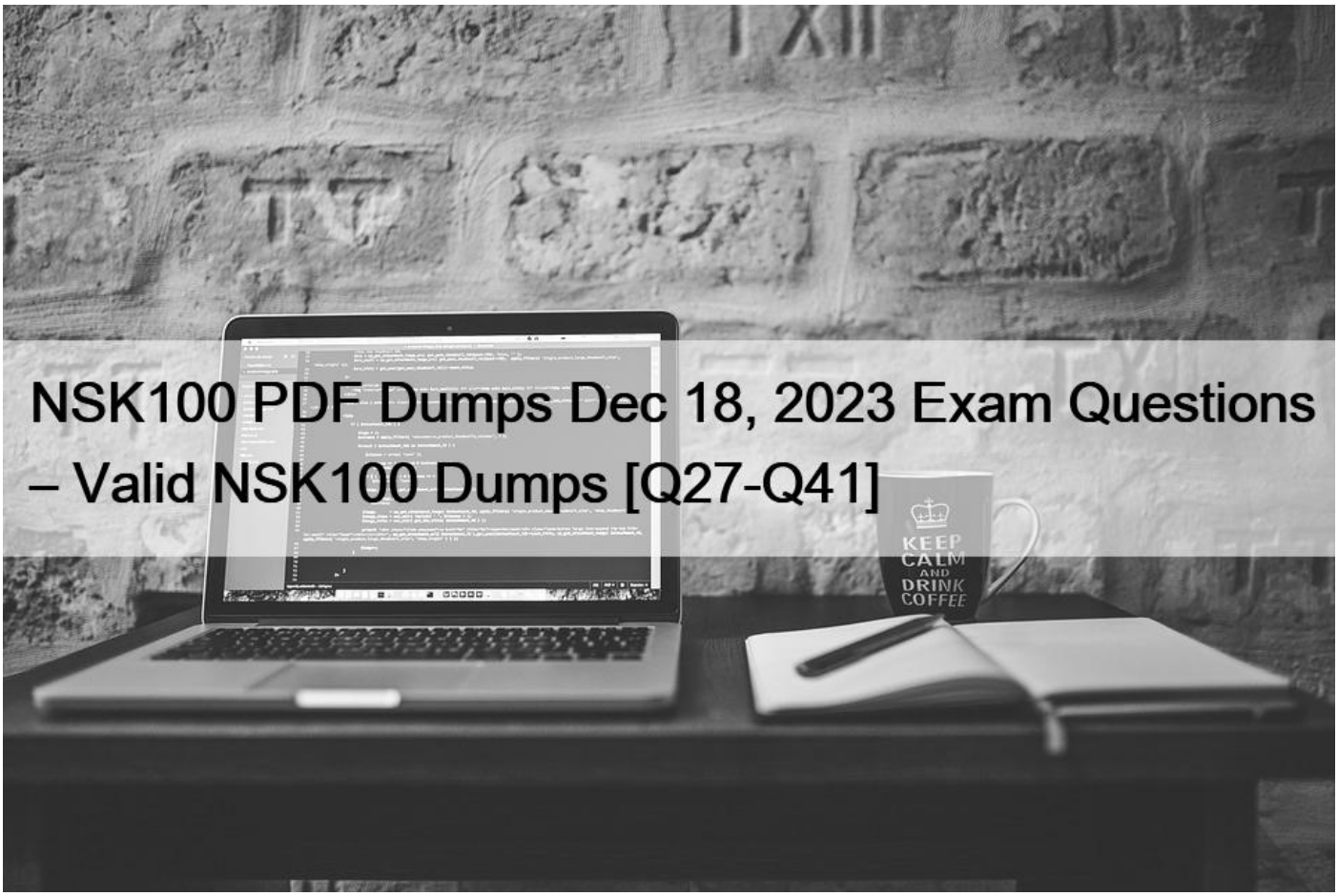
NSK100 PDF Dumps Dec 18, 2023 Exam Questions ? Valid NSK100 Dumps [Q27-Q41



