Netskope.NSK101.v2024-07-16.q23

Exam Code:	NSK101
Exam Name:	Netskope Certified Cloud Security Administrator
Certification Provider:	Netskope
Free Question Number:	23
Version:	v2024-07-16
# of views:	973
# of Questions views:	230
https://www.freepdfdumps.com/Netskope.NSK101.v2024-07-16.q23.html	

NEW QUESTION: 1
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: (SHOW ANSWER)
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 IndexCreating Real-Time Policies for Cloud Applications

NEW QUESTION: 2
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 (LEAVE A REPLY)
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.

NEW QUESTION: 3
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 (LEAVE A REPLY)
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 ConfigurationCreating a Steering Configuration

NEW QUESTION: 4
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 (LEAVE A REPLY)
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.

NEW QUESTION: 5
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: B,C (LEAVE A REPLY)
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].

NEW QUESTION: 6
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 (LEAVE A REPLY)
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

NEW QUESTION: 7
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: (SHOW ANSWER)
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].

NEW QUESTION: 8

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: (SHOW ANSWER)
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.

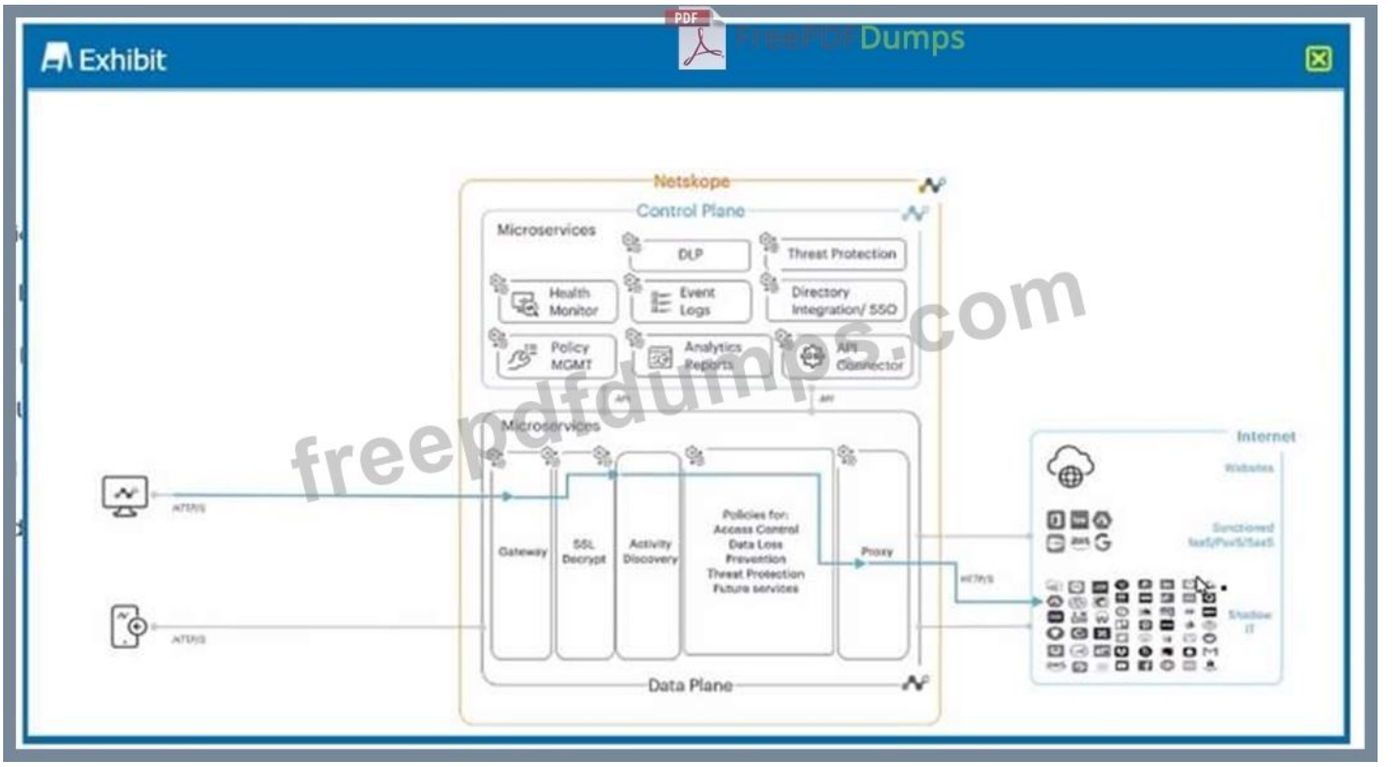
NEW QUESTION: 9
You are required to mitigate malicious scripts from being downloaded into your corporate devices every time a user goes to a website. Users need to access websites from a variety of categories, including new websites.
Which two actions would help you accomplish this task while allowing 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 (LEAVE A REPLY)
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].

NEW QUESTION: 10
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: C,D,E (LEAVE A REPLY)
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).

NEW QUESTION: 11
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: (SHOW ANSWER)
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].

NEW QUESTION: 12
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 the Incidents dashboard.
B. DLP incidents for a file are not visible when the file is deleted.
C. You can find DLP violations under Forensic profiles.
D. You must create a forensic profile so that an incident is created.
Answer: A (LEAVE A REPLY)
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

NEW QUESTION: 13
What are two characteristics of Netskope's Private Access Solution? (Choose two.)
A. It acts as a cloud-based firewall.
B. It provides protection for private applications.
C. It requires on-premises hardware.
D. It provides access to private applications.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 14
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 Wetransfer 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 (LEAVE A REPLY)
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? | CloudflareWhat is Shadow IT? | IBM

NEW QUESTION: 15
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 (LEAVE A REPLY)
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 sub-components 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.

NEW QUESTION: 16
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 (LEAVE A REPLY)

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].

NEW QUESTION: 17

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 (LEAVE A REPLY)

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].

NEW QUESTION: 18
What correctly defines the Zero Trust security model?
A. least privilege access
B. multi-layered security
C. strong authentication
D. double encryption
Answer: A (LEAVE A REPLY)
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.comWhat is Zero Trust Security? Principles of the Zero Trust Model

NEW QUESTION: 19
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 (LEAVE A REPLY)
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 ModeNetskope Steering Client [Netskope DLP Engine]

NEW QUESTION: 20
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: A,B (LEAVE A REPLY)
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].

NEW QUESTION: 21
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 (LEAVE A REPLY)
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.

NEW QUESTION: 22
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: B,C (LEAVE A REPLY)
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].

NEW QUESTION: 23
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 (LEAVE A REPLY)
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