

EXAM PREPARATION MATERIAL

Practice files designed to help you understand exam patterns, question styles and the overall assessment format.

IMPORTANT NOTE



Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns.



Stay connected with our support team for the latest file updates and exam-related information.

Question: 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: D

Explanation:

A file filter is a list of file hashes that you can use to exclude files from inspection by Netskope. By adding the hash of the file that triggered a false alarm to the file filter, you can prevent it from being scanned again by Netskope and avoid generating another incident. Quarantining the file, exporting the packet capture, or looking up the hash at VirusTotal are not effective ways to prevent the same file from triggering another incident, as they do not affect how Netskope handles the file. Reference: [Netskope Security Cloud Operation & Administration \(NSCO&A\) - Classroom Course](#), Module 6: Data Loss Prevention, Lesson 2: File Filters.

Question: 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: B, C

Explanation:

The Building Security in Maturity Model (BSIMM) is a framework that measures and compares the security activities of different organizations. It helps organizations to assess their current security practices and identify areas for improvement. ISO 27001 is an international standard that specifies the requirements for establishing, implementing, maintaining, and improving an information security management system. It helps organizations to manage their information security risks and demonstrate their compliance with best practices. Data Science Council of America (DASCA) is not a security framework, but a credentialing body for data science professionals. NIST Cybersecurity Framework (NIST CSF) is a security framework, but it is not commonly used to assess and validate a vendor's security practices, as it is more focused on improving the cybersecurity of critical infrastructure sectors in the United States. Reference: [BSIMM], [ISO 27001], [DASCA], [NIST CSF].

Question: 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: AB

Explanation:

If the Cloud Storage category is in the Steering Configuration as an exception, then Netskope will not steer any traffic to or from cloud storage applications, such as Microsoft 365 OneDrive, to its platform. This means that Netskope will not be able to inspect or apply any policies to this traffic, including DLP policies. Similarly, if the destination domain is excluded from decryption in the decryption policy, then Netskope will not decrypt any traffic to or from that domain, such as onedrive.com. This means that Netskope will not be able to inspect or apply any policies to this traffic, including DLP policies. The location of the Netskope POP or the use of IPsec as a steering option do not affect the application of DLP policies, as long as Netskope can steer and decrypt the relevant traffic. Reference: [Netskope Security Cloud Operation & Administration \(NSCO&A\) - Classroom Course](#), Module 3: Steering Configuration, Lesson 1: Steering Options and Lesson 2: Exceptions; Module 4: Decryption Policy, Lesson 1: Decryption Policy Overview and Lesson 2: Decryption Policy Configuration.

: <https://www.bsimm.com/> : <https://www.iso.org/isoiec-27001-information-security.html> : <https://www.dasca.org/> : <https://www.nist.gov/cyberframework>

Question: 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: B

Explanation:

The CCI scoring is a way to measure the security posture of cloud applications based on a set of criteria and weights. The default objective score is calculated by Netskope using industry best practices and standards. However, customers can change the CCI scoring to suit their own business needs and risk appetite. For example, a customer may want to place a higher business risk weight on vendors that claim ownership of their data, as this may affect their data sovereignty and privacy rights. Changing the CCI scoring for this reason would be valid, as it reflects the customer's own security requirements and preferences. Changing the CCI scoring for other reasons, such as discovering a new SaaS application, punishing an application vendor, or using an application under research, would not be valid, as they do not align with the purpose and methodology of the CCI scoring. Reference: [Netskope Security Cloud Operation & Administration \(NSCO&A\) - Classroom Course](#), Module 7: Cloud Confidence Index (CCI), Lesson 1: CCI Overview and Lesson 2: CCI Scoring.

Question: 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: A, D

Explanation:

Netskope's DLP solution is a powerful tool that can help customers protect their sensitive data from unauthorized access, exposure, or loss. One use case for Netskope's DLP solution is to stop unintentional data movement, such as accidental uploads, downloads, or sharing of confidential files or information to or from cloud applications. Another use case for Netskope's DLP solution is to ensure regulatory compliance, such as GDPR, HIPAA, PCI-DSS, or other industry-specific standards that require data protection and privacy measures. Netskope's DLP solution can help customers comply with these regulations by detecting and preventing data breaches, enforcing encryption policies, applying data retention rules, and generating audit reports. Detecting malware in files before they are uploaded to a cloud application or detecting sensitive data in password protected files are not use cases for Netskope's DLP solution, as they are more related to threat protection or file inspection capabilities. Reference: [Netskope Security Cloud Operation & Administration \(NSCO&A\) - Classroom Course](#), Module 6: Data Loss Prevention, Lesson 1: DLP Overview.

Question: 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: A, D

Explanation:

A Netskope Virtual Appliance is a software-based appliance that can be deployed on-premises or in the cloud to provide various functions and features for the Netskope Security Cloud platform. One use for deploying a Netskope Virtual Appliance is as an endpoint for Netskope Private Access (NPA), which is a service that allows users to securely access private applications without exposing them to the internet or using VPNs. Another use for deploying a Netskope Virtual Appliance is as a Secure Forwarder to steer traffic from on-premises devices or networks to the Netskope platform for inspection and policy enforcement. Using a Netskope Virtual Appliance as a local reverse-proxy to secure a SaaS application or as a log parser to discover in-use cloud applications are not valid uses, as these functions are performed by other components of the Netskope Security Cloud platform, such as the Cloud Access Security Broker (CASB) or the Cloud XD engine. Reference: [Netskope Security Cloud Operation & Administration \(NSCO&A\) - Classroom Course](#), Module 2:

Architecture Overview; [Netskope Private Access]; [Netskope Secure Forwarder].

Question: 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?

- A. SOC 3
- B. PCI-DSS
- C. AES-256
- D. ISO 27001

Answer: B

Explanation:

PCI-DSS stands for Payment Card Industry Data Security Standard, which is a set of security requirements for organizations that handle credit card data. It aims to protect cardholder data from unauthorized access, disclosure, or theft, both in transit and at rest. PCI-DSS covers various aspects of security, such as encryption, authentication, firewall, logging, monitoring, and incident response. If you are working with a large retail chain and have concerns about their customer data, you should use PCI-DSS as the regulatory compliance standard to govern this data. SOC 3, AES-256, and ISO 27001 are not specific to credit card data protection, although they may have some relevance to general security practices. Reference: [PCI-DSS], [SOC 3], [AES-256], [ISO 27001].

Question: 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: B

Explanation:

A real-time policy is a type of policy in Netskope's CASB that allows you to control the actions that users can perform on cloud applications in real time. You can use a real-time policy to block all users from uploading data files into risky collaboration applications by specifying the following elements: the application category (such as Collaboration), the activity (such as Upload), the file type (such as Data), the risk level (such as High or Very High), and the action (such as Block). A DLP rule, a DLP profile, and a block notification are not sufficient to accomplish this task, as they are either subcomponents or outcomes of a real-time policy. Reference: [Netskope Security Cloud Operation & Administration \(NSCO&A\) - Classroom Course](#), Module 5: Real-Time Policies, Lesson 1: Real-Time Policy Overview and Lesson 2: Real-Time Policy Configuration.

Question: 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: 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 web¹.](#)

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 users².](#)

Question: 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: 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. Reference: [Netskope SaaS API-enabled Protection].

Question: 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: 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. Reference: [Netskope Client Troubleshooting].

Question: 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: AB

Explanation:

Netskope's Private Access Solution is a service that allows users to securely access private applications without exposing them to the internet or using VPNs. It provides protection for private applications by encrypting the traffic, enforcing granular policies, and preventing data exfiltration. It also provides access to private applications by creating a secure tunnel between the user's device and the application's server, regardless of their location or network. It does not act as a cloud-based firewall, as it does not filter or block traffic based on ports or protocols. It does not require on-premises hardware, as it is a cloud-native solution that leverages Netskope's global network of points of presence (POPs).

Reference: [Netskope Private Access].

Question: 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: B, C

Explanation:

To mitigate malicious scripts from being downloaded into your corporate devices every time a user goes to a website, you need to use Netskope's threat protection features to block or isolate potentially harmful web traffic. Two actions that would help you accomplish this task while allowing the user to work are: block malware detected on download activity for all remaining categories and block known bad websites and enable RBI to uncategorized domains. The first action will prevent any files that contain malware from being downloaded to your devices from any website category, except those that are explicitly allowed or excluded by your policies. The second action will prevent any websites that are classified as malicious or phishing by Netskope from being accessed by your users and enable Remote Browser Isolation (RBI) to uncategorized domains, which are domains that have not been assigned a category by Netskope. RBI is a feature that allows users to browse websites in a virtual browser hosted in the cloud, without exposing their devices

to any scripts or content from the website. Allowing the user to browse uncategorized domains but restrict edit activities or allowing a limited amount of domains and block everything else are not effective actions, as they may either limit the user's productivity or expose them to unknown risks. Reference: [Netskope Threat Protection], [Netskope Remote Browser Isolation].

Question: 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: B

Explanation:

In this scenario, policy B is more restrictive than policy A, as it blocks users from downloading files from any OS other than Mac or Windows for cloud storage, while policy A only generates alerts when any user downloads, uploads, or shares files on a cloud storage application. Therefore, policy B should be implemented before policy A, as the policy order determines the order of evaluation and enforcement of the policies. If policy A is implemented before policy B, then policy B will never be triggered, as policy A will match all the download activities for cloud storage and generate alerts. The policy order is important; policies are not independent of each other, as they may have overlapping or conflicting conditions and actions. These two policies would actually work together, as long as they are ordered correctly. Reference: [Netskope Security Cloud Operation & Administration \(NSCO&A\) - Classroom Course](#), Module 5: Real-Time Policies, Lesson 3: Policy Order.

Question: 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: BCD

Explanation:

In this scenario, there are three probable causes for the issue of users not being able to access external websites from their browsers after attempting to steer traffic to Netskope using GRE tunnels. One cause is that the configured GRE peer in the Netskope platform is incorrect, which means that the Netskope POP that is supposed to receive the GRE traffic from the customer's network is not matching the IP address of the customer's router that is sending the GRE traffic. This will result in a failure to establish a GRE tunnel between the customer and Netskope. Another cause is that the corporate firewall might be blocking GRE traffic, which means that the firewall rules are not allowing the GRE protocol (IP protocol number 47) or the UDP port 4789 (for VXLAN encapsulation) to pass through. This will result in a failure to send or receive GRE packets between the customer and Netskope. A third cause is that the route map was applied to the wrong router interface, which means that the configuration that specifies which traffic should be steered to Netskope using GRE tunnels was not applied to the correct interface on the customer's router. This will result in a failure to steer the desired traffic to Netskope. The pre-shared key for the GRE tunnel is incorrect is not a probable cause for this issue, as GRE tunnels do not use pre-shared keys for authentication or encryption. Netskope does support GRE tunnels, so this is not a cause for this issue either. Reference: [Netskope Secure Forwarder], [Netskope Security Cloud Operation & Administration \(NSCO&A\) - Classroom Course](#), Module 3: Steering Configuration, Lesson 3: Secure Forwarder.

Question: 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: BC

Explanation:

The inline and API implementation of the Netskope platform are two different ways of connecting cloud applications to Netskope for inspection and policy enforcement. Two fundamental differences between them are: The API implementation can only be used with sanctioned applications, which are applications that are approved and authorized by the organization for business use. The API implementation relies on using out-of-band API connections to access data and events from these applications and apply near real-time policies. The inline implementation can effectively block a transaction in both sanctioned and unsanctioned applications, which are applications that are not approved or authorized by the organization for business use. The inline implementation relies on using in-band proxy or reverse-proxy connections to intercept traffic to and from these applications and apply real-time policies. The API implementation can be used with both sanctioned and unsanctioned applications and the inline implementation can only effectively block a transaction in sanctioned applications are not true statements, as they contradict the actual capabilities and limitations of each implementation method. Reference: [Netskope SaaS API-enabled Protection], [Netskope Inline CASB].

Question: 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: BC

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: 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: B

Explanation:

An App Instance is a feature in the Netskope platform that allows you to define and identify different instances of the same cloud application based on the domain name or URL. For example, you can define an App Instance for your enterprise Google Drive instance (such as drive.google.com/a/yourcompany.com) and another App Instance for your personal Google Drive instance (such as drive.google.com). This way, you can differentiate between them and apply different policies and actions based on the App Instance. You would want to define an App Instance to achieve this level of granularity and control over your cloud application activities. Creating an API Data Protection Policy for a personal Box instance, enabling the instance_id attribute in the advanced search field, or differentiating between an enterprise Google Drive instance vs. an enterprise Box instance are not valid reasons to define an App Instance, as they are either unrelated or irrelevant to the App Instance feature. Reference: [Netskope Security Cloud Operation & Administration \(NSCO&A\) - Classroom Course](#), Module 5: Real-Time Policies, Lesson 4: App Instances.

Question: 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: A, D

Explanation:

To enable Netskope to gain visibility into your users' cloud application activities in an inline mode, you need to use a deployment method that allows Netskope to intercept and inspect the traffic between your users and the cloud applications in real time. Two deployment methods that would match your inline use case are: use a forward proxy and use a reverse proxy. A forward proxy is a deployment method that allows Netskope to act as a proxy server for your users' outbound traffic to the internet. You can configure your users' devices or browsers to send their traffic to Netskope's proxy server, either manually or using PAC files or VPN profiles. A reverse proxy is a deployment method that allows Netskope to act as a proxy server for your users' inbound traffic from specific cloud applications. You can configure your cloud applications to redirect their traffic to Netskope's proxy server, either using custom URLs or certificates. Using an API connector or a log parser are not deployment methods that would match your inline use case,

as they are more suitable for out-of-band modes that rely on accessing data and events from the cloud applications using APIs or logs, rather than intercepting traffic in real time. Reference: [Netskope Inline CASB], [Netskope Security Cloud Operation & Administration \(NSCO&A\) - Classroom Course](#), Module 3: Steering Configuration, Lesson 4:

Forward Proxy and Lesson 5: Reverse Proxy.

Question: 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: 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. Reference: [SASE], [ZTNA], [CASB].

Question: 21

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: B, C

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. Reference: [Netskope Skope IT], [Netskope Security Cloud Operation & Administration \(NSCO&A\) - Classroom Course](#), Module 8: Skope IT.

Question: 22

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. Reference: [Netskope SaaS API-enabled Protection], [Netskope Data Loss Prevention].

Question: 23

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

- A. log parser
- B. DLP
- C. sandbox
- D. heuristics

Answer: C, D

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. Reference: [Netskope Threat Protection], [Netskope Security Cloud Operation & Administration \(NSCO&A\) - Classroom Course](#), Module 9: Threat Protection.

Question: 24

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 realtime 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 realtime 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. Reference: [Netskope Client], [Netskope Security Cloud Operation & Administration \(NSCO&A\) - Classroom Course](#), Module 4: Decryption Policy.

Question: 25

You consume application infrastructure (middleware) capabilities by a third-party provider. What is the cloud service model that you are using in this scenario?

- A. PaaS
- B. MaaS
- C. DaaS
- D. SaaS

Answer: A

Explanation:

If you consume application infrastructure (middleware) capabilities by a third-party provider, then the cloud service model that you are using in this scenario is PaaS, which stands for Platform as a Service. PaaS is a cloud service model that provides customers with a platform to develop, run, and manage applications without having to deal with the underlying infrastructure or software. PaaS typically includes middleware capabilities such as databases, web servers, development tools, integration services, etc., that customers can use to build and deploy their applications faster and easier. MaaS, DaaS, and SaaS are not cloud service models that match this scenario, as they stand for different types of services. MaaS stands for Monitoring as a Service, which is a service that provides customers with tools to monitor and manage their cloud resources and performance. DaaS stands for Desktop as a Service, which is a service that provides customers with virtual desktops that they can access from any device or location. SaaS stands for Software as a Service, which is a service that provides customers with software applications that they can use over the internet without installing or maintaining them. Reference: [PaaS], [MaaS], [DaaS], [SaaS].

Question: 26

You are deploying TLS support for real-time Web and SaaS transactions. What are two secure implementation methods in this scenario? (Choose two.)