NSK100 PDF Dumps Dec 18, 2023 Exam Questions – Valid NSK100 Dumps
Ultimate NSK100 Guide to Prepare Free Latest Netskope Practice Tests Dumps

NEW QUESTION 27

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.)
* Sanctioned = No
* CCL = High. Under Research
* User Device Type = Windows Device
* CCL = Medium. Low, Poor

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 ofunsanctioned 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. References: SkopeIT ApplicationsNetskope Cloud Confidence Index

NEW QUESTION 28

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

In this scenario, which Netskope feature would you recommend to the customer?
* Netskope Advanced DLP and Threat Protection
* Netskope Secure Web Gateway (SWG)
* Netskope SaaS Security Posture Management (SSPM)
* Netskope Cloud Security Posture Management (CSPM)

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. References: Netskope CSPMCloud Security Posture Management

NEW QUESTION 29

Which two statements are correct about DLP Incidents in the Netskope platform? (Choose two.)
* An incident can be associated to one or more DLP policies.
* An incident can have one or more DLP violations.
* An incident can be assigned to one or more administrators.
* An incident can be associated to one or more DLP rules.

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. References: About DLPDLP Profiles

NEW QUESTION 30

You want to block access to sites that use self-signed certificates. Which statement is true in this scenario?
* Certificate-related settings apply globally to the entire customer tenant.

* Certificate-related settings apply to each individual steering configuration level.
* Certificate-related settings apply to each individual client configuration level.
* Self-signed certificates must be changed to a publicly trusted CA signed certificate.

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. References: Netskope SSL DecryptionNetskope Steering Configuration

NEW QUESTION 31

What are two characteristics ofNetskope’s Private Access Solution? (Choose two.)

* It provides protection for private applications.
* It provides access to private applications.
* It acts as a cloud-based firewall.
* It requires on-premises hardware.

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. Itdoes not require on-premises hardware, as it is a cloud-native solution that leverages Netskope’s global network of points of presence (POPs). References: [Netskope Private Access].

NEW QUESTION 32

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

NEW QUESTION 33

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

* log parser

* DLP
* sandbox
* heuristics

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 URLsfrom 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. References: [Netskope Threat Protection], Netskope Security Cloud Operation & Administration (NSCO&A) – Classroom Course, Module 9: Threat Protection.

NEW QUESTION 34

You want to deploy Netskope’s zero trust network access (ZTNA) solution, NPA. In this scenario, which action would you perform to accomplish this task?

* Create an OAuth identity access control between your users and your applications.
* Set up a reverse proxy using SAML and an identity provider.
* Enable Steer all Private Apps in your existing steering configuration(s) from the admin console.
* Configure SCIM to exchange identity information and attributes with your applications.

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. References: [Netskope Private Access (NPA) Deployment Guide]

NEW QUESTION 35

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

* blocking file uploads to a personal Box account
* running a retroactive scan for data at rest in Google Drive
* using the Netskope steering client to provide user alerts when sensitive information is posted in Slack
* scanning Dropbox for credit card information

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. References: Netskope Inline Proxy ModeNetskope Steering Client [Netskope DLP Engine]

NEW QUESTION 36

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

NEW QUESTION 37

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

In this scenario, which Netskope feature would you recommend to the customer?
* Netskope Secure Web Gateway (SWG)
* Netskope Cloud Security Posture Management (CSPM)
* Netskope Advanced DLP and Threat Protection
* Netskope SaaS Security Posture Management (SSPM)
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. References: Netskope CSPMCloud Security Posture Management

NEW QUESTION 38

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?
* DLP Rule
* real-time policy

* DLP Profile
* block notification

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 sub-components or outcomes of a real-time policy. References: 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 39

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.)

* Use a forward proxy.
* Use an API connector
* Use a log parser.
* Use a reverse proxy.

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. References: [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 40

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?

* DLP forensics
* Risk Insights
* laaS API-enabled Protection
* SaaS API-enabled Protection

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

NEW QUESTION 41

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?

* Skope IT-> Alerts
* Incidents -> DLP
* API-enabled Protection -> Inventory
* Reports -> New Report

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. References: Netskope Incidents Dashboard