Netskope.NSK101.by.Matin.58q

Number: NSK101
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: NSK101

Exam Name: Netskope Certified Cloud Security Administrator Exam

Exam A

QUESTION 1

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

Correct Answer: A, B
Section:
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 2

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.

Correct Answer: B, C
Section:
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 3
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.

Correct Answer: A, B
Section:
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 4
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

Correct Answer: C
Section:
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 5
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

Correct Answer: C
Section:
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.
Netskope architecture documentation describing the roles of different components.
Detailed guides on how API-enabled protection integrates with the Netskope Data Plane for real-time traffic inspection.

QUESTION 6
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

Correct Answer: A
Section:
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.
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 7
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

Correct Answer: A, C, E
Section:
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.
Netskope documentation on using the NPA Troubleshooter Tool and the status indicators it provides.
Best practices for troubleshooting NPA connectivity and performance issues.

QUESTION 8
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.

Correct Answer: D
Section:
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 9
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

Correct Answer: B, C
Section:
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 10
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.

Correct Answer: A, B
Section:
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 11
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'.

Correct Answer: B
Section:
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 12
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

Correct Answer: A, D
Section:
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 13
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

Correct Answer: A, D
Section:
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 14
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?

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

Correct Answer: B
Section:
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 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

Correct Answer: B
Section:
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.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 16
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

Correct Answer: B, C, E
Section:
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 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. laaS API-enabled Protection
D. SaaS API-enabled Protection

Correct Answer: D
Section:
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 18
You need to create a service request ticket for a client-related issue using the Netskope client Ul. In this scenario, you generate the client logs by right-clicking on the system tray icon and choosing

A. Save logs
B. Configuration
C. Troubleshoot
D. Help

Correct Answer: C
Section:
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 19
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

Correct Answer: A, D
Section:
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.Reference:Netskope SASEWhat is SASE?

QUESTION 20
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.

Correct Answer: D
Section:
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 PortHow to explain Source IP Address, Destination IP Address & Service in easy way

QUESTION 21
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.

Correct Answer: B, C, D
Section:
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.

QUESTION 22
What are two pillars of CASB? (Choose two.)

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

Correct Answer: A, B
Section:
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)? | MicrosoftCASB Guide: What are the 4 Pillars of CASB? - Security Service Edge

QUESTION 23
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.

Correct Answer: B, D
Section:
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 PortalConfigure Box Instance in Netskope UI - Netskope Knowledge Portal

QUESTION 24
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

Correct Answer: A, B
Section:
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 25
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.

Correct Answer: B
Section:
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 26
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.

Correct Answer: B, D
Section:
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 ConnectorUser Provisioning with Azure AD

QUESTION 27
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.

Correct Answer: C
Section:
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 Knowledge PortalNetskope threat protection - Netskope

QUESTION 28
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

Correct Answer: A, B
Section:
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 29
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.

Correct Answer: A, D
Section:
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 30
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 paqes under Settinqs

Correct Answer: A, D
Section:
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.

