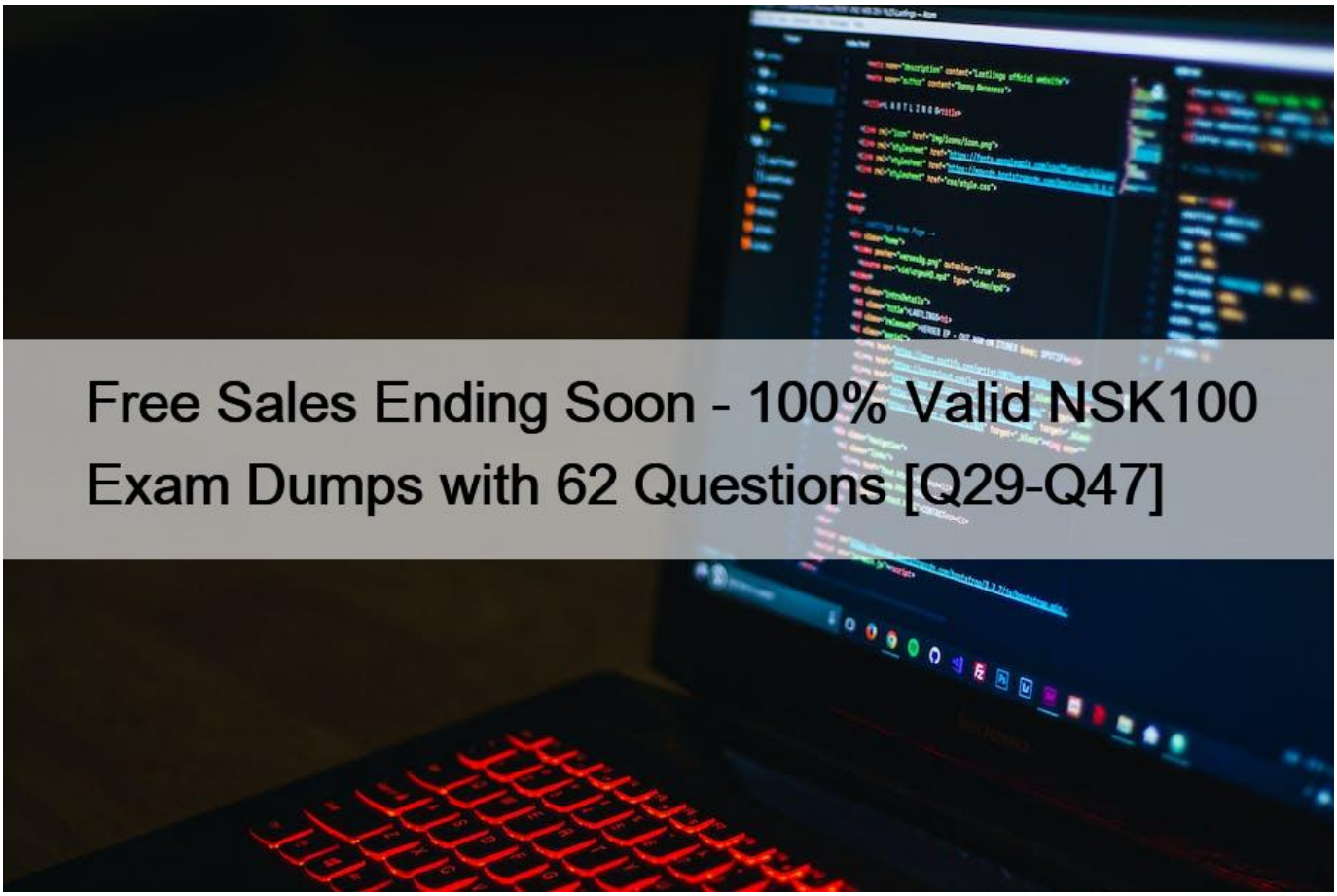
Free Sales Ending Soon - 100% Valid NSK100 Exam Dumps with 62 Questions [Q29-Q47



Free Sales Ending Soon - 100% Valid NSK100 Exam Dumps with 62 Questions
Verified NSK100 dumps Q&As on your Netskope NCCSA Exam Questions Certain Success!