- A. Bypass TLS 1.3 because it is not widely adopted.
- B. Downgrade to TLS 1.2 whenever possible.
- C. Support TLS 1.2 only when 1.3 is not supported by the server.
- D. Require TLS 1.3 for every server that accepts it.

Answer: C, D

Explanation:

If you are deploying TLS support for real-time Web and SaaS transactions, then you need to use secure implementation methods that ensure the highest level of encryption and security for your traffic. Two secure implementation methods in this scenario are: support TLS 1.2 only when 1.3 is not supported by the server and require TLS 1.3 for every server that accepts it. TLS stands for Transport Layer Security, which is a protocol that provides secure communication over the internet by encrypting and authenticating data exchanged between two parties. TLS 1.3 is the latest version of TLS, which offers several improvements over TLS 1.2, such as faster handshake, stronger encryption algorithms, better forward secrecy, and reduced attack surface. Therefore, it is recommended to use TLS 1.3 whenever possible for real-time Web and SaaS transactions, as it provides better security and performance than TLS 1.2. However, some servers may not support TLS 1.3 yet, so in those cases, it is acceptable to use TLS 1.2 as a fallback option, as it is still considered secure and widely adopted. Bypassing TLS 1.3 because it is not widely adopted or downgrading to TLS 1.2 whenever possible are not secure implementation methods in this scenario, as they would compromise the security and performance of your traffic by using an older or weaker version of TLS than necessary. Reference: [TLS], [TLS 1.3].

Question: 27

What correctly defines the Zero Trust security model?

- A. least privilege access
- B. multi-layered security
- C. strong authentication
- D. double encryption

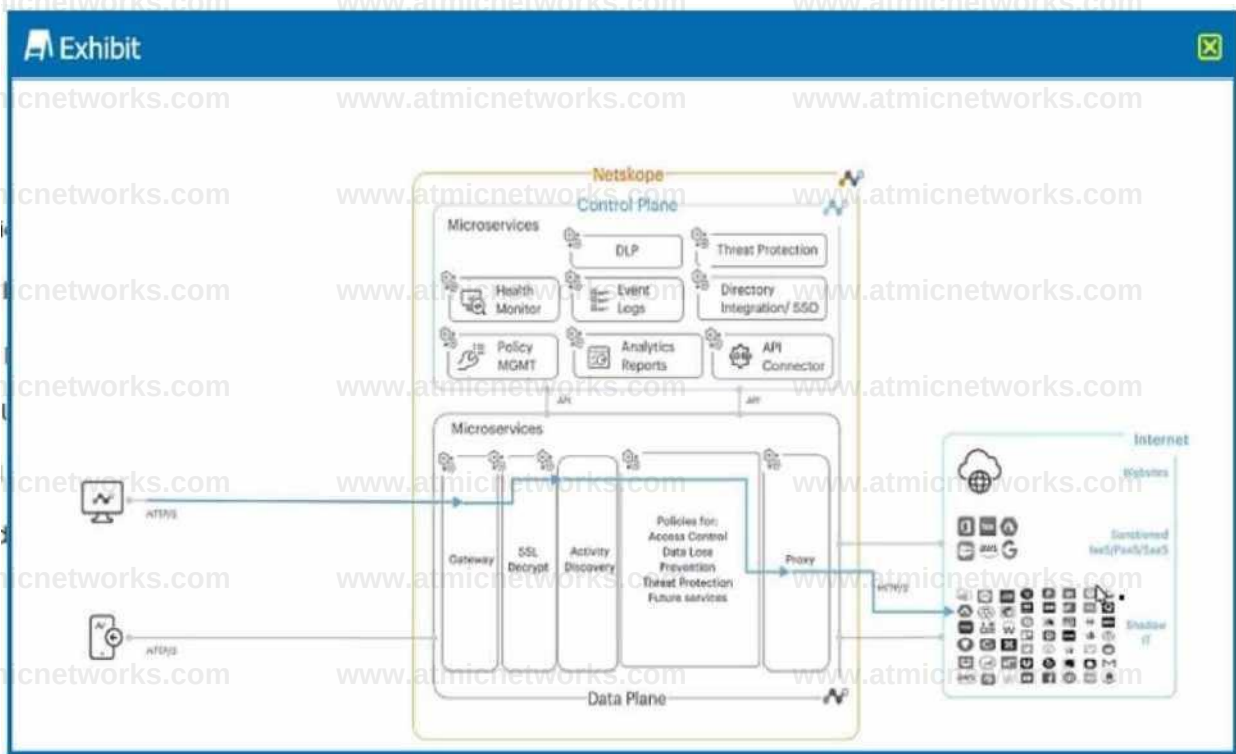
Answer: A

Explanation:

The term that correctly defines the Zero Trust security model is least privilege access. The Zero Trust security model is a modern security strategy based on the principle: never trust, always verify. Instead of assuming everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an open network. One of the core principles of the Zero Trust model is to use least privilege access, which means granting users or systems only the minimum level of access they need to perform their tasks, and only for a limited time. This helps reduce the attack surface and minimize the impact of a potential breach. Reference: [Zero Trust Security - microsoft.com](#)
[What is Zero Trust Security? Principles of the Zero Trust Model](#)

Question: 28

Exhibit



A user is connected to a cloud application through Netskope's proxy.

In this scenario, what information is available at Skope IT? (Choose three.)

- A. username, device location
- B. destination IP, OS patch version
- C. account instance, URL category
- D. user activity, cloud app risk rating
- E. file version, shared folder

Answer: ACD

Explanation:

In this scenario, a user is connected to a cloud application through Netskope's proxy, which is a deployment method that allows Netskope to intercept and inspect the traffic between the user and the cloud application in real time. In this case, Netskope can collect and display various information about the user and the cloud application at Skope IT, which is a feature in the Netskope platform that allows you to view and analyze all the activities performed by users on cloud applications. Some of the information that is available at Skope IT are: username, device location, account instance, URL category, user activity, and cloud app risk rating. Username is the name or identifier of the user who is accessing the cloud

application. Device location is the geographical location of the device that the user is using to access the cloud application. Account instance is the specific instance of the cloud application that the user is accessing, such as a personal or enterprise instance. URL category is the classification of the web page that the user is visiting within the cloud application, such as Business or Social Media. User activity is the action that the user is performing on the cloud application, such as Upload or Share. Cloud app risk rating is the score that Netskope assigns to the cloud application based on its security posture and compliance with best practices. Destination IP, OS patch version, file version, and shared folder are not information that is available at Skope IT in this scenario, as they are either unrelated or irrelevant to the proxy connection or the Skope IT feature. Reference: [Netskope Inline CASB], [Netskope Skope IT].

Question: 29

What is a benefit that Netskope instance awareness provides?

- A. It prevents movement of corporate sensitive data to a personal Dropbox account.
- B. It prevents the user from copying information from a corporate email and pasting the information into a GitHub repository.
- C. It differentiates between an IT managed Google Drive instance versus a personal Dropbox account.
- D. It differentiates between an IT managed Google Drive instance versus a personal Google Drive instance.

Answer: D

Explanation:

A benefit that Netskope instance awareness provides is that it differentiates between an IT managed Google Drive instance versus a personal Google Drive instance. Instance awareness is a feature in the Netskope platform that allows you to define and identify different instances of the same cloud application based on the domain name or URL. For example, you can define an instance for your IT managed Google Drive instance (such as drive.google.com/a/yourcompany.com) and another instance for your personal Google Drive instance (such as drive.google.com). This way, you can differentiate between them and apply different policies and actions based on the instance. This can help you prevent data leakage, enforce compliance, or improve visibility for your cloud application activities. Preventing movement of corporate sensitive data to a personal Dropbox account, preventing the user from copying information from a corporate email and pasting it into a GitHub repository, or differentiating between an IT managed Google Drive instance versus an IT managed Box instance are not benefits that Netskope instance awareness provides, as they are either unrelated or irrelevant to the instance awareness feature. Reference: [Netskope Security Cloud Operation & Administration \(NSCO&A\) - Classroom Course](#), Module 5: Real-Time Policies, Lesson 4: App Instances.

Question: 30

According to Netskope, what are two preferred methods to report a URL miscategorization? (Choose two.)

- A. Use www.netskope.com/url-lookup.
- B. Use the URL Lookup page in the dashboard.
- C. Email support@netskope.com.
- D. Tag Netskope on Twitter.

Answer: A, B

Explanation:

According to Netskope, two preferred methods to report a URL miscategorization are: use www.netskope.com/url-lookup and use the URL Lookup page in the dashboard. The first method allows you to visit www.netskope.com/url-lookup in your browser and enter any URL that you want to check or report for miscategorization. You will see the current category assigned by Netskope for that URL and you can submit a request to change it if you think it is incorrect. The second method allows you to use the URL Lookup page in the dashboard of your Netskope platform tenant and enter any URL that you want to check or report for miscategorization. You will see the current category assigned by Netskope for that URL and you can submit a request to change it if you think it is incorrect. Emailing support@netskope.com or tagging Netskope on Twitter are not preferred methods to report a URL miscategorization, as they are not designed for this purpose and may not be as efficient or effective as using the dedicated tools provided by Netskope. Reference: [Netskope URL Lookup], [Netskope Security Cloud Operation & Administration \(NSCO&A\) - Classroom Course](#), Module 8: Skope IT, Lesson 2: Page Events.

Question: 31

You want to deploy Netskope's zero trust network access (ZTNA) solution, NP

- A. In this scenario, which action would you perform to accomplish this task?
- B. Create an OAuth identity access control between your users and your applications.
- C. Set up a reverse proxy using SAML and an identity provider.
- D. Enable Steer all Private Apps in your existing steering configuration(s) from the admin console.
- E. Configure SCIM to exchange identity information and attributes with your applications.

Answer: C

Explanation:

To deploy Netskope's zero trust network access (ZTNA) solution, NPA, you need to enable Steer all Private Apps in your existing steering configuration(s) from the admin console. This will allow you to create private app profiles and assign them to your applications. NPA will then provide secure and granular access to your applications without exposing them to the internet or requiring VPNs. Reference: [Netskope Private Access (NPA) Deployment Guide]

Question: 32

What is the limitation of using a legacy proxy compared to Netskope's solution?

- A. Netskope architecture requires on-premises components.
- B. Legacy solutions offer higher performance and scalability for corporate and remote users.
- C. Legacy on-premises solutions fail to provide protection for traffic from on-premises users.
- D. To enforce policies, traffic needs to traverse back through a customer's on-premises security stack.

Answer: D

Explanation:

A limitation of using a legacy proxy compared to Netskope's solution is that to enforce policies, traffic needs to traverse back through a customer's on-premises security stack. This creates latency, bandwidth, and scalability issues for remote users and cloud applications. Netskope's solution, on the other hand, leverages a cloud-native architecture that provides high-performance and scalable inspection of traffic from any location and device. Reference: [Netskope Architecture Overview]

Question: 33

You are creating a real-time policy for cloud applications.

In addition to users, groups, and organizational units, which two source criteria would support this scenario? (Choose two.)

- A. protocol version
- B. access method
- C. browser version
- D. device classification

Answer: BD

Explanation:

When creating a real-time policy for cloud applications, you can use access method and device classification as source criteria, in addition to users, groups, and organizational units. Access method refers to how the user accesses the cloud application, such as browser, sync client, mobile app, etc. Device classification refers to the type of device used by the user, such as managed or unmanaged, Windows or Mac, etc. These criteria can help you define granular policies based on different scenarios and risks. Reference: [Creating Real-Time Policies for Cloud Applications]

Question: 34

What are two reasons why legacy solutions, such as on-premises firewalls and proxies, fail to secure the data and data access compared to Netskope Secure Web Gateway? (Choose two.)

- A. Legacy solutions are unable to see the user who is trying to access the application.
- B. The applications where the data resides are no longer in one central location.
- C. Legacy solutions do not meet compliance standards.
- D. The users accessing this data are not in one central place.

Answer: BD

Explanation:

Legacy solutions, such as on-premises firewalls and proxies, fail to secure the data and data access compared to Netskope Secure Web Gateway because they are designed for a perimeter-based security model, where the applications and the users are both within the corporate network. However, with the rise of cloud computing and remote work, this model is no longer valid. The applications where the data resides are no longer in one central location, but distributed across multiple cloud services and regions. The users accessing this data are not in one central place, but working from anywhere, on any device. Legacy solutions cannot provide adequate visibility and control over this dynamic and complex environment,

resulting in security gaps and performance issues. Netskope Secure Web Gateway, on the other hand, leverages a cloud-native architecture that provides high-performance and scalable inspection of traffic from any location and device, as well as granular policies and advanced threat and data protection for web and cloud applications. Reference: [Netskope Architecture Overview](#)[Netskope Next Gen SWG](#)

Question: 35

There is a DLP violation on a file in your sanctioned Google Drive instance. The file is in a deleted state. You need to locate information pertaining to this DLP violation using Netskope. In this scenario, which statement is correct?

- A. You can find DLP violations under Forensic profiles.
- B. DLP incidents for a file are not visible when the file is deleted.
- C. You can find DLP violations under the Incidents dashboard.
- D. You must create a forensic profile so that an incident is created.

Answer: C

Explanation:

To locate information pertaining to a DLP violation on a file in your sanctioned Google Drive instance, you can use the Incidents dashboard in Netskope. The Incidents dashboard provides a comprehensive view of all the incidents that have occurred in your cloud environment, such as DLP violations, malware infections, anomalous activities, etc. You can filter the incidents by various criteria, such as app name, incident type, severity, user name, etc. You can also drill down into each incident to see more details, such as file name, file path, file owner, file size, file type, etc. The Incidents dashboard can show DLP violations for files that are in a deleted state, as long as they are still recoverable from the trash bin of the app. If the file is permanently deleted from the app, then the incident will not be visible in the dashboard. Reference: [Netskope Incidents Dashboard](#)

Question: 36

What are two CASB inline interception use cases? (Choose two.)

- A. blocking file uploads to a personal Box account

- B. running a retroactive scan for data at rest in Google Drive
- C. using the Netskope steering client to provide user alerts when sensitive information is posted in Slack
- D. scanning Dropbox for credit card information

Answer: A, C

Explanation:

CASB inline interception use cases are scenarios where you need to apply real-time policies and actions on the traffic between users and cloud applications. For example, you may want to block file uploads to a personal Box account to prevent data leakage or exfiltration. You can use Netskope's inline proxy mode to intercept and inspect the traffic between users and Box, and apply granular policies based on user identity, device type, app instance, file metadata, etc. You can also use Netskope's inline proxy mode to provide user alerts when sensitive information is posted in Slack. For example, you may want to warn users when they share credit card numbers or social security numbers in Slack channels or messages. You can use Netskope's steering client to redirect the traffic between users and Slack to Netskope's inline proxy for inspection and enforcement. You can also use Netskope's DLP engine to detect sensitive data patterns and apply actions such as alerting or blocking. Reference: [Netskope Inline Proxy Mode](#)[Netskope Steering Client](#) [Netskope DLP Engine]

Question: 37

You want to take into account some recent adjustments to CCI scoring that were made in your Netskope tenant.

In this scenario, which two CCI aspects in the UI would be used in a real-time protection policy? (Choose two.)

- A. App Tag
- B. CCL
- C. App Score
- D. GDPR Readiness

Answer: A, C

Explanation:

To take into account some recent adjustments to CCI scoring that were made in your Netskope tenant, you can use the App

Tag and App Score aspects in the UI to create a real-time protection policy. The App Tag is a label that indicates the level of enterprise readiness of a cloud app based on its CCI score. The App Score is a numerical value that represents the CCI score of a cloud app based on various criteria such as security, auditability, and business continuity. You can use these aspects to filter cloud apps by their CCI ratings and apply policies accordingly. For example, you can create a policy that blocks access to cloud apps with an App Tag of Poor or an App Score below

50. Reference: [Netskope Cloud Confidence Index](#) [Creating Real-Time Policies for Cloud Applications](#)

Question: 38

You are working with traffic from applications with pinned certificates. In this scenario, which statement is correct?