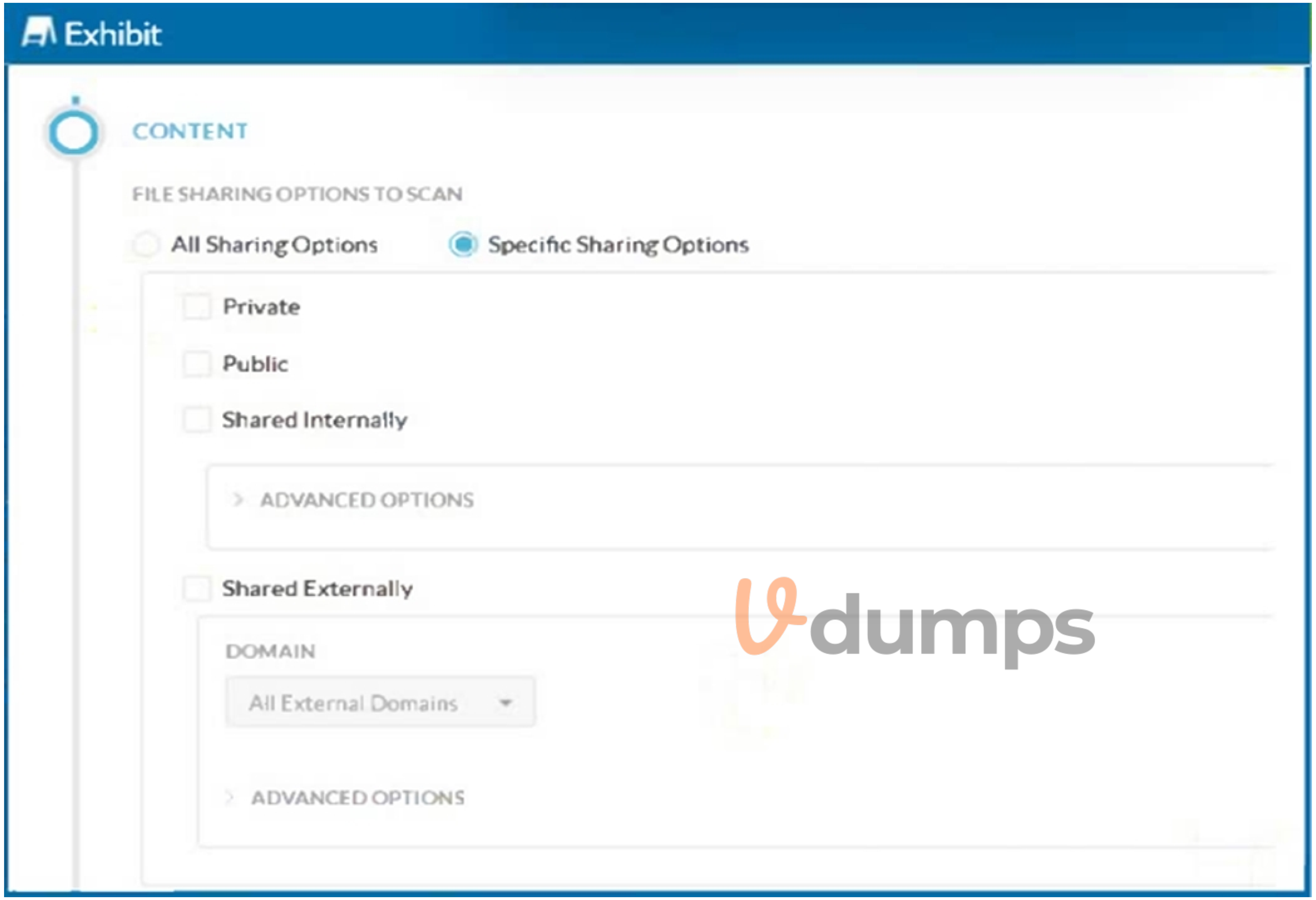
These details are confirmed based on the features and configurations available within the Netskope Admin UI settings, as documented in the Netskope Knowledge Portal.

QUESTION 31
You need to locate events for specific activities such as 'edit' or 'login successful' in a cloud application.
In which SkopeIT Events & Alerts page would this information be found?

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

Correct Answer: C
Section:
Explanation:
The Application Events page in the SkopeIT 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.
========
REST API v2 Overview - Netskope Knowledge Portal
Using the REST API v2 UCI Impact Endpoints - Netskope Knowledge Portal
Postman Collection for Netskope API

QUESTION 32
Click the Exhibit button.



Exhibit

CONTENT

FILE SHARING OPTIONS TO SCAN

○ All Sharing Options ● Specific Sharing Options

□ Private

□ Public

□ Shared Internally

> ADVANCED OPTIONS

□ Shared Externally

DOMAIN

All External Domains ▾

> ADVANCED OPTIONS

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.