NO.29 Which two traffic steering configurations are supported by Netskope? (Choose two.)
* browser isolation traffic only
* cloud applications only
* all Web traffic including cloud applications
* Web traffic only

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. References: Steering ConfigurationCreating a Steering Configuration

NO.30 Which two controls are covered by Netskope’s security platform? (Choose two.)
* ZTNA
* VPN
* CASB
* EDR

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. References: Netskope PlatformNetskope ZTNANetskope CASB

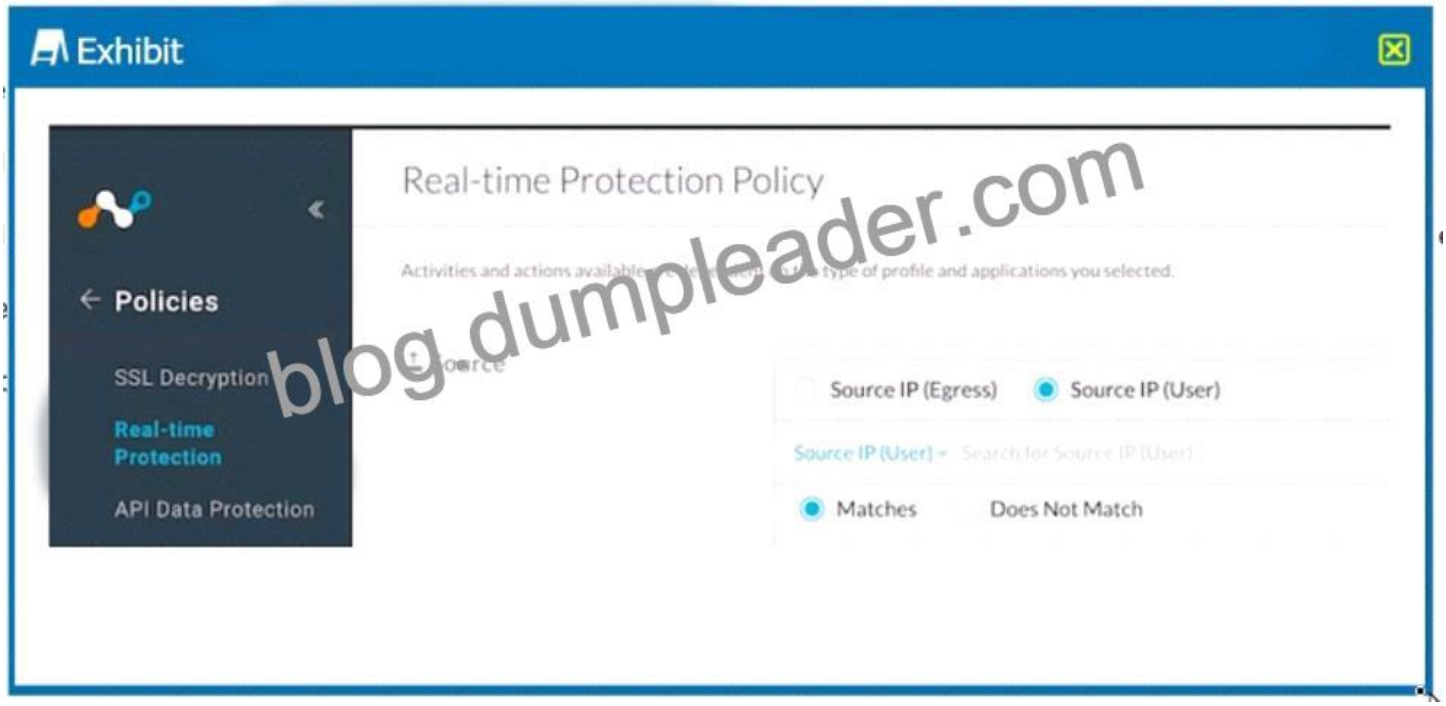
NO.31 What correctly defines the Zero Trust security model?
* least privilege access
* multi-layered security
* strong authentication
* double encryption

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. References: Zero Trust Security – microsoft.comWhat is Zero Trust Security?

Principles of the Zero Trust Model

NO.32



Click the Exhibit button.

Referring to the exhibit, which statement accurately describes the difference between Source IP (Egress) and Source IP (User) address?
* Source IP (Egress) is the IP address of the destination Web server while Source IP (User) is the IP address assigned to your network.
* 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.
* You must always leave the source IP fields blank and configure the user identity as a source criteria.
* Source IP (Egress) is the public IP address of your Internet edge router while Source IP (User) is the address assigned to the endpoint.
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. References: Source Address / Source Port vs Destination Address / Destination PortHow to explain Source IP Address, Destination IP Address & Service in easy way

NO.33 Which two functions are available for both inline and API protection? (Choose two.)
* multi-factor authentication
* threat protection
* DLP
* Cloud Security Posture Management (CSPM)
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. References: Netskope Inline Proxy ModeNetskope API ProtectionNetskope Threat ProtectionNetskope DLP Engine

NO.34 Which two statements describe a website categorized as a domain generated algorithm (DGA)? (Choose two.)
* The website is used for domain registration.
* The domain contains malicious algorithms.
* The website is used to hide a command-and-control server.
* The domain was created by a program.
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. References: Domain generation algorithmAmong cyber-attack techniques, what is a DGA?

NO.35 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?
* The customer has discovered a new SaaS application that is not yet rated in the CCI database.
* The customer’s organization places a higher business risk weight on vendors that claim ownership of their data.
* The customer wants to punish an application vendor for providing poor customer service.
* The customer’s organization uses a SaaS application that is currently listed as “under research”.