- A. An exception should be added to the steering configuration.
- B. The domains used by certificate-pinned applications should be added to the authentication bypass list.
- C. Traffic with pinned certificates should be blocked.
- D. The domains used by applications with pinned certificates should be allowed in an inline policy.

Answer: A

Explanation:

When working with traffic from applications with pinned certificates, you should add an exception to the steering configuration to bypass them. Pinned certificates are a security technique that prevents man-in-the-middle attacks by validating the server certificates against a hardcoded list of certificates in the application. If you try to intercept or inspect the traffic from such applications, they will reject the connection or display an error message. Therefore, you should add the domains used by certificate-pinned applications as exceptions in your steering configuration, so that they are not steered to Netskope for analysis and enforcement. Reference: [Certificate Pinned Applications](#) [Creating a Steering Configuration](#)

Question: 39

Which two traffic steering configurations are supported by Netskope? (Choose two.)

- A. browser isolation traffic only
- B. cloud applications only
- C. all Web traffic including cloud applications
- D. Web traffic only

Answer: B, C

Explanation:

The two traffic steering configurations that are supported by Netskope are cloud applications only and all Web traffic including cloud applications. These configurations allow you to control what kind of traffic gets steered to Netskope for real-time deep analysis and what kind of traffic gets bypassed. You can choose one of these options for both on-premises and off-premises scenarios, depending on your network environment and security needs. You can also create exceptions for specific domains, IP addresses, or certificate-pinned applications that you want to bypass or steer regardless of the configuration option. Reference: [Steering Configuration](#)[Creating a Steering Configuration](#)

Question: 40

Which three technologies describe the primary cloud service models as defined by the National Institute of Standards and Technology (NIST)? (Choose three.)

- A. Cloud Service Provider (CSP)
- B. Identity as a Service (IDaaS)
- C. Platform as a Service (PaaS)
- D. Software as a Service (SaaS)
- E. Infrastructure as a Service (IaaS)

Answer: CDE

Explanation:

The three technologies that describe the primary cloud service models as defined by the National

Institute of Standards and Technology (NIST) are Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS). These service models are based on the type of computing capability that is provided by the cloud provider to the cloud consumer over a network. According to NIST, these service models have the following definitions:

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Reference: [The NIST Definition of Cloud Computing](#)[NIST Cloud Computing Program](#)

Question: 41

Which two controls are covered by Netskope's security platform? (Choose two.)

- A. ZTNA
- B. VPN
- C. CASB
- D. EDR

Answer: A, C

Explanation:

Netskope's security platform covers two controls: ZTNA and CASB. ZTNA stands for Zero Trust Network Access, which is a

solution that provides secure and granular access to private applications without exposing them to the internet or requiring VPNs. CASB stands for Cloud Access Security Broker, which is a solution that provides visibility and control over cloud services and web traffic, as well as data and threat protection for cloud users and devices. Reference: [Netskope PlatformNetskope ZTNANetskope CASB](#)

Question: 42

Which two statements are correct about DLP Incidents in the Netskope platform? (Choose two.)

- A. An incident can be associated to one or more DLP policies.
- B. An incident can have one or more DLP violations.
- C. An incident can be assigned to one or more administrators.
- D. An incident can be associated to one or more DLP rules.

Answer: BD

Explanation:

Two statements that are correct about DLP Incidents in the Netskope platform are: An incident can have one or more DLP violations and an incident can be associated to one or more DLP rules. A DLP violation occurs when a file or object matches a DLP rule used in a DLP profile. A DLP rule defines the criteria for detecting sensitive data, such as keywords, regular expressions, fingerprints, machine learning classifiers, etc. A DLP profile is a collection of DLP rules that can be applied to a policy. An incident is a record of a file or object that triggered a DLP policy violation. An incident can have multiple violations if the file or object matches multiple DLP rules from different profiles. An incident can also be associated to multiple DLP rules if the file or object matches more than one rule from the same profile. Reference: [About DLPDLP Profiles](#)

Question: 43

Which two statements describe a website categorized as a domain generated algorithm (DGA)? (Choose two.)

- A. The website is used for domain registration.
- B. The domain contains malicious algorithms.
- C. The website is used to hide a command-and-control server.

D. The domain was created by a program.

Answer: C, D

Explanation:

Two statements that describe a website categorized as a domain generated algorithm (DGA) are: The website is used to hide a command-and-control server and the domain was created by a program. A domain generated algorithm (DGA) is a technique used by cyber attackers to generate new domain names and IP addresses for malware's command and control servers. Executed in a manner that seems random, it makes it nearly impossible for threat hunters to detect and contain the attack. A command-and-control server is a server that communicates with malware installed on infected machines and sends commands or updates to them. A program is a piece of software that performs a specific task or function. A domain generated algorithm is implemented by a program that runs on the attacker's machine or the malware itself, and produces a large number of domain names based on some logic, such as date, time, seed, dictionary, etc. Reference: [Domain generation algorithm](#) Among cyber-attack techniques, what is a DGA?

Question: 44

Which two functions are available for both inline and API protection? (Choose two.)

- A. multi-factor authentication
- B. threat protection
- C. DLP
- D. Cloud Security Posture Management (CSPM)

Answer: BC

Explanation:

Netskope provides both inline and API protection for cloud applications and web traffic. Inline protection refers to the real-time inspection and enforcement of policies on the traffic between users and cloud applications, using Netskope's inline proxy mode. API protection refers to the retrospective inspection and enforcement of policies on the data that is already stored in cloud applications, using Netskope's API connectors. Two functions that are available for both inline and API protection are threat protection and DLP. Threat protection is the capability to detect and block malware, ransomware, phishing, and other cyber threats that may compromise cloud data or users. DLP is the capability to detect

and protect sensitive data, such as personal information, intellectual property, or regulated data, that may be exposed or leaked through cloud applications. Reference: [Netskope Inline Proxy Mode](#)[Netskope API Protection](#)[Netskope Threat Protection](#)[Netskope DLP Engine](#)

Question: 45

A customer wants to detect misconfigurations in their AWS cloud instances.

In this scenario, which Netskope feature would you recommend to the customer?

- A. Netskope Secure Web Gateway (SWG)
- B. Netskope Cloud Security Posture Management (CSPM)
- C. Netskope Advanced DLP and Threat Protection
- D. Netskope SaaS Security Posture Management (SSPM)

Answer: B

Explanation:

If a customer wants to detect misconfigurations in their AWS cloud instances, the Netskope feature that I would recommend to them is Netskope Cloud Security Posture Management (CSPM). Netskope CSPM 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 AWS and other cloud service providers 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 customer's security standards and best practices. Netskope CSPM can also alert, report, or remediate the misconfigurations automatically or manually. Reference: [Netskope CSPM Cloud Security Posture Management](#)

Question: 46

Which two use cases would be considered examples of Shadow IT within an organization? (Choose two.)

- A. a sanctioned Salesforce account used by a contractor to upload non-sensitive data
- B. a sanctioned Wettransfer being used by a corporate user to share sensitive data

- C. an unsanctioned Microsoft 365 OneDrive account being used by a corporate user to upload sensitive data
- D. an unsanctioned Google Drive account used by a corporate user to upload non-sensitive data

Answer: C, D

Explanation:

Shadow IT is the term for the unauthorized use of IT resources and functions by employees within an organization. It can include cloud services, software, and hardware that are not approved or managed by the IT department. Two use cases that would be considered examples of shadow IT within an organization are: an unsanctioned Microsoft 365 OneDrive account being used by a corporate user to upload sensitive data and an unsanctioned Google Drive account used by a corporate user to upload non-sensitive data. In both cases, the corporate user is using a personal cloud storage service that is not sanctioned by the organization to store work-related data. This can introduce security risks, such as data leakage, data loss, compliance violations, malware infections, etc. The IT department may not have visibility or control over these cloud services or the data stored in them. Reference: [What is shadow IT? | Cloudflare](#)[What is Shadow IT? | IBM](#)

Question: 47

In which scenario would you use a SAML reverse proxy?

- A. When the API-enabled protection exceeds the Cloud App API usage limits and cannot be used anymore.
- B. When the organization wants to perform inline inspection of cloud application traffic for roaming users that do not have the Netskope agent installed.
- C. When there are multiple SAML IdPs in use and the SAML reverse proxy can help federate them all together.
- D. When PAC files or explicit proxies can be used to steer traffic to the Netskope platform.

Answer: C

Explanation:

A SAML reverse proxy is a service that acts as an intermediary between a SAML service provider (SP) and one or more SAML identity providers (IdPs). It can perform various functions, such as authentication, authorization, load balancing, caching, etc. One scenario where you would use a SAML reverse proxy is when there are multiple SAML IdPs in use and the SAML reverse proxy can help federate them all together. For example, suppose you have an internal application that needs to authenticate users from different domains or organizations, each with their own SAML IdP. Instead of

configuring the application to trust each IdP separately, you can use a SAML reverse proxy to act as a single SP for the application and a single IdP for the users. The SAML reverse proxy can then redirect the users to their respective IdPs for authentication and relay the SAML assertions back to the application. This way, you can simplify the integration and management of multiple SAML IdPs and provide a seamless user experience. Reference: [SAML Reverse ProxyWhat is application proxy & SAML SSO?](#)

Question: 48

You need to provide a quick view under the Skope IT Applications page showing only risky shadow IT cloud applications being used.

In this scenario, which two filter combinations would you use to accomplish this task? (Choose two.)

- A. Sanctioned = No
- B. CCL = High. Under Research
- C. User Device Type = Windows Device
- D. CCL = Medium. Low, Poor

Answer: A, D

Explanation:

To provide a quick view under the Skope IT Applications page showing only risky shadow IT cloud applications being used, you can use two filter combinations: Sanctioned = No and CCL = Medium, Low, Poor. The Sanctioned filter allows you to select whether you want to see only sanctioned or unsanctioned apps in your organization. Sanctioned apps are those that are approved and managed by your IT department, while unsanctioned apps are those that are used without authorization or oversight by your employees. Shadow IT refers to the use of unsanctioned apps that may pose security or compliance risks for your organization. The CCL filter allows you to select the Cloud Confidence Level (CCL) ratings of the apps you want to see. The CCL rating is a measure of how enterprise-ready a cloud app is based on various criteria such as security, auditability, business continuity, etc. The CCL rating ranges from Excellent to Poor, with Excellent being the most secure and compliant and Poor being the least. Risky cloud apps are those that have a low CCL rating, such as Medium, Low, or Poor. By applying these two filters, you can narrow down the list of apps to only those that are unsanctioned and have a low CCL rating, which indicates that they are risky shadow IT cloud applications being used in your organization. Reference: [SkopeIT ApplicationsNetskope Cloud Confidence Index](#)

Question: 49

You want to prevent Man-in-the-Middle (MITM) attacks on an encrypted website or application. In this scenario, which method would you use?

- A. Use a stronger encryption algorithm.
- B. Use certificate pinning.
- C. Use a proxy for the connection.
- D. Use a weaker encryption algorithm.

Answer: B

Explanation:

To prevent Man-in-the-Middle (MITM) attacks on an encrypted website or application, one method that you can use is certificate pinning. Certificate pinning is a technique that restricts which certificates are considered valid for a particular website or application, limiting risk. Instead of allowing any trusted certificate to be used, operators "pin" the certificate authority (CA) issuer(s), public keys or even end-entity certificates of their choice. Certificate pinning helps to prevent MITM attacks by validating the server certificates against a hardcoded list of certificates in the website or application. If an attacker tries to intercept or modify the traffic using a fraudulent or compromised certificate, it will be rejected by the website or application as invalid, even if it is signed by a trusted CA. Reference: [Certificate pinning - IBM Certificate and Public Key Pinning | OWASP Foundation](#)

Question: 50

Exhibit

A Exhibit



Which portion of the interface shown in the exhibit allows an administrator to set severity, assign ownership, track progress, and perform forensic analysis with excerpts of violating content?

- A. Skope IT-> Alerts
- B. Incidents -> DLP
- C. API-enabled Protection -> Inventory
- D. Reports -> New Report

Answer: B

Explanation:

The portion of the interface shown in the exhibit that allows an administrator to set severity, assign ownership, track progress, and perform forensic analysis with excerpts of violating content is Incidents -> DLP. The Incidents dashboard provides a comprehensive view of all the incidents that have occurred in your cloud environment, such as DLP violations, malware infections, anomalous activities, etc. You can filter the incidents by various criteria, such as app name, incident type,

severity, user name, etc. You can also drill down into each incident to see more details, such as file name, file path, file owner, file size, file type, etc. You can also assign an owner to an incident, change its status and severity, add notes or comments, and view the excerpts of the violating content that triggered the DLP policy. Reference: [Netskope Incidents Dashboard](#)

Question: 51

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

- 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 onpremises 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: 52

Click the Exhibit button.

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

- 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 Port](#)[How to explain Source IP Address, Destination IP Address & Service in easy way](#)

Question: 53

Which three statements are correct about Netskope's NewEdge Security Cloud Network Infrastructure? (Choose three.)

- A. It takes advantage of the public cloud by deploying security services on Google Cloud Platform.
- B. It includes direct peering with Microsoft and Google in every data center.
- C. It is a private security cloud network that is massively over provisioned, highly elastic, and built for scale.
- D. It delivers a single, unified network with no surcharges or reliance on public cloud infrastructure or virtual PoPs.
- E. It simplifies the administrator's job by limiting access to pre-defined availability zones.

Answer: BCD

Explanation:

Netskope's NewEdge Security Cloud Network Infrastructure is a global network that powers the Netskope Security Cloud, providing real-time inline and out-of-band API-driven services for cloud and web security. Three statements that are correct about Netskope's NewEdge Security Cloud Network Infrastructure are:

It includes direct peering with Microsoft and Google in every data center. This means that Netskope has established high-speed, low-latency connections with these major cloud service providers, ensuring optimal performance and user experience for their customers. Direct peering also reduces the risk of network congestion, packet loss, or routing issues that may affect the quality of service.

It is a private security cloud network that is massively over provisioned, highly elastic, and built for scale. This means that Netskope owns and operates its own network infrastructure, without relying on third-party providers or public cloud platforms. Netskope has invested over \$150 million to build the world's largest and fastest security private cloud, with data centers in more than 65 regions and growing. Netskope can dynamically scale its network capacity and resources to meet the growing demand and traffic volume of its customers, without compromising on security or performance.

It delivers a single, unified network with no surcharges or reliance on public cloud infrastructure or virtual PoPs. This means that Netskope provides a consistent and transparent network service to its customers, regardless of their location or device. Netskope does not charge any additional fees or hidden costs for accessing its network services, unlike some other providers that may impose surcharges based on geography or bandwidth usage. Netskope also does not use virtual points of presence (PoPs) that are hosted on public cloud platforms, which may introduce latency, complexity, or security risks.

Reference: [Netskope NewEdgeNetskope NewEdge Data SheetNetskope SASE](#)

Question: 54

What are two pillars of CASB? (Choose two.)

- A. visibility
- B. compliance
- C. cloud native
- D. SASE

Answer: A, B

Explanation:

Two pillars of CASB are visibility and compliance. CASB stands for Cloud Access Security Broker, which is a solution that provides visibility and control over cloud services and web traffic, as well as data and threat protection for cloud users and devices. Visibility is the capability to identify all cloud services in use and assess their risk factors, such as security, auditability, business continuity, etc. Compliance is the capability to ensure that cloud services and data meet the regulatory standards and policies of the organization or industry, such as GDPR, HIPAA, PCI DSS, etc. Reference: [What Is a Cloud Access Security Broker \(CASB\)? | Microsoft Edge](#)
[CASB Guide: What are the 4 Pillars of CASB? - Security Service](#)

Question: 55

You want to set up a Netskope API connection to Box.

What two actions must be completed to enable this connection? (Choose two.)

- A. Install the Box desktop sync client.
- B. Authorize the Netskope application in Box.
- C. Integrate Box with the corporate IdP.
- D. Configure Box in SaaS API Data protection.