Correct Answer: B
Section:
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.
Netskope CASB Policy Configuration Documentation

QUESTION 33
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.

Correct Answer: B
Section:
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.
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

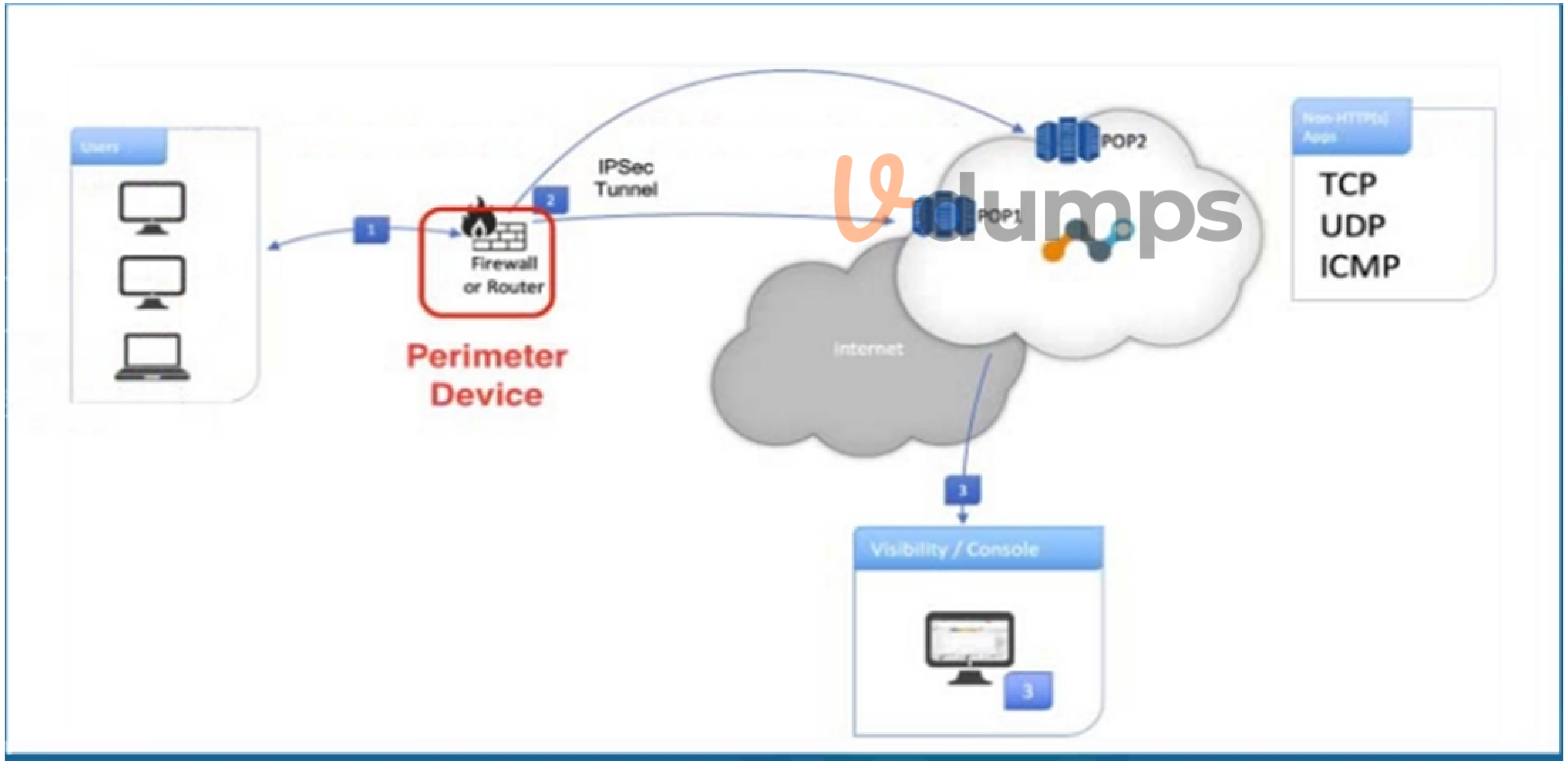
QUESTION 34
You added a new private app definition and created a Real-time Protection policy to allow access for all users. You have a user who reports that they are unable to access the application but all other applications work fine.
Which statement correctly describes how to troubleshoot this issue using the Netskope Web UI?

