sanctioned cloud applications, you need to use a deployment model that allows Netskope to access and scan the data stored in these applications using out-of-band API connections. The deployment model that would match this requirement is API-enabled protection, which is a feature in the Netskope platform that allows you to connect your sanctioned cloud applications to Netskope using API connectors. This enables you to discover sensitive data, enforce near real-time policy controls, and quarantine malware in your cloud applications without affecting user experience or performance. You can use Netskope's data loss prevention (DLP) engine to scan for GDPR data in your cloud applications and identify any public exposure or sharing settings that may violate the regulation. A reverse proxy, an on-premises appliance, or an inline protection are not deployment models that would help you discover GDPR data publicly exposed in your sanctioned cloud applications, as they are more suitable for inline modes that rely on intercepting traffic to and from these applications in real time, rather than accessing data stored in these applications using APIs.

QUESTION 7
Which two technologies form a part of Netskope's Threat Protection module? (Choose two.)

A. log parser
B. DLP

C. sandbox
D. heuristics

Answer: CD
Explanation:
To protect your users from malicious scripts that may be downloaded from websites, you need to use technologies that can detect and prevent malware, ransomware, phishing, and other advanced threats in web traffic. Two technologies that form a part of Netskope's Threat Protection module, which is a feature in the Netskope platform that provides these capabilities, are sandbox and heuristics. Sandbox is a technology that allows Netskope to analyze suspicious files or URLs in a virtual environment isolated from the rest of the network. It simulates the execution of the files or URLs and observes their behavior and impact on the system. It then generates a verdict based on the analysis and blocks any malicious files or URLs from reaching your users or devices. Heuristics is a technology that allows Netskope to identify unknown or emerging threats based on their characteristics or patterns, rather than relying on predefined signatures or rules. It uses machine learning and artificial intelligence to analyze various attributes of files or URLs, such as file type, size, entropy, metadata, code structure, etc., and assigns a risk score based on the analysis. It then blocks any files or URLs that exceed a certain risk threshold from reaching your users or devices. A log parser or DLP are not technologies that form a part of Netskope's Threat Protection module, as they are more related to discovering cloud applications or protecting sensitive data.

QUESTION 8
You just deployed the Netskope client in Web mode and several users mention that their messenger application is no longer working. Although you have a specific real-time policy that allows this application, upon further investigation you discover that it is using proprietary encryption. You need to permit access to all the users and maintain some visibility. In this scenario, which configuration change would accomplish this task?

A. Change the real-time policy to block the messenger application.
B. Create a new custom cloud application using the custom connector that can be used in the real-time policy.
C. Add a policy in the SSL decryption section to bypass the messenger domain(s).
D. Edit the steering configuration and add a steering exception for the messenger application.

Answer: C
Explanation:
In this scenario, you have deployed the Netskope client in Web mode, which is a feature that allows you to steer your users' web traffic to Netskope for inspection and policy enforcement. However, some users report that their messenger application is no longer working, even though you have a specific real-time policy that allows this application. Upon further investigation, you discover that the messenger application is using proprietary encryption, which means that Netskope cannot decrypt or inspect the traffic from this application. To resolve this issue, you need to permit access to all the users and maintain some visibility. The configuration change that would accomplish this task is to add a policy in the SSL decryption section to bypass the messenger domain(s). This will allow Netskope to skip the decryption process for the traffic from the messenger application and pass it through without any modification. However, Netskope will still be able to log some basic information about the traffic, such as source, destination, bytes, etc., for visibility purposes. Changing the real- time policy to block the messenger application, creating a new custom cloud application using the custom connector, or editing the steering configuration and adding a steering exception for the messenger application are not configuration changes that would accomplish this task, as they would either prevent access to the application, require additional steps or resources, or reduce visibility.