Answer: BD

Explanation:

To set up a Netskope API connection to Box, two actions that must be completed are: authorize the Netskope application in Box and configure Box in SaaS API Data protection. Authorizing the Netskope application in Box allows Netskope to access the Box API and perform out-of-band inspection and enforcement of policies on the data that is already stored in Box. Configuring Box in SaaS API Data protection allows you to specify the Box instance details, such as domain name, admin email, etc., and enable features such as retroactive scan, event stream, etc. Reference: [Authorize Netskope Introspection App on Box Enterprise - Netskope Knowledge Portal](#)[Configure Box Instance in Netskope UI - Netskope Knowledge Portal](#)

Question: 56

When using an out-of-band API connection with your sanctioned cloud service, what are two capabilities available to the administrator? (Choose two.)

- A. to quarantine malware
- B. to find sensitive content
- C. to block uploads
- D. to allow real-time access

Answer: AB

Explanation:

When using an out-of-band API connection with your sanctioned cloud service, two capabilities available to the administrator are: to quarantine malware and to find sensitive content. An out-of-band API connection is a method of integrating Netskope with your cloud service provider using the APIs exposed by the cloud service. This allows Netskope to access the data that is already stored in the cloud service and perform retrospective inspection and enforcement of policies. One capability that the administrator can use with an out-of-band API connection is to quarantine malware. This means that Netskope can scan the files in the cloud service for malware, ransomware, phishing, and other threats, and move them to a quarantine folder or delete them if they are found to be malicious. Another capability that the administrator can use with an out-of-band API connection is to find sensitive content. This means that Netskope can scan the files in the cloud service for sensitive data, such as personal information, intellectual property, or regulated

data, and apply data loss prevention (DLP) policies to protect them. For example, Netskope can encrypt, redact, or watermark the files that contain sensitive content, or notify the administrator or the file owner about the exposure.

Reference: [Netskope API ProtectionReal-time Control and Data Protection via Out-of-Band API](#)

Question: 57

You want to block access to sites that use self-signed certificates. Which statement is true in this scenario?

- A. Certificate-related settings apply globally to the entire customer tenant.
- B. Certificate-related settings apply to each individual steering configuration level.
- C. Certificate-related settings apply to each individual client configuration level.
- D. Self-signed certificates must be changed to a publicly trusted CA signed certificate.

Answer: B

Explanation:

The statement that is true in this scenario is: Certificate-related settings apply to each individual steering configuration level. Certificate-related settings are the options that allow you to configure how Netskope handles SSL/TLS certificates for encrypted web traffic. For example, you can choose whether to allow or block self-signed certificates, expired certificates, revoked certificates, etc. You can also choose whether to enable SSL decryption for specific domains or categories. Certificate-related settings apply to each individual steering configuration level, which means that you can have different settings for different types of traffic or devices. For example, you can have one steering configuration for managed devices and another one for unmanaged devices, and apply different certificate-related settings for each one.

This allows you to customize your security policies based on your needs and preferences. Reference: [Netskope SSL DecryptionNetskope Steering Configuration](#)

Question: 58

How do you provision users to your customer's Netskope tenant? (Choose two.)

- A. Use Microsoft Intune.
- B. Use the AD Connector.
- C. Use SCIM.

D. Use the Directory Importer.

Answer: B, D

Explanation:

To provision users to your customer's Netskope tenant, two methods that you can use are: use the AD Connector and use SCIM. The AD Connector is a tool that allows you to synchronize users and groups from your Active Directory (AD) domain to your Netskope tenant. The AD Connector runs as a Windows service on a machine that has access to your AD domain controller. The AD Connector periodically queries your AD domain for any changes in users and groups and updates them in your Netskope tenant accordingly. The AD Connector also supports filtering users and groups based on attributes or organizational units (OUs). SCIM stands for System for Cross-domain Identity Management, which is a standard protocol for managing user identities across different applications and services. SCIM allows you to provision users and groups from your identity provider (IdP), such as Azure AD or Okta, to your Netskope tenant using APIs. SCIM also supports creating, updating, deleting, and searching users and groups in your Netskope tenant based on your IdP's configuration. Reference: [Netskope AD Connector User Provisioning with Azure AD](#)

Question: 59

When would an administrator need to use a tombstone file?

- A. You use a tombstone file when a policy causes a file download to be blocked.
- B. You use a tombstone file when a policy causes a publicly shared file to be encrypted.
- C. You use a tombstone file when the policy causes a file to be moved to quarantine.
- D. You use a tombstone file when a policy causes a file to be moved to legal hold.

Answer: C

Explanation:

A tombstone file is a placeholder file that replaces the original file when it is moved to quarantine by a Netskope policy. The tombstone file contains information about the original file, such as its name, size, type, owner, and the reason why it was quarantined. The tombstone file also provides a link to the Netskope UI where the administrator or the file owner can view more details about the incident and take appropriate actions, such as restoring or deleting the file. The purpose of using a tombstone file is to preserve the metadata and location of the original file, as well as to notify the users about the quarantine action and how to access the file if needed. Reference: [Threat Protection - Netskope](#)

Question: 60

You have an issue with the Netskope client connecting to the tenant.

In this scenario, what are two ways to collect the logs from the client machine? (Choose two.)

- A. from the Netskope client UI About page
- B. from the command line using the nsdiag command
- C. from the Netskope client system tray icon
- D. from the Netskope client UI Configuration page

Answer: A, B

Explanation:

To collect the logs from the client machine when you have an issue with the Netskope client connecting to the tenant, two ways that you can use are: from the Netskope client UI About page and

from the command line using the nsdiag command. From the Netskope client UI About page, you can click on the "Collect Logs" button to generate a zip file containing all the relevant logs and configuration files from the client machine. You can then send this zip file to Netskope support for troubleshooting. From the command line, you can use the nsdiag command with various options to collect different types of logs and diagnostic information from the client machine. For example, you can use nsdiag -l to collect all logs, nsdiag -c to collect configuration files, nsdiag -t to collect traffic statistics, etc. You can also use nsdiag -h to see all available options and usage instructions. You can then send the output files to Netskope support for troubleshooting. Reference: [Netskope Client Configuration overviewInstall and Test the Client - Netskope Knowledge Portal](#)

Question: 61

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.)

- 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: 62

As an administrator, you are asked to monitor the status of your IPsec and GRE tunnels.

In the Netskope Admin UI, which two sections would you use in this scenario? (Choose two.)

- A. Steering Configuration page under Settings
- B. Bandwidth Consumption module of Digital Experience Management
- C. Network Steering page of Digital Experience Management
- D. IPsec Site and GRE Site pages under Settings

Answer: A, D

Explanation:

Steering Configuration page under Settings (A):

The Steering Configuration page under Settings is used to configure and manage the steering policies, including IPsec and GRE tunnels. This section provides the necessary tools to configure the network traffic routing and ensures that the configurations are set according to the organization's requirements.

IPsec Site and GRE Site pages under Settings (D):

These specific pages under the Settings section allow administrators to monitor and manage the status of IPsec and GRE tunnels. They provide detailed information about the tunnel configurations, status, and other metrics that are essential for maintaining the health and performance of the network connections.

These details are confirmed based on the features and configurations available within the Netskope Admin UI settings, as documented in the Netskope Knowledge Portal.

Question: 63

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

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

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

Answer: C

Explanation:

The Application Events page in the SkopelT 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.

Reference:

REST API v2 Overview - Netskope Knowledge Portal

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

Postman Collection for Netskope API

Question: 64

Click the Exhibit button.

The screenshot shows the 'Exhibit' page in the Microsoft 365 Security & Compliance Center. The page is titled 'Exhibit' and has a 'CONTENT' tab selected. Under the 'CONTENT' tab, there is a section titled 'FILE SHARING OPTIONS TO SCAN'. This section has two radio buttons: 'All Sharing Options' and 'Specific Sharing Options'. The 'Specific Sharing Options' radio button is selected. Below these radio buttons, there are three checkboxes: 'Private', 'Public', and 'Shared Internally'. The 'Shared Internally' checkbox is selected. Below these checkboxes, there is a section titled 'ADVANCED OPTIONS'. Under 'ADVANCED OPTIONS', there is a checkbox for 'Shared Externally', which is also selected. Below 'Shared Externally', there is a 'DOMAIN' section with a dropdown menu set to 'All External Domains'. Below the dropdown menu, there is another 'ADVANCED OPTIONS' section.

A customer has created a CASB API-enabled Protection policy to detect files containing sensitive data that are shared outside of their organization.

Referring to the exhibit, which statement is correct?

A. The administrator needs to use Shared Externally as the only shared option.

B. The administrator needs to use Shared Externally and Public as the shared options.

C. The administrator must select Private as the only shared option.

D. The administrator needs to use Public as the only shared option.

Answer: B

Explanation:

To detect files containing sensitive data that are shared outside of the organization, the administrator should select both "Shared Externally" and "Public" sharing options. These settings ensure that any files shared externally (outside the organization) or publicly are scanned for sensitive data. This comprehensive approach covers all potential scenarios where data could be exposed outside the organization.

Step-by-Step Configuration:

Select Specific Sharing Options:

Navigate to the CASB API-enabled Protection policy configuration page.

Choose the option for "Specific Sharing Options" to limit the scan to files shared under certain conditions.

Enable Shared Externally and Public:

Check both "Shared Externally" and "Public" options. This setting ensures that files shared either publicly or with external domains are included in the scan.

Configure Advanced Options:

For further granularity, configure the advanced options under each sharing type if needed (e.g., specifying particular external domains).

This configuration aligns with the best practices for CASB policies and ensures that all files potentially leaving the organization are scanned for sensitive data.

Reference:

Netskope CASB Policy Configuration Documentation

Question: 65

Which statement is correct about Netskope's Instance Awareness?

A. It prevents users from browsing the Internet using outdated Microsoft Internet Explorer but allows them access if they use the latest version of Microsoft Edge.

B. It identifies that a form hosted in Microsoft Forms belongs to the corporate Microsoft 365 tenant and not a

tenant from a third party.

C. It differentiates personal code from work-related code being uploaded to GitHub.

D. It identifies if e-mails are being sent using Microsoft 365 through Outlook, Thunderbird, or the Web application in outlook.com.

Answer: B

Explanation:

Instance Awareness in Netskope provides visibility and control over instances of applications used by the organization. Specifically, it helps in differentiating between corporate and personal instances of the same application. This feature is particularly crucial in ensuring that corporate data is not uploaded to personal instances of applications and vice versa.

For example, it can identify that a form hosted in Microsoft Forms belongs to the corporate Microsoft 365 tenant, thereby preventing data from being mistakenly or maliciously sent to a third-party tenant. This ensures that only authorized instances of applications are used for corporate data, maintaining data security and compliance.

Reference:

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

REST API v2 Overview - Netskope Knowledge Portal

Using the REST API v2 dataexport Iterator Endpoints - Netskope Knowledge Portal

Question: 66

You added a new private app definition and created a Real-time Protection policy to allow access for all users. You have a user who reports that they are unable to access the application but all other applications work fine.

Which statement correctly describes how to troubleshoot this issue using the Netskope Web UI?

A. You can verify the user's policy, steering configuration, client status and other relevant details using the Advanced Debugging tools in the Netskope Client.

B. You can verify the user's policy, steering configuration, client status and other relevant details using the App Discovery dashboard.

C. You can verify the user's policy, steering configuration, client status and other relevant details using DEM.

D. You can verify the user's policy, steering configuration, client status and other relevant details using the NPA

Troubleshooter tool

Answer: D

Explanation:

When a user is unable to access a newly added private application despite having the correct Realtime Protection policy in place, the NPA (Netskope Private Access) Troubleshooter tool can be used to diagnose and resolve the issue.

Accessing NPA Troubleshooter:

Navigate to the Netskope Web UI.

Go to the Troubleshooting section and select NPA Troubleshooter.

Verifying User Policy:

Check the specific policy applied to the user to ensure that it allows access to the application.

Ensure that there are no conflicting policies that might be blocking access.

Checking Steering Configuration:

Verify that the steering configuration is correctly set up to route the user's traffic to the Netskope platform.

Ensure that the correct gateways are being used and that the traffic is not being bypassed.

Client Status:

Confirm that the Netskope client is installed and running on the user's device.

Check the client logs for any errors or issues that might be preventing access.

Additional Details:

Review any other relevant details such as the user's network configuration, device status, and any recent changes that might have impacted connectivity.

By systematically using the NPA Troubleshooter tool to verify these aspects, you can identify and resolve the underlying issue preventing access to the private application.

Reference:

[REST API v2 Overview - Netskope Knowledge Portal](#)

[Using the REST API v2 dataexport Iterator Endpoints - Netskope Knowledge Portal](#)

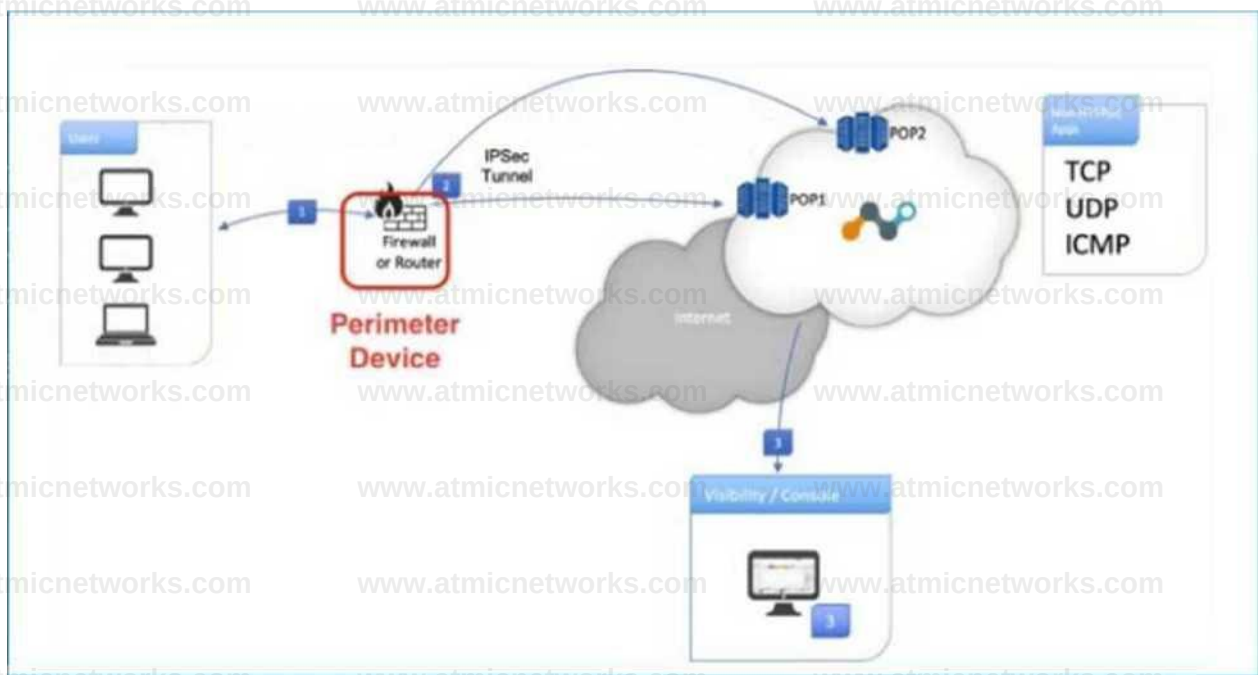
[Using the REST API v2 UCI Impact Endpoints - Netskope Knowledge Portal](#)

netskopesdk · PyPI

[Netskope Rest APIv2\(OAS 3.1\) - Postman Collection](#)

Question: 67

Click the Exhibit button.



Referring to the exhibit, what are two recommended steps to be set on the perimeter device to monitor IPsec tunnels to a Netskope data plane? (Choose two.)

- A. Enable IKE Dead Peer Detection (DPD) for each tunnel.
- B. Send ICMP requests to the Netskope location's Probe IP.
- C. Send HTTP requests to the Netskope location's Probe IP.
- D. Send ICMP requests to the Netskope location's proxy IPs.