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

Correct Answer: D
Section:
Explanation:
When a user is unable to access a newly added private application despite having the correct Real-time 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.
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 35
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.)

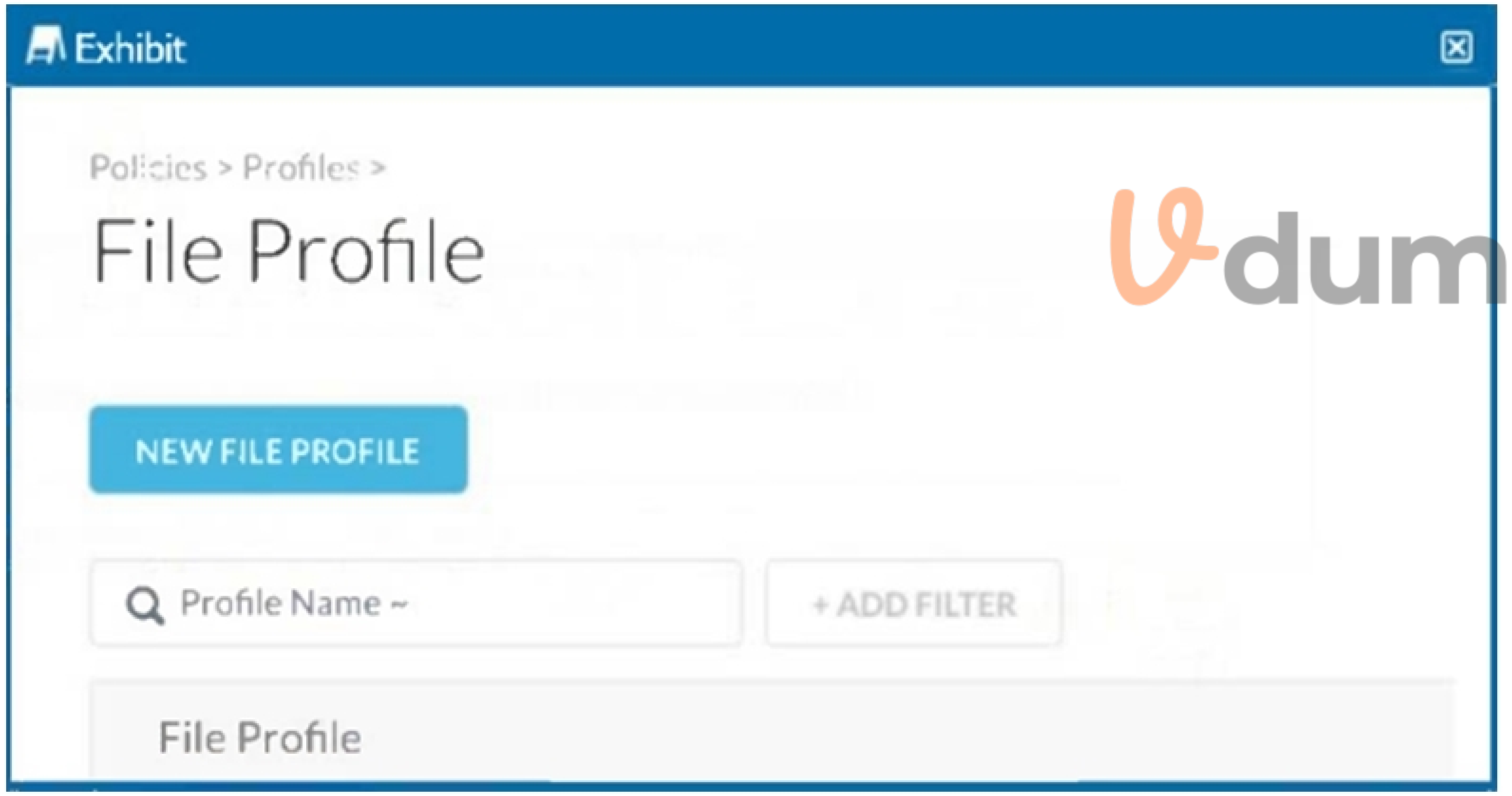
A. Enable IKE Dead Peer Detection (DPD) for each tunnel.
B. Send ICMP requests to the Netskope location's Probe IP