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. References: Netskope Security Cloud Operation & Administration (NSCO&A) – Classroom Course, Module 7: Cloud Confidence Index (CCI), Lesson 1: CCI Overview and Lesson 2: CCI Scoring.

NO.36 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.)
* The Cloud Storage category is in the Steering Configuration as an exception.
* The destination domain is excluded from decryption in the decryption policy.
* A Netskope POP is not in your local country and therefore DLP policies cannot be applied.
* DLP policies do not apply when using IPsec as a steering option.

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. References: 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

NO.37 What are two primary advantages of Netskope’s Secure Access Service Edge (SASE) architecture? (Choose two.
* no on-premises hardware required for policy enforcement
* Bayesian spam filtering
* Endpoint Detection and Response (EDR)
* single management console
Explanation

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

NO.38 According to Netskope. what are two preferred methods to report a URL miscategorization? (Choose two.)
* Use www.netskope.com/url-lookup.
* Use the URL Lookup page in the dashboard.
* Email support@netskope.com.
* Tag Netskope on Twitter.
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. References: [Netskope URL Lookup], Netskope Security Cloud Operation & Administration (NSCO&A) – Classroom Course, Module 8: Skope IT, Lesson 2: Page Events.

NO.39 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.)
* Use the Netskope reporting engine.
* Export the data from Skope IT Application Events.
* Use the Netskope REST API.
* Export the data from Skope IT Alerts.
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. References: [Netskope Skope IT Application Events],

[Netskope REST API].

NO.40 Which two cloud security and infrastructure enablement technologies does Secure Access Service Edge (SASE) combine into its unified platform? (Choose two.)
* Distributed Denial of Service Protection (DDoS)
* Zero Trust Network Access (ZTNA)
* Cloud Access Security Broker (CASB)
* Unified Threat Management (UTM)

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. References: [SASE], [ZTNA],

[CASB].

NO.41 You are working with a large retail chain and have concerns about their customer data. 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?
* SOC 3
* PCI-DSS
* AES-256
* ISO 27001

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, andincident 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. References: [PCI-DSS], [SOC 3], [AES-256],

[ISO 27001].

NO.42 What are two fundamental differences between the inline and API implementation of the Netskope platform?

(Choose two.)

* The API implementation can be used with both sanctioned and unsanctioned applications.
* The API implementation can only be used with sanctioned applications.
* The inline implementation can effectively block a transaction in both sanctioned and unsanctioned applications.
* The inline implementation can only effectively block a transaction in sanctioned applications.

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. References: [Netskope SaaS API-enabled Protection], [Netskope Inline CASB].

NO.43 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.)

* The pre-shared key for the GRE tunnel is incorrect.
* The configured GRE peer in the Netskope platform is incorrect.
* The corporate firewall might be blocking GRE traffic.
* The route map was applied to the wrong router interface.
* Netskope does not support GRE tunnels.

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 tunnelsdo not use pre-shared keys for authentication or encryption.

Netskope does support GRE tunnels, so this is not a cause for this issue either. References: [Netskope Secure Forwarder], Netskope Security Cloud Operation & Administration (NSCO&A) – Classroom Course, Module

3: Steering Configuration, Lesson 3: Secure Forwarder.

NO.44 When would an administrator need to use a tombstone file?

* You use a tombstone file when a policy causes a file download to be blocked.
* You use a tombstone file when a policy causes a publicly shared file to be encrypted.

* You use a tombstone file when the policy causes a file to be moved to quarantine.
* You use a tombstone file when a policy causes a file to be moved to legal hold.

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. References: Threat Protection – Netskope Knowledge PortalNetskope threat protection – Netskope

NO.45 You want to set up a Netskope API connection to Box.

What two actions must be completed to enable this connection? (Choose two.)
* Install the Box desktop sync client.
* Authorize the Netskope application in Box.
* Integrate Box with the corporate IdP.
* Configure Box in SaaS API Data protection.

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. References: Authorize Netskope Introspection App on Box Enterprise – Netskope Knowledge PortalConfigure Box Instance in Netskope UI – Netskope Knowledge Portal

NO.46 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?
* You can find DLP violations under Forensic profiles.
* DLP incidents for a file are not visible when the file is deleted.
* You can find DLP violations under the Incidents dashboard.
* You must create a forensic profile so that an incident is created.

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. References: Netskope Incidents Dashboard

NO.47 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.)
* Allow the user to browse uncategorized domains but restrict edit activities.
* Block malware detected on download activity for all remaining categories.
* Block known bad websites and enable RBI to uncategorized domains.

* Allow a limited amount of domains and block everything else.
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. References: [Netskope Threat Protection],

[Netskope Remote Browser Isolation].