Answer: A, B

Explanation:

To monitor IPsec tunnels to a Netskope data plane, it is essential to ensure the stability and responsiveness of the tunnels. The recommended steps involve enabling monitoring mechanisms that detect and respond to tunnel failures. Here's a detailed explanation of the two recommended steps:

Enable IKE Dead Peer Detection (DPD) for each tunnel:

Explanation: IKE Dead Peer Detection (DPD) is a method used to detect if the peer (remote endpoint of the tunnel) is no longer available or reachable. By enabling DPD, the device can automatically

detect and tear down the IPsec tunnel if the peer does not respond, allowing for quick reestablishment of the tunnel if needed.

Implementation: Configure DPD in the IPsec settings of the perimeter device. This ensures that if the Netskope data plane is unreachable, the tunnel is automatically terminated and re-negotiated.

Send ICMP requests to the Netskope location's Probe IP:

Explanation: Sending ICMP requests (ping) to the Netskope location's Probe IP helps in monitoring the availability and latency of the connection to the Netskope data plane. If the ICMP requests fail, it indicates a potential issue with the connectivity.

Implementation: Set up regular ICMP requests (ping) from the perimeter device to the Netskope Probe IPs. This allows for continuous monitoring of the tunnel's health and immediate detection of connectivity issues.

Reference:

[REST API v2 Overview - Netskope Knowledge Portal](#)

[Using the REST API v2 dataexport Iterator Endpoints - Netskope Knowledge Portal](#)

[Using the REST API v2 UCI Impact Endpoints - Netskope Knowledge Portal](#)

Question: 68

Click the Exhibit button.



What are two use cases where the parameter shown in the exhibit is required? (Choose two.)

- A. When you create a policy to prevent file transfer between a sanctioned Google Drive and personal Google Drive.
- B. When you share the JoC between a third-party security solution and the Threat Protection Profile.
- C. When you create a policy to prevent binary files larger than 5 MB that are shared publicly on a sanctioned OneDrive.
- D. When you share Incident details about files detected in a DLP incident.

Answer: A, C

Explanation:

The parameter shown in the exhibit (File Profile) is crucial in policies where file type, size, and other attributes need to be specified. Here are two use cases where this parameter is required:

When you create a policy to prevent file transfer between a sanctioned Google Drive and personal Google Drive:

Explanation: In this use case, the File Profile is used to define the types of files that are not allowed

to be transferred between different Google Drive instances. By specifying the file types in the policy, administrators can

ensure that sensitive corporate data is not transferred to personal accounts.

Implementation: Create a new File Profile with the desired file types and apply this profile in the policy that governs the data transfer rules between sanctioned and personal Google Drive instances.

When you create a policy to prevent binary files larger than 5 MB that are shared publicly on a sanctioned OneDrive:

Explanation: This use case involves creating a policy that restricts the sharing of large binary files (e.g., executable files) on publicly accessible folders in OneDrive. The File Profile parameter allows defining the file size and type criteria.

Implementation: Define a File Profile that specifies binary files and sets a size limit (e.g., 5 MB). Apply this profile in the policy to prevent such files from being shared publicly.

Reference:

[REST API v2 Overview - Netskope Knowledge Portal](#)

[Using the REST API v2 dataexport Iterator Endpoints - Netskope Knowledge Portal](#)

[Using the REST API v2 UCI Impact Endpoints - Netskope Knowledge Portal](#)

netskopesdk · PyPI

[Netskope Rest APIv2\(OAS 3.1\) - Postman Collection](#)

Question: 69

Click the Exhibit button.

Exhibit

Source

Destination

Profile & Action

Access Methods = Explicit Proxy

ADD CRITERIA ▾

Category
Category = Webmail

ACTIVITIES & CONSTRAINTS
Any

ADD CRITERIA ▾

Action: Block

ADD PROFILE ▾

policy that has a predefined webmail category blocked. However the user is still able to access Yahoo mail.

- A. The user is not part of the correct AD group or OU.
- B. The user is not steered using an explicit proxy.
- C. The webmail category does not include Yahoo mail when using an explicit proxy
- D. The user's AD group must be added to the policy.

Answer: C

Explanation:

The given exhibit shows an inline policy blocking the predefined webmail category via an explicit proxy. However, the user can still access Yahoo Mail, indicating that Yahoo Mail is not included in the webmail category when using an explicit proxy.

Policy Configuration:

The policy is set to block access to the webmail category through an explicit proxy.

The action for this policy is 'Block'.

Understanding the Webmail Category:

Netskope's predefined categories may not always cover all services under a category, especially when it comes to specific configurations like explicit proxy.

The webmail category in the policy might not have included Yahoo Mail when using explicit proxy configurations.

Checking the Category Definitions:

It is important to verify what URLs or services are included under the "webmail" category in the Netskope administration console.

Administrators can check the category definitions and manually add Yahoo Mail if it's not included by default.

Reference:

[REST API v2 Overview - Netskope Knowledge Portal](#)

[Using the REST API v2 dataexport Iterator Endpoints - Netskope Knowledge Portal](#)

[Using the REST API v2 UCI Impact Endpoints - Netskope Knowledge Portal](#)

netskopesdk · PyPI

[Netskope Rest APIv2\(OAS 3.1\) - Postman Collection](#)

Question: 70

A Netskope administrator wants to create a policy to quarantine files based on sensitive content.

In this scenario, which variable must be included in the policy to achieve this goal?

- A. Organizational Unit
- B. Cloud Confidence Index level
- C. DLP Profile
- D. Threat Protection Profile

Answer: C

Explanation:

To create a policy to quarantine files based on sensitive content in Netskope, you need to include the DLP Profile variable. Here's a detailed explanation of the steps involved:

Access Netskope Admin Console: First, log in to your Netskope admin console.

Navigate to Policies: Go to the Policies section where you can create and manage different types of policies.

Create a New Policy: Click on the option to create a new policy. Select the type of policy you want to create. In this case, it will be a Data Loss Prevention (DLP) policy.

Define Policy Criteria: Define the criteria for your policy. This includes specifying the conditions under which files should be quarantined. You will need to include sensitive content detection as part of the criteria.

Include DLP Profile: The most crucial step is to include a DLP Profile in your policy. The DLP Profile will define the sensitive content that the policy will monitor for. Netskope provides various predefined DLP profiles that you can use, or you can create custom DLP profiles based on your organization's needs.

Set Action to Quarantine: Specify the action to be taken when the policy criteria are met. In this case, you want to quarantine the files. Select the "Quarantine" action from the available options.

Save and Apply Policy: Once you have configured the policy with the DLP profile and action, save the policy and apply it to the relevant users, groups, or organizational units.

Reference:

Netskope Knowledge Portal: Using DLP Profiles and Policies.

Question: 71

You are attempting to allow access to an application using NP

A. Private Apps steering is already enabled for all users.

In this scenario, which two actions are required to accomplish this task? (Choose two.)

A. Disable Cloud & Firewall Apps in Steering Config.

B. Create a Real-time Protection "Allow" policy for the Private App.

C. Create a Private App.

D. Ensure that SSO is in place.

Answer: B, C

Explanation:

To allow access to an application using Netskope Private Access (NPA) with Private Apps steering already enabled for all users, follow these steps:

Create a Private App:

Go to the Netskope admin console.

Navigate to the Private Access section.

Create a new Private App by specifying the necessary details such as app name, IP address, ports, and protocols. This step is essential for defining the private application that users will access through NPA.

Create a Real-time Protection "Allow" Policy:

Navigate to the Policies section in the Netskope admin console.

Create a new Real-time Protection policy.

Set the policy action to "Allow".

Define the criteria for the policy to match the traffic directed to the newly created Private App.

Apply the policy to the relevant users or groups to ensure that access to the Private App is allowed.

Ensure Other Required Settings:

Ensure that SSO (Single Sign-On) is properly configured if it is needed for user authentication.

Verify that Private App steering is enabled for all users, which might already be the case as per the scenario.

Reference:

Netskope API Documentation: Configuring Private Apps and Real-time Protection Policies.

By following these steps, you ensure that the private app is properly defined and that users are allowed to access it through the appropriate Real-time Protection policies. This approach leverages Netskope's capabilities to manage and secure access to private applications seamlessly.

Question: 72

Your organization has recently implemented Netskope Private Access. During an investigation, your security team has asked you to provide a list of all hosts including domains and IP addresses that a user accessed through Netskope Private Access for the past seven days.

Which two locations in the Netskope Web UI would allow you to obtain and export the requested data? (Choose two.)

- A. Private Apps page in SkopeIT
- B. Users page in SkopeIT
- C. Network Events page in SkopeIT
- D. Transaction Events collection in Advanced Analytics

Answer: AC

Explanation:

To obtain and export a list of all hosts including domains and IP addresses that a user accessed through Netskope Private Access for the past seven days, you can follow these steps:

Access the Netskope Web UI: Log in to your Netskope admin console.

Navigate to SkopeIT:

Go to the SkopeIT section in the Netskope admin console.

Private Apps page in SkopeIT:

In the SkopeIT section, navigate to the "Private Apps" page.

Here, you can find detailed information about the private applications accessed by users, including the domains and IP addresses.

Use the filter options to specify the user and the time range (past seven days).

Export the data as needed for your investigation.

Network Events page in SkopeIT:

In the SkopeIT section, navigate to the "Network Events" page.

This page provides a comprehensive list of network events, including details about the hosts accessed through Netskope Private Access.

Again, use the filter options to specify the user and the time range.

Export the data for reporting purposes.

These two locations within the SkopeIT section of the Netskope Web UI will provide you with the necessary data to meet your security team's requirements.

Reference:

Netskope Knowledge Portal: Using SkopeIT for Network and Private Apps Analysis.

Question: 73

Click the Exhibit button.



Referring to the exhibit, you have a user reporting that a blocked website is needed for legitimate business reasons.

Upon review, you determine that the user has been blocked by the Global Block policy. You need to create an exception for that domain. You create a custom URL list that includes the domain.

In this scenario, which two actions would allow this access? (Choose two.)

- A. Create a custom category with the custom URL list as an included URL list and add it to an allow policy below the triggered Global Block policy.
- B. Create a custom category with the custom URL list as an included URL list and add it to an allow policy above the triggered Global Block policy.
- C. Add the custom URL list as an excluded URL list to the category in the Global Allow policy.
- D. Add the custom URL list as an excluded URL list to the category in the Global Block policy.

Answer: B, C

Explanation:

Identify the Blocked Policy: According to the exhibit, the website is blocked by the "Global Block Policy."

Create a Custom URL List: To create an exception for the domain, you need to first create a custom URL list that includes the domain in question.

Navigate to the URL List section in the Netskope UI.

Create a new URL list and add the domain that needs to be allowed.

Option B: Create a custom category with the custom URL list as an included URL list and add it to an allow policy above the Global Block policy.

Go to the Policy section in the Netskope UI.

Create a new policy, ensuring it is an "Allow" policy.

Add the custom category to this allow policy.

Position this allow policy above the Global Block policy to ensure it takes precedence.

This ensures that the URLs in the custom list are allowed before the Global Block policy is evaluated.

Option C: Add the custom URL list as an excluded URL list to the category in the Global Block policy.

Edit the existing Global Block policy.

Add the custom URL list to the excluded URL list section of this policy.

This will exclude the URLs in the custom list from being blocked by the Global Block policy.

Reference:

Refer to the Netskope Knowledge Portal for managing custom URL lists and policy configurations.

Question: 74

Which two capabilities are part of Netskope's Adaptive Zero Trust Data Protection? (Choose two.)

- A. contextual risk awareness
- B. continuous adaptive policies
- C. continuous enforcement of all policies
- D. contextual metadata storage

Answer: A, B

Explanation:

Adaptive Zero Trust Data Protection Overview:

Netskope's Adaptive Zero Trust Data Protection ensures that data is protected based on continuous risk assessments and adaptive policies that respond to changing contexts and threats.

Contextual Risk Awareness:

This capability involves understanding the context around data access and usage to assess risk dynamically.

Netskope leverages various signals such as user behavior, device security posture, location, and other factors to gauge risk levels.

By continuously evaluating these factors, Netskope can enforce appropriate security measures in real-time.

Continuous Adaptive Policies:

Policies in the Netskope platform adapt continuously based on the assessed risk and changing contexts.

These policies are not static; they evolve based on ongoing risk assessments and threat intelligence.

Adaptive policies ensure that security measures are always aligned with the current threat landscape and

organizational requirements.

Reference:

For detailed capabilities and how they are implemented, refer to the Netskope documentation on Adaptive Zero Trust Data Protection.

Question: 75

What are two supported ways to provision users to your customer's Netskope tenant? (Choose two.)

- A. Use Microsoft Intune.
- B. Use the AD Connector.
- C. Use SCIM.
- D. Use the Directory Importer.

Answer: B, C

Explanation:

AD Connector:

The AD Connector is used to integrate your Netskope tenant with Active Directory (AD) to provision and synchronize user accounts.

It ensures that user information in Netskope is always up-to-date by periodically synchronizing with AD.

To set up the AD Connector:

Navigate to Settings > Tools > Directory Importer.

Configure the AD Connector with your AD details.

Set the synchronization schedule.

This method is commonly used in enterprise environments where AD is the primary user directory.

SCIM (System for Cross-domain Identity Management):

SCIM is an open standard for automating the exchange of user identity information between identity domains or IT systems.

Netskope supports SCIM for provisioning users from identity providers like Okta, Azure AD, and others.

To configure SCIM:

Go to Settings > Tools > SCIM.

Follow the instructions to set up SCIM with your identity provider.

SCIM is beneficial for environments using modern identity management solutions.

Reference:

For detailed configuration steps and additional information, refer to the Netskope documentation on provisioning users using the AD Connector and SCIM.

Question: 76

All users are going through Netskope's Next Gen SWG. Your CISO requests a monthly report of all users who are accessing cloud applications with a "Low" or a "Poor" CCL, where the activity is either "Edit" or "Upload".

Using the Advanced Analytics interface, which two statements describe which actions must be performed in this scenario? (Choose two.)

- A. Create a report using the Data Collection "Page Events", filtering on the activities "Edit" and "Upload" for cloud apps with CCL values of "Low" or "Poor".
- B. Schedule a report with a monthly recurrence to be sent by e-mail with the attached PDF document at the end of each month.
- C. Create a report using the Data Collection "Application Events" filtering on the activities "Edit" and "Upload" for cloud apps with CCL values of "Low" or "Poor".
- D. Schedule a report with a monthly recurrence to be sent by SMS with the attached PDF document at the end of each month.

Answer: A, B

Explanation:

Create the Report in Advanced Analytics:

Data Collection:

Use the "Page Events" data collection, which captures detailed user activities on web pages, including edits and uploads.

Filters:

Apply filters to include only the activities "Edit" and "Upload".

Add another filter for the Cloud Confidence Level (CCL) to include only those with "Low" or "Poor" ratings.

This ensures the report focuses on the specified user activities within cloud applications that have lower security ratings.

Steps:

Navigate to Advanced Analytics > Reports.

Create a new report and select "Page Events" as the data collection source.

Apply the necessary filters for activities and CCL values.

Schedule the Report:

Monthly Recurrence:

Set the report to run on a monthly schedule to ensure regular updates.

Configure the report to be sent via email with a PDF attachment.

Steps:

In the report scheduling options, set the recurrence to monthly.

Specify the email recipients, ensuring the CISO receives the report.

Select PDF as the report format.

Reference:

For more details on creating and scheduling reports, refer to the Netskope documentation on Advanced Analytics and report generation.

Question: 77

Users are connecting to sanctioned cloud applications from public computers, such as from a hotel business center.

Which traffic steering method would work in this scenario?

- A. proxy chaining
- B. IPsec/GRE tunnel
- C. reverse proxy
- D. steering client

Answer: C

Explanation:

Reverse Proxy Overview:

A reverse proxy allows users to access sanctioned cloud applications securely from public or untrusted networks.

It ensures that the traffic is inspected and policy controls are enforced before reaching the cloud application.

Scenario Justification:

Users connecting from public computers, such as those in hotel business centers, cannot have a steering client installed, and IPsec/GRE tunnels are not feasible.

Proxy chaining requires control over the client's browser settings, which is not possible in this scenario.