C. Send HTTP requests to the Netskope location's Probe IP.

D. Send ICMP requests to the Netskope location's proxy IPs.

Correct Answer: A, B
Section:
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:
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:
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.
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 36
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.

Correct Answer: A, C
Section:

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:

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:

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.

REST API v2 Overview - Netskope Knowledge Portal

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

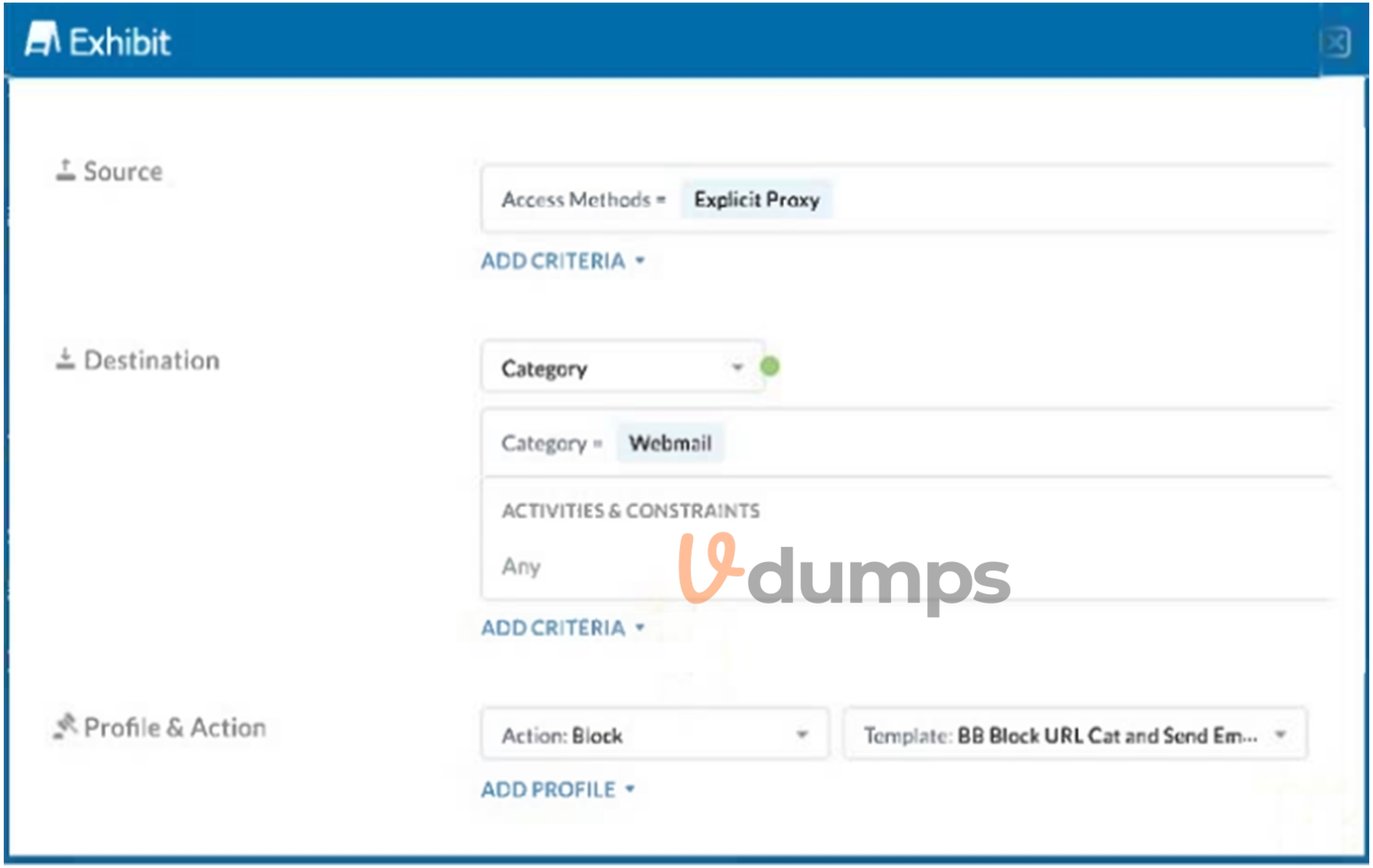
Using the REST API v2 UCI Impact Endpoints - Netskope Knowledge Portal