A reverse proxy can handle the traffic without requiring configuration changes on the public computer.

Implementation:

Configure the reverse proxy to handle traffic for sanctioned applications.

Ensure the reverse proxy settings are enforced via your organization's security policies.

Reference:

Detailed configurations and use cases can be found in the Netskope documentation on reverse proxy solutions.

Question: 78

You determine that a business application uses non-standard HTTPS ports. You want to steer all HTTPS traffic for this application and have visibility and control over user activities.

Which action will allow you to accomplish this task?

- A. Create a steering exception for the application's domain and ports.
- B. Define a Private Agg for the application's domain and ports.
- C. Configure Non-standard ports in the Steering Configuration.
- D. Select All Traffic in the Steering Configuration.

Answer: C

Explanation:

Identify Non-standard HTTPS Ports:

Determine the specific non-standard HTTPS ports used by the business application.

Create a Steering Exception:

Navigate to the Netskope admin console.

Go to the steering configuration section and create a new steering exception.

Specify the domain of the business application and include the non-standard HTTPS ports.

This exception will ensure that traffic to this application is steered correctly for inspection and control.

Configure Non-standard Ports in the Steering Configuration:

Go to the steering configuration settings.

Add the identified non-standard HTTPS ports to ensure that all traffic using these ports is captured and inspected.

This ensures comprehensive visibility and control over the user activities on the application.

Reference:

For more details on steering configurations and managing exceptions, refer to the Netskope documentation on steering traffic and configuring non-standard ports.

Question: 79

Which Netskope platform component uses NewEdge Traffic Management for traffic steering?

- A. Cloud Exchange
- B. Client

- C. Data Plane On-Premises
- D. Explicit Proxy Over Tunnel

Answer: B

Explanation:

NewEdge Traffic Management:

NewEdge is Netskope's high-performance global network designed to deliver fast and secure access to the internet and cloud applications.

NewEdge Traffic Management ensures efficient routing and traffic steering for optimal performance and security.

Client Integration:

The Netskope Client uses NewEdge Traffic Management to steer traffic securely to the Netskope cloud.

It ensures that user traffic is routed through the best possible path for performance and security.

The Client component is responsible for redirecting user traffic to the NewEdge network, applying security policies, and ensuring secure access.

Reference:

For detailed information on NewEdge Traffic Management and how the Netskope Client utilizes it, refer to the Netskope documentation on traffic management and client configuration.

Question: 80

How do you protect your data at rest intellectual property (IP), such as source code or product designs, stored in Microsoft 365 SharePoint?

- A. by configuring Netskope Explicit Proxy in the user's browser
- B. by steering SharePoint traffic over GRE or IPsec to a Netskope cloud proxy
- C. by using Netskope's API-enabled Protection for SharePoint
- D. by steering SharePoint traffic using the Netskope Client

Answer: C

Explanation:

Protecting Data at Rest in SharePoint:

Protecting intellectual property stored in Microsoft 365 SharePoint requires a solution that can monitor and control data access and usage.

Netskope's API-enabled Protection integrates directly with Microsoft 365 to provide comprehensive security for data at rest.

API-enabled Protection:

Netskope's API-enabled Protection allows direct integration with SharePoint, enabling continuous monitoring and enforcement of security policies.

It ensures that data such as source code or product designs are protected from unauthorized access and potential data breaches.

Configuration:

Configure API-enabled Protection by navigating to the Netskope admin console.

Set up the necessary API integrations with Microsoft 365 SharePoint.

Define security policies to monitor and control access to sensitive data stored in SharePoint.

Reference:

For more details on setting up and configuring API-enabled Protection for SharePoint, refer to the Netskope documentation on API-enabled protection solutions.

Question: 81

You want to determine which NewEdge data planes that your remote users have been recently using.

Which area of the Netskope Tenant UI would provide this information?

- A. Client Steering under Digital Experience Management
- B. Network Steering under Digital Experience Management
- C. Users page under Settings
- D. Devices page under Settings

Answer: A

Explanation:

NewEdge Data Planes Monitoring:

To determine which NewEdge data planes your remote users have been using, you need to access the relevant monitoring section in the Netskope Tenant UI.

Client Steering under Digital Experience Management:

The Client Steering section under Digital Experience Management provides detailed information on how traffic is being steered for remote users.

This section includes insights into the NewEdge data planes being utilized by users.

Steps:

Navigate to Digital Experience Management in the Netskope Tenant UI.

Select Client Steering to view detailed reports and logs on traffic steering.

Analyze the data to identify the NewEdge data planes used by remote users recently.

Reference:

For more details on accessing and using the Client Steering section under Digital Experience Management, refer to the Netskope documentation on digital experience management and client steering.

Question: 82

How does a cloud security solution achieve visibility into TLS/SSL-protected Web traffic?

- A. by altering the TLS handshake and forcing the website to use a weak encryption algorithm which can be brute-forced
- B. by altering the TLS handshake and forcing the website to use insecure (HTTP) access
- C. by performing the TLS handshake on behalf of the website and replacing the site's certificate with its own
- D. by using government-issued universal decryption keys for the ciphers

Answer: C

Explanation:

TLS/SSL Inspection:

Cloud security solutions achieve visibility into TLS/SSL-protected web traffic through a process known as TLS/SSL interception or inspection.

How It Works:

The security solution acts as an intermediary (man-in-the-middle) during the TLS handshake.

When a user initiates a connection to a TLS/SSL-protected website, the security solution intercepts this connection.

It completes the TLS handshake with the user's device using its own certificate, and simultaneously performs the handshake with the destination website.

Certificate Replacement:

The security solution decrypts the traffic, inspects it, and then re-encrypts it before forwarding it to the destination website.

The user's browser trusts the security solution's certificate, which replaces the original website's certificate.

Security Implications:

This method allows the security solution to inspect encrypted traffic for threats or policy violations while maintaining secure communication.

Reference:

Detailed explanations and implementation steps can be found in Netskope documentation on SSL/TLS inspection.

Question: 83

You want to see the actual data that caused the policy violation within a DLP Incident view.

In this scenario, which profile must be set up?

- A. Quarantine Profile
- B. Forensics Profile
- C. Legal Hold Profile
- D. a GDPR DLP Profile

Answer: B

Explanation:

DLP Incident View:

To see the actual data that caused a policy violation within a DLP incident, detailed logging and data capture are required.

Forensics Profile:

A Forensics Profile in Netskope is designed to capture and store detailed information about policy violations, including the actual data that triggered the incident.

It provides a comprehensive view of the incident for investigation and compliance purposes.

Setup Process:

Navigate to the DLP settings in the Netskope admin console.

Configure a Forensics Profile to capture detailed logs and data for policy violations.

Ensure that this profile is associated with the relevant DLP policies.

Reference:

For detailed configuration steps, refer to the Netskope documentation on setting up Forensics Profiles for DLP incidents.

Question: 84

What are two correct methods to gather logs from the Netskope Client? (Choose two.)

- A. From the Netskope Console in the device detail view, select Collect Log.
- B. Right-click on the Netskope task tray icon and click Save Logs...
- C. Open the Netskope Client application and click the Advanced Debugging button.
- D. Search for the systeminfo.log file in Explorer and submit the results.

Answer: A, B

Explanation:

From the Netskope Console in the device detail view, select Collect Log:

Step 1: Access the Netskope Admin Console.

Step 2: Navigate to the specific device detail view.

Step 3: Locate and select the "Collect Log" option.

Reference: This method is described in the Netskope documentation under device management and log collection sections.

Right-click on the Netskope task tray icon and click Save Logs...:

Step 1: Go to the device running the Netskope Client.

Step 2: Locate the Netskope icon in the task tray.

Step 3: Right-click on the Netskope icon.

Step 4: Select "Save Logs..." from the context menu.

Reference: This method is commonly described in user guides for collecting logs locally from client applications.

Reference:

Netskope Knowledge Portal: Detailed guides on collecting logs via the Netskope Console and client applications.

Question: 85

Which compliance standard should a company consider if both controllers and processors have legal entities in the EU?

- A. PCI-DSS
- B. GDPR
- C. Safe Harbor
- D. LGPD

Answer: B

Explanation:

The General Data Protection Regulation (GDPR) is the compliance standard a company should consider if both controllers and processors have legal entities in the EU. The GDPR applies to any organization that processes personal data of individuals within the EU, regardless of where the organization itself is based. This regulation imposes strict rules on data handling and provides robust protection for personal data.

Reference:

GDPR is designed to protect data privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas.

Question: 86

A new customer is concerned about performance, especially with respect to Microsoft 365. They have offices in 20 countries around the world and their workforce is mostly mobile.

In this scenario, which two statements about NewEdge would align with the customer's requirements? (Choose two.)

- A. NewEdge accurately identifies Microsoft 365 violations and data risks.
- B. NewEdge provides advanced public cloud infrastructure security.
- C. NewEdge provides direct peering with Microsoft in every data center.
- D. NewEdge delivers a single, unified network with all services available in all locations worldwide.

Answer: C, D

Explanation:

NewEdge is Netskope's security private cloud, offering high-performance, low-latency access to the internet and cloud services. For a customer concerned about performance, especially with respect to Microsoft 365, NewEdge provides significant benefits:

Direct Peering with Microsoft: NewEdge establishes direct peering connections with Microsoft in every data center. This ensures optimal routing and performance for Microsoft 365 services, which is crucial for customers with a global, mobile workforce.

Unified Global Network: NewEdge delivers a single, unified network with all security services available in all locations worldwide. This ensures consistent security policies and performance regardless of where users are located, providing seamless access and reducing latency.

Question: 87

Your company has implemented Netskope's Cloud Firewall and requires that all FTP connections are blocked regardless of the ports being used.

Which two statements correctly identify how to block FTP access? (Choose two.)

- A. Create a Real-time Protection policy with FTP as the destination application and Block as the action.
- B. Create a Real-time Protection policy with a custom Firewall App Definition for TCP port 21 as the destination application and Block as the action.
- C. Ensure there are no Real-time Protection policies that allow FTP and change the default non-Web action to Block.
- D. Create a custom Firewall App Definition for TCP port 21 and add it to the default tenant Steering Configuration as an exception.

Answer: A, B

Explanation:

To block all FTP connections regardless of the ports being used, the following steps should be taken using Netskope's

Cloud Firewall:

Real-time Protection Policy:

Create a Real-time Protection policy where FTP is defined as the destination application.

Set the action to "Block" to ensure that any FTP traffic is blocked regardless of the port being used.

Custom Firewall App Definition:

Create a custom Firewall App Definition specifically for TCP port 21.

Define the action as "Block" to ensure any traffic directed to this port is blocked, preventing FTP access.

These configurations ensure that FTP traffic is effectively blocked, securing the network from potential threats and unauthorized data transfers via FTP.

Question: 88

When accessing an encrypted website (HTTPS), what is a reason why you might receive a "certificate not trusted" browser message?

- A. A certificate authority is installed on the server.
- B. A self-signed certificate is installed on the server.
- C. A public certificate is installed on the server.

D. There is no certificate installed on the server.

Answer: B

Explanation:

When accessing an encrypted website (HTTPS), a "certificate not trusted" message in the browser usually occurs because the certificate presented by the website is not issued by a trusted Certificate Authority (CA). A common scenario for this is when a self-signed certificate is installed on the server. Self-signed certificates are not signed by a CA that is recognized by the browser, so the browser cannot verify the authenticity of the certificate, leading to the "certificate not trusted" message.

Reference:

"If the SSL certificate is self-signed, the browser will not trust the certificate because it has not been issued by a trusted CA."

Question: 89

The Netskope deployment for your organization is deployed in CASB-only mode. You want to view dropbox.com traffic but do not see it when using SkopelT.

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

- A. The Dropbox Web application is certificate pinned and cannot be steered to the Netskope tenant.
- B. The Dropbox domains have not been configured to steer to the Netskope tenant.
- C. The Dropbox desktop application is certificate pinned and cannot be steered to the Netskope tenant.
- D. The Dropbox domains are configured to steer to the Netskope tenant.

Answer: A, B

Explanation:

In a CASB-only deployment of Netskope, there could be several reasons why Dropbox.com traffic is not visible in SkopelT:

Certificate Pinning:

The Dropbox Web application might be using certificate pinning, which means it only accepts specific certificates for its connections. This can prevent the traffic from being steered to the Netskope tenant because the proxy's certificate might not match the pinned certificate.

Configuration of Dropbox Domains:

If the Dropbox domains are not properly configured to be steered to the Netskope tenant, then the traffic will bypass the Netskope inspection and will not be visible in SkopelT. Ensuring that the domains are configured correctly is essential for the traffic to be captured and analyzed by Netskope.

Reference:

"Certificate pinning prevents the interception of traffic by requiring that the presented certificate matches a known good certificate. This can interfere with traffic steering in CASB deployments."

"Proper configuration of application domains is necessary to ensure traffic is steered to the Netskope tenant for inspection and visibility."

Question: 90

You are required to present a view of all upload activities completed by users tunneled from the Los Angeles office to cloud storage applications.

Which two basic filters would you use on the SkopelT Applications page to satisfy this requirement? (Choose two.)

- A. Activity
- B. Access Method
- C. Action
- D. CCL

Answer: A, B

Explanation:

To present a view of all upload activities completed by users tunneled from the Los Angeles office to cloud storage applications, the following two basic filters should be used on the SkopelT Applications page:

Activity: This filter will allow you to specify the type of activity, in this case, "upload."

Access Method: This filter will help to specify the method of access, which is necessary to filter activities that are tunneled.

These filters combined will provide a comprehensive view of the required activities. For further details, please refer to the Netskope documentation on setting up and using filters in SkopeIT Applications.

Reference:

[Netskope Knowledge Portal: REST API v2 Overview.](#)

[Postman Collection: API v2.](#)

Question: 91

What information is displayed in an application's Cloud Confidence Index (CCI) page? (Choose two.)

- A. top users by sessions
- B. policy violations
- C. GDPR readiness
- D. stock price

Answer: A, C

Explanation:

The Cloud Confidence Index (CCI) page in Netskope provides various metrics and information about an application.

Among these, the two relevant pieces of information displayed are:

Top users by sessions: This metric provides insights into which users are most active within the application, giving a view of user engagement and activity levels.

GDPR readiness: This metric indicates how well the application complies with GDPR regulations, providing a readiness score or status based on the app's handling of personal data.

These metrics help administrators and security professionals to evaluate the usage and compliance status of cloud applications.

Reference:

[Using the REST API v2 UCI Impact Endpoints.](#)

[Netskope Knowledge Portal: Dataexport Iterator Endpoints.](#)

Question: 92

An administrator has created a DLP rule to search for text within documents that match a specific pattern. After creating a Real-time Protection Policy to make use of this DLP rule, the administrator suspects the rule is generating false positives.

Within the Netskope tenant, which feature allows administrators to review the data that was matched by the DLP rule?

- A. Risk Insights
- B. Forensic
- C. Quarantine
- D. Legal Hold

Answer: B

Explanation:

When an administrator suspects that a DLP rule is generating false positives, the Forensic feature within the Netskope tenant allows for reviewing the data that was matched by the DLP rule. This feature provides detailed logs and insights into why a specific piece of data was flagged, enabling the administrator to analyze and adjust the rule as needed.

To access and use the Forensic feature:

Navigate to the Forensic section in the Netskope UI.

Review the detailed logs and matched data to understand the context and reason behind each match.

Adjust the DLP rules if necessary to reduce false positives and improve accuracy.

Reference:

[Netskope REST API Overview.](#)

[Netskope SDK Documentation.](#)

Question: 93

Your organization has implemented Netskope Private Access (NPA) for all users. Users from the European region are reporting that they are unable to access many of their applications. You suspect that the publishers for the European data center may be disconnected and you want to verify the Publishers' status.

Which two methods describe how you would accomplish this task? (Choose two.)

- A. Use the Status field on the Publishers page.
- B. Use the Network Events page in
- C. Use the Netskope Private Access Troubleshooter.
- D. Use the Private Apps page in

Answer: A, C

Explanation:

To verify the status of the Publishers in the European data center, the following methods can be used:

Use the Status field on the Publishers page:

Navigate to the Publishers page in the Netskope UI.