netskopesdk * PyPI

Netskope Rest APIv2(OAS 3.1) - Postman Collection

QUESTION 37

Click the Exhibit button.



A user has the Netskope Client enabled with the correct steering configuration applied. The exhibit shows an inline policy that has a predefined webmail category blocked. However the user is still able to access Yahoo mail. Which statement is correct in this scenario?

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.

Correct Answer: C
Section:
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.
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 38
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

Correct Answer: C
Section:
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.
Netskope Knowledge Portal: Using DLP Profiles and Policies.

QUESTION 39
You are attempting to allow access to an application using NPA. 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.

Correct Answer: B, C

Section:
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.
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.

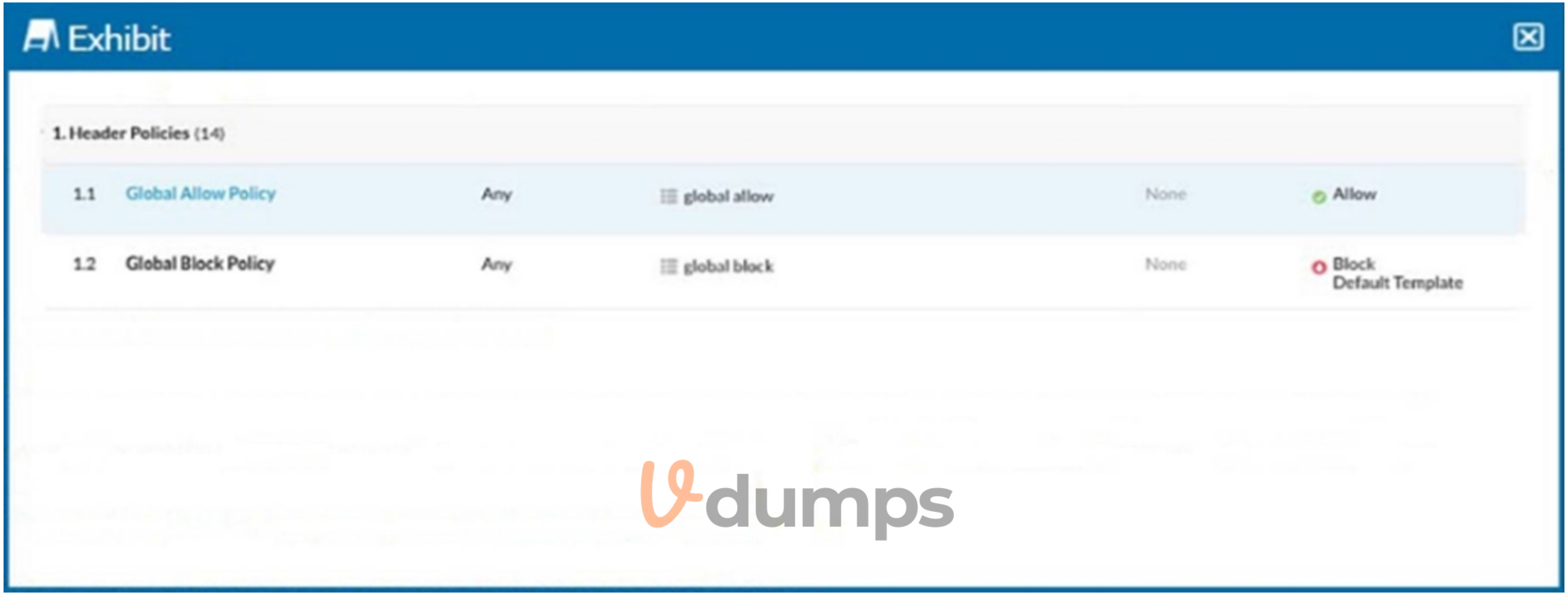
QUESTION 40
Your organization has recently implemented Netskope Private Access. During an investigation, your security team has asked you to provide a list of all hosts including domains and IP addresses that a user accessed through Netskope Private Access for the past seven days.
Which two locations 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