Check the Status field to see if any Publishers are disconnected or experiencing issues.

Use the Netskope Private Access Troubleshooter:

Access the Netskope Private Access Troubleshooter tool.

This tool provides detailed diagnostic information and helps identify connectivity issues with Publishers.

These methods provide direct insights into the health and connectivity status of the Publishers, helping to quickly identify and resolve any issues affecting user access.

Reference:

Netskope Knowledge Portal: Private Access

Netskope Private Access Troubleshooter

Question: 94

Which three statements about Netskope Private Access Publishers are correct? (Choose three.)

- A. Publishers can run on Windows or Linux servers.
- B. Publishers can be deployed in both private data centers and public cloud providers to provide access to applications across disparate locations.
- C. Publisher deployment can be automated in public cloud environments using Netskope's REST API.
- D. Publishers only make outbound connections to the Netskope Security Cloud which reduces the amount of public exposure.
- E. Publishers can be deployed as hardware or software appliances to provide access to applications across disparate locations.

Answer: ABD

Explanation:

The following statements about Netskope Private Access Publishers are correct:

Publishers can run on Windows or Linux servers:

Publishers are versatile and can be installed on both Windows and Linux operating systems.

Publishers can be deployed in both private data centers and public cloud providers to provide access to applications across disparate locations:

This flexibility allows organizations to use Publishers to connect applications hosted in various environments, ensuring seamless access across locations.

Publishers only make outbound connections to the Netskope Security Cloud which reduces the amount of public exposure:

By making only outbound connections, Publishers minimize the attack surface, enhancing security by reducing public exposure.

Reference:

Netskope Private Access Deployment Guide

[Netskope REST API v2 Overview](#)

Question: 95

A customer is considering the cloud shared responsibility model.

In this scenario, which two criteria become the customer's responsibility? (Choose two.)

- A. controlling access
- B. third-party certification
- C. enforcing service level agreements
- D. preventing data leakage

Answer: A, D

Explanation:

In the context of the cloud shared responsibility model, the customer's responsibilities include:

Controlling access:

Customers must manage access controls to ensure that only authorized users can access their data and applications. This includes implementing identity and access management (IAM) policies, multifactor authentication (MFA), and regular auditing of access permissions.

Preventing data leakage:

Customers are responsible for implementing data loss prevention (DLP) strategies to protect sensitive information from unauthorized access, disclosure, or exfiltration. This involves configuring and monitoring DLP policies, encryption, and other security measures.

These responsibilities are critical for maintaining the security and integrity of data in the cloud, complementing the cloud provider's responsibilities for the infrastructure and services.

Reference:

Netskope Knowledge Portal: Cloud Security

[Shared Responsibility Model](#)

Question: 96

You are required to create a policy that will notify and allow users to log into their personal Google Drive instance.

Which two policy components must be configured to enforce this use case? (Choose two.)

- A. Storage Constraint Profile
- B. Steering Exception
- C. User Alert
- D. User Constraint Profile

Answer: B, C

Explanation:

To create a policy that will notify and allow users to log into their personal Google Drive instance, you need to configure the following components:

Steering Exception:

This component allows you to create exceptions for specific traffic. In this case, you will configure a steering exception to allow traffic to personal Google Drive instances. This ensures that the policy correctly routes the traffic to the appropriate destination without being blocked or filtered incorrectly.

User Alert:

A User Alert component will be configured to notify users when they attempt to log into their personal Google Drive. This alert can provide information about the policy and any actions the user may need to take. It helps in enforcing the policy by informing users about the specific conditions or restrictions.

Reference:

Netskope Knowledge Portal: Configuring Steering Exceptions

Netskope Knowledge Portal: Creating User Alerts

Question: 97

In which two scenarios would you use SD-WAN technology? (Choose two.)

- A. to differentiate between corporate and personal SaaS applications
- B. to optimize utilization and performance across multiple Internet connections

- C. to ensure a user's corporate laptop has all of the required security compliance software in place
- D. to replace dedicated MPLS connections with multiple broadband WAN and mobile options

Answer: B, D

Explanation:

SD-WAN technology is used in the following scenarios:

To optimize utilization and performance across multiple Internet connections:

SD-WAN allows organizations to aggregate multiple Internet connections and optimize traffic flow based on application requirements and network conditions. This improves overall network performance and ensures efficient use of available bandwidth.

To replace dedicated MPLS connections with multiple broadband WAN and mobile options:

SD-WAN provides the flexibility to use a mix of broadband, LTE, and other connectivity options to replace traditional MPLS circuits. This can significantly reduce costs and improve agility in network deployment and management.

Reference:

Netskope Knowledge Portal: SD-WAN Integration

Netskope Knowledge Portal: Benefits of SD-WAN

Question: 98

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.)

- 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.

Reference:

Netskope Knowledge Portal: Digital Experience Management

Netskope Knowledge Portal: Devices Page

Question: 99

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

- 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.

Reference:

Netskope Knowledge Portal: Deploying Virtual Appliances

Netskope Private Access Overview

Question: 100

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

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

Answer: D

Explanation:

When comparing data in motion with data at rest, it is important to understand how each type of data is handled in terms of security and monitoring:

Data in motion refers to data actively moving from one location to another, such as through email, instant messaging, or any other form of communication over the internet. To secure and monitor data in motion, Netskope typically requires the deployment of the Netskope client on user devices. The client helps enforce security policies, monitor data transfers, and protect against data loss and other threats during the data's transit.

Reference:

Netskope Knowledge Portal: Data Protection

Netskope Client Overview

Question: 101

You want to take into account some recent adjustments to CCI scoring that were made in your Netskope tenant.

In this scenario, which two CCI attributes in the UI would be used in a Real-time Protection policy? (Choose two.)

- A. Domains
- B. App Tag
- C. CCL Level
- D. GDPR Readiness

Answer: BC

Explanation:

When adjusting Cloud Confidence Index (CCI) scoring in your Netskope tenant, you can use the following two CCI attributes in a Real-time Protection policy:

App Tag:

App Tags are used to categorize and tag applications based on their functionality, risk level, or compliance requirements. By using App Tags in Real-time Protection policies, you can enforce security measures and monitor activities based on the specific tags assigned to applications.

CCL Level:

CCL (Cloud Confidence Level) is a score assigned to cloud applications based on their risk profile and compliance with security standards. By incorporating CCL Level into your Real-time Protection policies, you can ensure that actions are taken based on the risk level of the applications, such as blocking or monitoring high-risk applications.

Reference:

Netskope Knowledge Portal: Cloud Confidence Index

Netskope Real-time Protection Policies

Question: 102

Which two statements are correct about Netskope's NewEdge Security Cloud Network Infrastructure? (Choose two.)

- A. It utilizes virtual POPs for traffic onboarding ensuring low latency.
- B. It includes direct peering with Microsoft and Google in every data center.

- C. It is a private security cloud network that is over-provisioned, elastic, and built for scale.
- D. It utilizes multiple public cloud providers for inline services ensuring high availability and elasticity.

Answer: BC

Explanation:

Netskope's NewEdge Security Cloud Network Infrastructure is designed to provide high performance, security, and scalability for cloud traffic. The following statements are correct about this infrastructure:

It includes direct peering with Microsoft and Google in every data center:

Netskope has established direct peering relationships with major cloud service providers like Microsoft and Google. This direct peering ensures optimized and low-latency connections to these services, improving performance for end-users.

It is a private security cloud network that is over-provisioned, elastic, and built for scale:

The NewEdge network is a private security cloud network that is designed to be highly scalable and elastic. It is over-provisioned to handle large volumes of traffic and can scale up as needed to meet demand. This ensures high availability and performance for users accessing cloud services.

Reference:

Netskope NewEdge Overview

Netskope Knowledge Portal: NewEdge Network

Question: 103

Which three components make up the Borderless SD-WAN solution? (Choose three)

- A. Endpoint SD-WAN Client
- B. SASE Orchestrator
- C. NPA Publisher
- D. SASE Gateway
- E. On-Premises Log Parser

Answer: ABD

Explanation:

The three components that make up the Borderless SD-WAN solution are:

Endpoint SD-WAN Client: This client is installed on endpoints (such as laptops and mobile devices) to ensure secure and optimized connectivity to the corporate network, even when users are remote. The Endpoint SD-WAN Client is a critical part of extending SD-WAN capabilities to individual users and devices, providing seamless connectivity and security.

SASE Orchestrator: The Secure Access Service Edge (SASE) Orchestrator is responsible for managing and orchestrating the various components of the SD-WAN solution. It ensures that policies are enforced consistently across the network, manages the deployment of network functions, and provides centralized control and visibility.

SASE Gateway: The SASE Gateway provides secure, optimized access to cloud applications and services. It combines SD-WAN capabilities with advanced security functions, such as firewalling, intrusion prevention, and secure web gateways, to protect data and users as they access resources from different locations.

These components work together to provide a comprehensive SD-WAN solution that addresses the needs of modern, distributed workforces by combining networking and security functions in a unified architecture.

Reference:

Netskope REST API v2 Overview.

Using the REST API v2 dataexport Iterator Endpoints.

Using the REST API v2 UCI Impact Endpoints.

Netskope SDK on PyPI.

Postman Collection for Netskope REST API.

Question: 104

Click the Exhibit button.

^ Exhibit

• I Compromised Acco... O

Monitor for and detect activity indicative of a corporate cloud application account that has been compromised and controlled by an external attacker

APP

9



Dats Exhiltration CD

Detect suspicious transfer of data outside the organization.

Some



Malicious Insider

Identify corporate users whose activity Indicates a potential risk * either accidental or deliberate - to the security posture of your environment

0

The exhibit shows security rules that are part of which component of the Netskope platform?

- A. Real-time Protection
- B. Advanced Malware Protection
- C. Security Posture
- D. Behavior Analytics

Answer: D

Explanation:

The exhibit displays rules related to detecting compromised accounts, data exfiltration, and malicious

insiders. These types of activities are typically analyzed and detected through user behavior analytics, which involves monitoring and analyzing the behavior of users to identify anomalies that may indicate security incidents or threats.

Behavior Analytics is a component of the Netskope platform that focuses on identifying potential security risks based on user behavior. This includes monitoring for compromised accounts, data exfiltration, and identifying malicious insiders. These analytics help in proactively identifying and mitigating threats by analyzing patterns and anomalies in user activities.

Reference:

The exhibit showing rules related to compromised accounts, data exfiltration, and malicious insiders aligns with the capabilities provided by Behavior Analytics.

Documentation from the Netskope Knowledge Portal on the behavior analytics capabilities supports this identification.

Question: 105

You are required to restrict cloud users from uploading data to any risky cloud storage service as defined by the Cloud Confidence Index. In the Netskope platform, which two policy elements would enable you to implement this control? (Choose two)

- A. Device Classification
- B. Category
- C. Cloud App
- D. Cloud Confidence Level

Answer: BD

Explanation:

To restrict cloud users from uploading data to risky cloud storage services as defined by the Cloud Confidence Index (CCI) in the Netskope platform, you would use the following policy elements:

Category: This policy element allows you to define and restrict actions based on the category of the cloud application. For example, you can categorize cloud storage services and create policies that restrict uploads to any application that falls under this category.

Cloud Confidence Level: This policy element leverages the Cloud Confidence Index (CCI), which rates the risk level of cloud applications. By using the Cloud Confidence Level, you can create policies that restrict uploads to applications with a low confidence level, thereby preventing data uploads to risky cloud storage services.

Reference:

Using the Netskope Knowledge Portal documentation, specifically under policy configuration and enforcement, which details how to use categories and Cloud Confidence Level in policy creation.

Postman collection and API documentation that describes the usage of these elements in the Netskope API.

Question: 106

A customer wants to receive e-mail alerts whenever Netskope publishes an incident involving a specific service, or if Netskope publishes information regarding planned maintenance. Which two Netskope sites allow an administrator to subscribe to service notifications? (Choose two.)

- A. <https://notify.netskope.com>
- B. <https://communitynetskope.com/>
- C. <https://supportnetskope.com>
- D. <https://trust.netskope.com>

Answer: AD

Explanation:

Administrators can subscribe to service notifications, including incidents and planned maintenance, through the following Netskope sites:

<https://notify.netskope.com>: This site provides notifications about incidents and maintenance updates.

Administrators can subscribe to receive email alerts whenever there are updates involving specific services or planned maintenance.

<https://trust.netskope.com>: This site offers detailed information about Netskope's operational status, including any incidents, planned maintenance, and security updates. Administrators can subscribe to receive notifications and stay informed about the service status.

Reference:

Netskope documentation and support articles on subscribing to service notifications and updates.

Netskope's service notification and operational status sites providing subscription options for alerts and updates.

Question: 107

Click the Exhibit button.



A user is uploading a file containing PCI-DSS data to the corporate Google Drive instance. You notice that the upload is not blocked by the policy shown in the exhibit. Which statement is correct in this scenario?

- A. The policy is not applied to the correct user group.
- B. The policy is not applied to the correct URL category.
- C. The policy is not applied in the correct order.
- D. The policy is not applied to the correct application activity.

Answer: C

Explanation:

In the exhibit, a user is uploading a file containing PCI-DSS data to the corporate Google Drive instance. Despite the policy that blocks DLP (Data Loss Prevention) uploads being active, the upload is not

blocked. This indicates that the policy is not applied in the correct order.

Netskope applies policies in a top-down manner. If there are multiple policies that could apply to an action, the order in which the policies are evaluated is crucial. In this case, another policy might be allowing the upload before the DLP policy can block it. Ensuring that the DLP policy is higher in the order can resolve this issue.

Reference:

Netskope policy configuration and enforcement documentation.

Details on how Netskope processes and applies policies based on their order in the policy list.

Question: 108

You are setting up a real-time threat protection policy for patient zero to block previously unseen files until a benign verdict is produced by the Netskope Threat Protection Service. In this scenario, which two policy parameters must you configure? (Choose two)

- A. block action
- B. CCL destination criterion
- C. file type activity constraint
- D. remediation profile

Answer: AD

Explanation:

To set up a real-time threat protection policy for patient zero to block previously unseen files until a benign verdict is produced by the Netskope Threat Protection Service, you need to configure the following parameters:

Block Action: This action ensures that any previously unseen file is blocked until it has been analyzed and a verdict has been reached. By blocking the file, the policy prevents potential threats from entering the network until they are deemed safe.

Remediation Profile: This profile defines the actions to be taken when a threat is detected. It includes configuring the alerts and responses (such as notifying administrators) when a file is blocked. This ensures that there is a process in place for handling detected threats and that appropriate measures are taken.

Reference:

Netskope Threat Protection documentation detailing the setup of real-time threat protection policies.

Configuration guides for policy actions and remediation profiles in the Netskope platform.

Question: 109

Which networking function does a SASE solution provide above and beyond an SSE solution?

- A. Secure Web Gateway
- B. Cloud Access Security Broker
- C. Data Loss Prevention
- D. Software Defined Wide Area Network

Answer: D

Explanation:

A SASE (Secure Access Service Edge) solution provides networking functions that go beyond the capabilities of an SSE (Security Service Edge) solution. Specifically, a SASE solution integrates:

Software Defined Wide Area Network (SD-WAN): SD-WAN enhances network performance and efficiency by dynamically routing traffic across the best available paths. It provides greater flexibility, improved application performance, and reduced costs compared to traditional WAN solutions.

In contrast, SSE focuses on security services like Secure Web Gateway, Cloud Access Security Broker, and Data Loss Prevention, but does not include networking functions such as SD-WAN.

Reference:

Netskope's documentation on SASE and SSE solutions, highlighting the differences and additional functionalities provided by SASE, including SD-WAN.

Detailed explanation of SD-WAN and its integration into SASE solutions.

Question: 110

You are adding a new tenant administrator in the Admins page. Which additional security measure would you be able to enable for only this new account?

- A. Activate SSO authentication using an external identity provider.
- B. Activate MFA to log in to the Netskope management console.
- C. Set the password expiration.
- D. Add the administrator to the Administration Audit Log.