Correct Answer: A, C
Section:
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.
Netskope Knowledge Portal: Using SkopeIT for Network and Private Apps Analysis.

QUESTION 41

Click the Exhibit button.



1. Header Policies (14)

1.1	Global Allow Policy	Any	global allow	None	Allow
1.2	Global Block Policy	Any	global block	None	Block Default Template

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 forthat 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.

Correct Answer: B, C

Section:

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

QUESTION 42
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.

Correct Answer: C
Section:
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 43
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

Correct Answer: B
Section:
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 44
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

Correct Answer: B
Section:
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 45
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.

Correct Answer: A, B
Section:
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.
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.
Netskope Knowledge Portal: Detailed guides on collecting logs via the Netskope Console and client applications.

QUESTION 46
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

Correct Answer: B
Section:
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.
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 47
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.

Correct Answer: C, D
Section:
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 48
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 polices 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.

Correct Answer: A, B
Section:

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 49
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.

Correct Answer: B
Section:
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.
'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 50
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 SkopeIT.
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.

Correct Answer: A, B
Section:
Explanation:
In a CASB-only deployment of Netskope, there could be several reasons why Dropbox.com traffic is not visible in SkopeIT:
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 SkopeIT. Ensuring that the domains are configured correctly is essential for the traffic to be captured and analyzed by Netskope.
'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 51

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 SkopeIT Applications page to satisfy this requirement? (Choose two.)

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

Correct Answer: A, B
Section:
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 SkopeIT 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.
Netskope Knowledge Portal: REST API v2 Overview.
Postman Collection: API v2.

QUESTION 52
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

Correct Answer: A, C
Section:
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.
Using the REST API v2 UCI Impact Endpoints.
Netskope Knowledge Portal: Dataexport Iterator Endpoints.

QUESTION 53
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. Leaal Hold

Correct Answer: B
Section:

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.
Netskope REST API Overview.
Netskope SDK Documentation.

QUESTION 54

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

Correct Answer: A, C
Section:
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.
Netskope Knowledge Portal: Private Access
Netskope Private Access Troubleshooter

QUESTION 55

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.

Correct Answer: A, B, D
Section:
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.
Netskope Private Access Deployment Guide
Netskope REST API v2 Overview

QUESTION 56
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

Correct Answer: C
Section:
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 57
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

Correct Answer: A
Section:
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 58
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

Correct Answer: C
Section:
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.