Answer: B

Explanation:

When adding a new tenant administrator in the Admins page, you can enhance the security for the new account by enabling Multi-Factor Authentication (MFA). MFA adds an extra layer of security by requiring the administrator to provide a second form of verification in addition to the password, thus protecting against unauthorized access.

Reference:

Netskope documentation on user and admin account management, including the configuration and benefits of enabling MFA.

Security best practices guides from Netskope, emphasizing the importance of MFA for enhanced account security.

Question: 111

In the Tenant III, which two methods would an administrator use to update a File Profile with malicious file hashes? (Choose two)

- A. Upload a CSV file of malicious file hashes.

- B. Create a Threat Protection Profile to define a block list of malicious files.
- C. Input a list of malicious file hashes.
- D. Upload a JSON file of malicious file hashes.

Answer: AC

Explanation:

To update a File Profile with malicious file hashes in the Netskope platform, an administrator can use the following methods:

Upload a CSV file of malicious file hashes: Administrators can prepare a CSV file containing the malicious file hashes and upload it to the platform. This method allows for bulk updates of the file profile with multiple hashes at once.

Input a list of malicious file hashes: Administrators can manually input a list of malicious file hashes directly into the platform. This method is useful for adding individual hashes or making small updates to the file profile.

These methods ensure that the file profile is updated with the latest malicious file information, enabling the platform to detect and block known threats effectively.

Reference:

Netskope documentation on managing File Profiles and updating them with malicious file hashes.

Instructions and best practices for uploading and managing threat intelligence data within the Netskope platform.

Question: 112

Click the Exhibit button.

B Exhibit

• 3 Cloud Firewall Polick* <21

11	Allow SSH for Group A	A Group A	S faw«SMtSSH)	H«	»»"
12	Allow SSH and RDP for Group B E Group B	^ Secure Shell fSSH)	Remote DeeMrtp Protocol	h	-Allow
		(Wwdowi Ttrwunil Server / RDP)			

You configured a set of Cloud Firewall policies as shown in the exhibit and changed your Steering Configuration to All Traffic for Group A and Group B. Users in Group A report that they are unable to access a third-party server using TCP port 3389. Referring to the exhibit, which action correctly describes how you would allow these connections without allowing unnecessary access?

- A. Add Group A to the Group B Allow policy.
- B. Create an Allow policy using a custom application including the destination IP and TCP port 3389.
- C. Move the Group B Allow policy above the Group A Allow policy.
- D. Change the default action to Allow.

Answer: B

Explanation:

The exhibit shows that Group A is allowed only SSH traffic, while Group B is allowed both SSH and RDP traffic. Since users in Group A need access to a third-party server using TCP port 3389 (RDP), you need to create a specific policy to allow this traffic without granting unnecessary access.

Creating an Allow policy using a custom application that includes the destination IP and TCP port 3389 will precisely target the required traffic and ensure that only the necessary connections are

permitted. This method avoids broader policy changes that could introduce unnecessary access.

Reference:

Netskope documentation on creating and managing Cloud Firewall policies.

Best practices for configuring application-specific policies to control network traffic effectively.

Question: 113

What are two benefits of creating a policy group as a logical collection of Real-time Protection policies?
(Choose two.)

- A. To split up policies by region or business unit.
- B. To enable Alert and Continue policies.
- C. To simplify workflow, allowing exact access to a specific set of policies.
- D. To provide additional actions based on policy match criteria.

Answer: AC

Explanation:

Creating a policy group as a logical collection of Real-time Protection policies provides several benefits:

To split up policies by region or business unit: This allows for more granular control and management of policies based on organizational structure. Each region or business unit can have its own set of policies tailored to its specific needs and compliance requirements.

To simplify workflow, allowing exact access to a specific set of policies: Policy groups help streamline the management process by grouping related policies together. This simplifies the workflow for administrators by providing them with access to only the relevant policies they need to manage, reducing complexity and potential for errors.

Reference:

Netskope documentation on creating and managing policy groups.

Best practices for organizing policies to enhance manageability and operational efficiency.

Question: 114

Your customer has cloud storage repositories containing sensitive files of their partners, including bank statements, consulting, and disclosure agreements. In this scenario, which feature would help them control the flow of these types of documents?

- A. ZTNA
- B. Netskope Advanced Analytics
- C. DLP document classifiers
- D. Sandboxing

Answer: C

Explanation:

Data Loss Prevention (DLP) document classifiers are designed to identify and control the flow of sensitive information based on predefined patterns and criteria. In this scenario, where the customer has cloud storage repositories containing sensitive files such as bank statements, consulting agreements, and disclosure agreements, DLP document classifiers can help:

Identify sensitive documents: By scanning and classifying documents based on their content, DLP document classifiers ensure that sensitive files are recognized and handled appropriately.

Control data flow: Policies can be applied to prevent unauthorized access, sharing, or movement of sensitive files, thereby protecting the data from leakage or exposure.

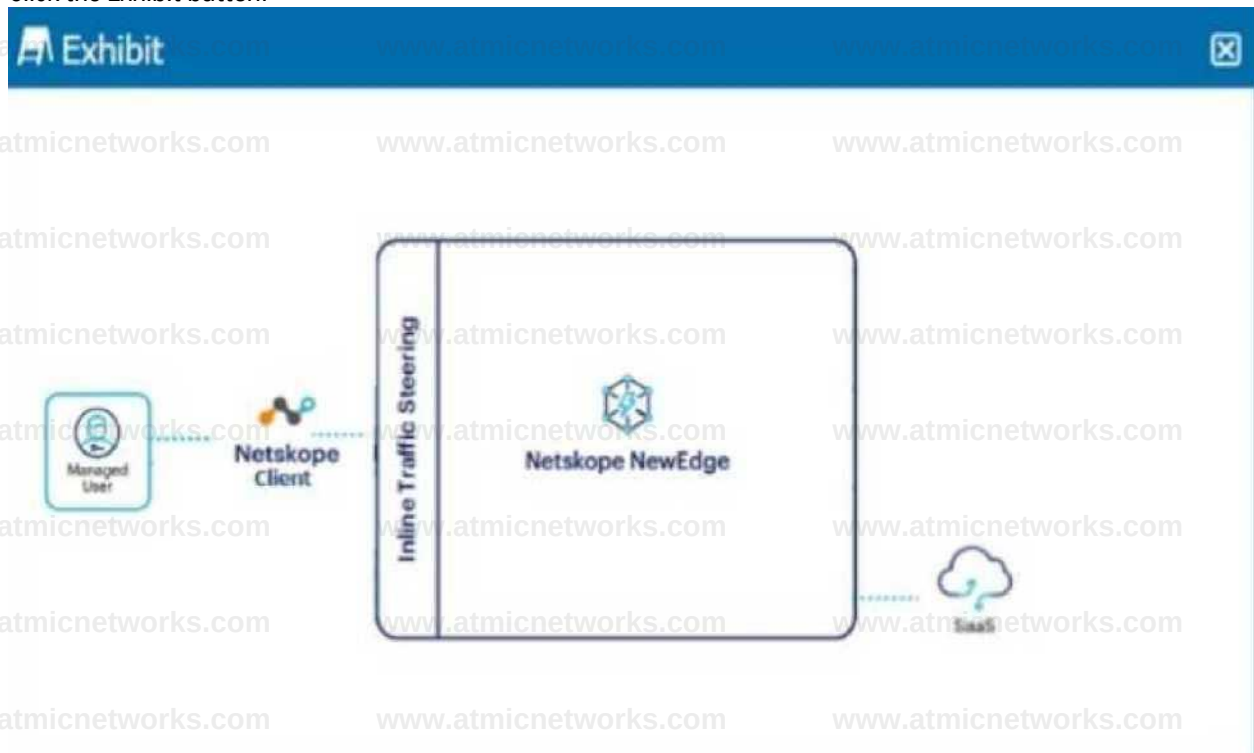
Reference:

Netskope DLP documentation, detailing how document classifiers work and how they can be configured to protect sensitive information.

Best practices for implementing DLP solutions to safeguard sensitive data in cloud storage environments.

Question: 115

Click the Exhibit button.



A user is connected to a SaaS application through Netskope's Next Gen SWG with SSL inspection enabled. In this scenario, what information is available in SkopeIT? (Choose three.)

A. User activity, CCL

- B. Destination IP, OS patch version
- C. Account instance, category
- D. Username, source location
- E. File version, shared folder

Answer: ACD

Explanation:

In the scenario where a user is connected to a SaaS application through Netskope's Next Gen Secure Web Gateway (SWG) with SSL inspection enabled, the following information is available in SkopelT:

User activity, CCL: SkopelT provides detailed logs of user activities, including actions taken within SaaS applications, and uses the Cloud Confidence Level (CCL) to rate the trustworthiness of cloud applications.

Account instance, category: It logs information about the specific instance of the account being accessed and categorizes the type of service or application in use, which helps in identifying the context of the user's activities.

Username, source location: The username of the user accessing the SaaS application and their source location (such as IP address or geographic location) are logged for audit and compliance purposes.

Reference:

Netskope documentation on SSL inspection and SkopelT logging.

Detailed configuration guides on using Next Gen SWG and the types of data collected by SkopelT.

Question: 116

You are asked to review files affected by malware in your organization. In this scenario, which two actions are possible and would be accessible from the Netskope UI -> Incidents --> Malware? (Choose two)

- A. Download the original malware file generating the alert to be analyzed by the SOC team

- B. Identify the exposure of the file identified as malware.
- C. Remediate the compromised devices.
- D. Determine the Detection Engine used to identify the malware.

Answer: BD

Explanation:

When reviewing files affected by malware in the Netskope UI under Incidents -> Malware, you have the following options:

Identify the exposure of the file identified as malware: This allows you to see where the malware has spread within the organization, which users or systems are affected, and any potential data exposure resulting from the malware.

Determine the Detection Engine used to identify the malware: Netskope provides details on which detection engine (such as AV, sandboxing, or other heuristic engines) identified the malware. This helps in understanding the threat vector and the reliability of the detection.

Downloading the original malware file (option A) is generally not recommended for security reasons and may not be supported directly from the Netskope UI. Remediation of compromised devices (option C) would typically be handled through endpoint security solutions rather than directly from the Netskope UI.

Reference:

Netskope documentation on malware detection and incident response.

Best practices for handling malware incidents and using the Netskope UI for threat analysis.

Question: 117

Your customer asks you to secure all Web traffic as part of the initial configuration. In the Netskope platform, which statement is correct in this scenario?

- A. Add the all Web traffic option to the steering configuration.

- B. Netskope automatically steers all Web traffic.
- C. Netskope cannot steer Web traffic.
- D. Select all Web traffic in the SSL decryption section.

Answer: A

Explanation:

To secure all web traffic as part of the initial configuration in the Netskope platform, you need to:

Add the all Web traffic option to the steering configuration: This ensures that all web traffic is routed through Netskope for inspection and policy enforcement. By steering all web traffic, you enable Netskope to apply security measures, such as SSL decryption, threat protection, and DLP, to all HTTP and HTTPS traffic.

Netskope does not automatically steer all web traffic by default; it requires configuration in the steering policies. Selecting all web traffic in the SSL decryption section only pertains to decrypting traffic, not the actual steering of the traffic.

Reference:

Netskope documentation on configuring steering settings and policies.

Guidelines for setting up web traffic steering and SSL decryption in the Netskope platform.

Question: 118

As an administrator, you are investigating an increase in the number of incidents related to

compromised credentials. You are using the Netskope Compromised Credentials feature on your tenant to assess the situation. Which insights would you find when using this feature? (Choose two)

- A. Compromised usernames
- B. Breach information source

- C. Compromised passwords
- D. Affected managed applications

Answer: AB

Explanation:

When using the Netskope Compromised Credentials feature, administrators can gain valuable insights into security incidents related to compromised credentials. The insights provided by this feature include:

Compromised usernames: This information helps identify which user accounts have been compromised, allowing administrators to take necessary actions such as resetting passwords and notifying affected users.

Breach information source: Netskope provides details on the source of the breach, such as which third-party service or data breach resulted in the compromise of credentials. This helps in understanding the context of the breach and implementing measures to prevent future incidents.

While compromised passwords (option C) are indirectly involved, they are not explicitly listed as an insight provided by this feature. Similarly, affected managed applications (option D) are related but not directly part of the primary insights.

Reference:

Netskope documentation on Compromised Credentials feature and incident response.

Security best practices for managing and mitigating compromised credential incidents.

Question: 119

Digital Experience Management (DEM) allows an administrator to monitor which two areas? (Choose two.)

- A. User activities
- B. Bandwidth consumption
- C. Information on triggered policies
- D. Client steering data

Answer: BD

Explanation:

Digital Experience Management (DEM) in Netskope allows administrators to monitor the following areas:

Bandwidth consumption: DEM provides insights into how much bandwidth is being used by different applications and services, helping administrators to optimize network performance and ensure efficient use of resources.

Client steering data: DEM collects data on how traffic is being steered through the Netskope infrastructure, including details about routing decisions, performance metrics, and user experiences. This helps administrators understand the impact of their steering policies and make adjustments to improve performance.

User activities (option A) and information on triggered policies (option C) are more directly related to other features such as activity logs and policy enforcement dashboards rather than DEM.

Reference:

Netskope documentation on Digital Experience Management.

Guides on monitoring and optimizing network performance using DEM.

Question: 120

Which Netskope component would an administrator use to see an overview of private application usage and performance?

- A. Digital Experience Management
- B. Publishers page
- C. Incident Management
- D. Cloud Exchange

Answer: A

Explanation:

An administrator would use the Digital Experience Management (DEM) component to see an overview of private application usage and performance. DEM provides comprehensive insights into the performance and user experience of private applications, including metrics on latency, bandwidth, and application health.

Digital Experience Management (DEM): This component focuses on monitoring and optimizing the user experience for private and public applications by collecting detailed performance data and providing

actionable insights.

The other options do not provide the same level of detailed performance and usage overview for private applications:

Publishers page: Typically used for managing and configuring Netskope Publishers.

Incident Management: Focuses on tracking and resolving security incidents.

Cloud Exchange: Deals with integrations and data sharing between Netskope and other security solutions.

Reference:

Netskope documentation on Digital Experience Management and its capabilities.

Best practices for using DEM to monitor application performance and enhance user experience.

Question: 121

A user has performed a bulk delete activity. In this scenario, which Netskope feature monitors potential risky users for a malicious activity that would cause data loss?

- A. Netskope's Threat Protection inline policies
- B. Netskope's Behavior Analytics rule-based policies
- C. Netskope's API Data Protection policies
- D. Netskope's Cloud Threat Exchange integration

Answer: B

Explanation:

Netskope's Behavior Analytics rule-based policies are designed to monitor user behavior for patterns that may indicate risky or malicious activities, such as bulk deletions. These policies can identify anomalies in user behavior that deviate from the norm, flagging potential threats and taking appropriate actions to prevent data loss.

Netskope's Behavior Analytics rule-based policies: This feature analyzes user actions and behaviors to detect anomalies and potentially malicious activities. It helps in identifying and mitigating risks associated with compromised accounts, insider threats, and other suspicious activities.

Reference:

Netskope documentation on Behavior Analytics and its capabilities.

Security best practices for detecting and responding to insider threats and anomalous user behavior.

Question: 122

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

- 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.

Reference:

Netskope architecture documentation describing the roles of different components.

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

Question: 123

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

- 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.

Reference:

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: 124

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

- A. Steering configuration
- B. Client configuration timestamp
- C. Publisher connectivity
- D. Client version

E. Reachability of the private app

Answer: ACE

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.

Reference:

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

Best practices for troubleshooting NPA connectivity and performance issues.

Question: 125

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?

- 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.

Reference:

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: 126

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

- 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: CD

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.

Reference:

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: 127

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.)

- A. Settings -> Security Cloud Platform -> Devices
- B. Settings -> Security Cloud Platform -> Client Configuration
- C. SkopelT -> Alerts -> View Details
- D. System Tray -> Configuration

Answer: BC

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.

Reference:

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: 128

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

- 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: CD

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.

Reference:

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: 129

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?

- 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.

Reference:

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.