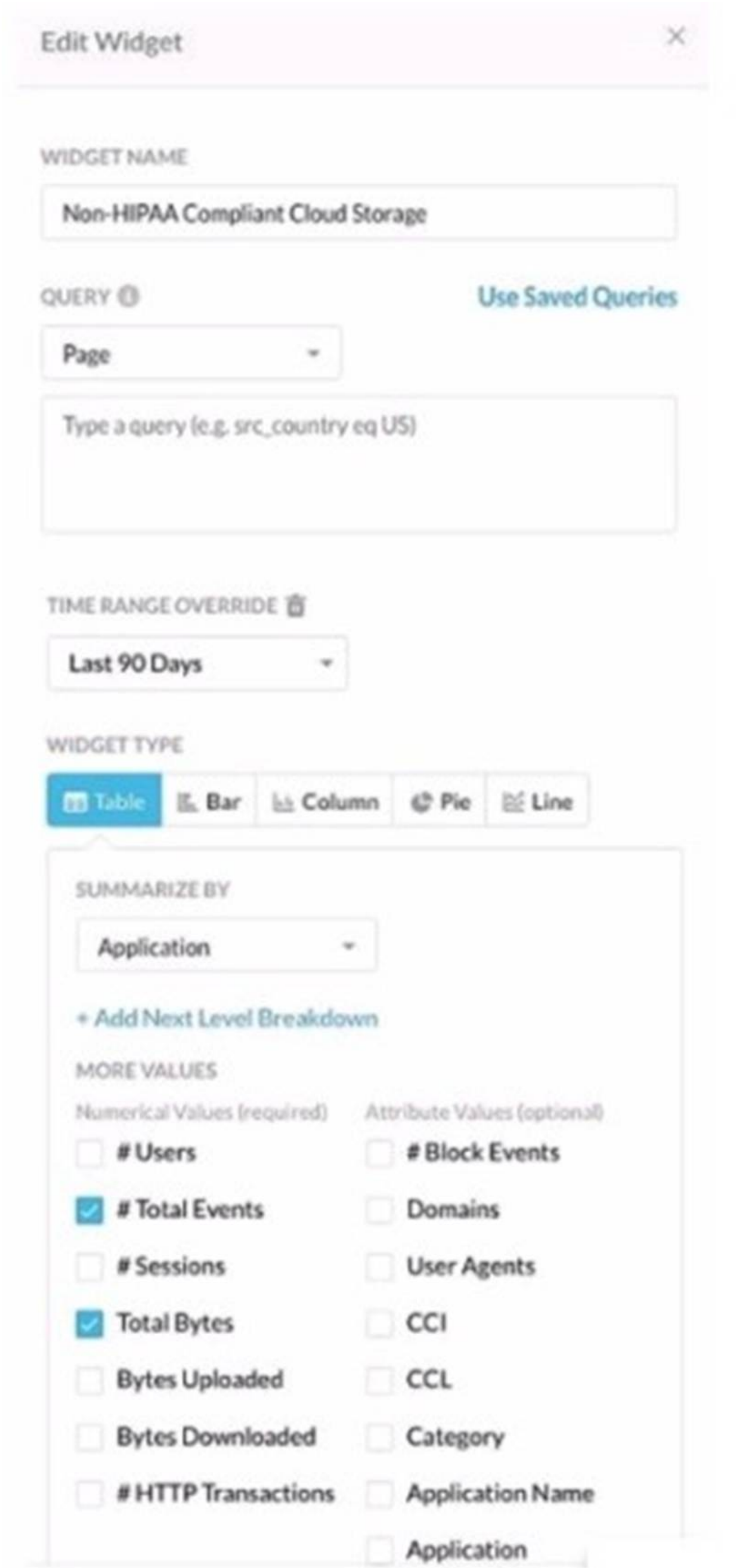
Netskope

Exam Questions NSK300

Netskope Certified Cloud Security Architect Exam

NEW QUESTION 1
Review the exhibit.


Edit Widget
WIDGET NAME
Non-HIPAA Compliant Cloud Storage
QUERY
Use Saved Queries
Page
Type a query (e.g. src_country eq US)
TIME RANGE OVERRIDE
Last 90 Days
WIDGET TYPE
Table
Bar
Column
Pie
Line
SUMMARIZE BY
Application
+ Add Next Level Breakdown
MORE VALUES
Numerical Values (required)
Attribute Values (optional)
Users
Block Events
Total Events
Domains
Sessions
User Agents
Total Bytes
CCI
Bytes Uploaded
CCL
Bytes Downloaded
Category
HTTP Transactions
Application Name
Application

You work for a medical insurance provider. You have Netskope Next Gen Secure Web Gateway deployed to all managed user devices with limited block policies. Your manager asks that you begin blocking Cloud Storage applications that are not HIPAA compliant Prior to implementing this policy, you want to verity that no business or departmental applications would be blocked by this policy.
Referring to the exhibit, which query would you use in the Edit Widget window to narrow down the results?

A. app-ccl-compliance-cert neq 'HIPAA' and category eq 'Cloud Storage'
B. Cloud Confidence Compliance neq HIPAA and Cloud Confidence Category is Cloud Storage
C. SELECT application WHERE 'HIPAA' NOT IN app-cci-compliance AND WHERE 'Cloud Storage' IN category
D. app-compliance does not contain HIPAA and category must equal Cloud Storage

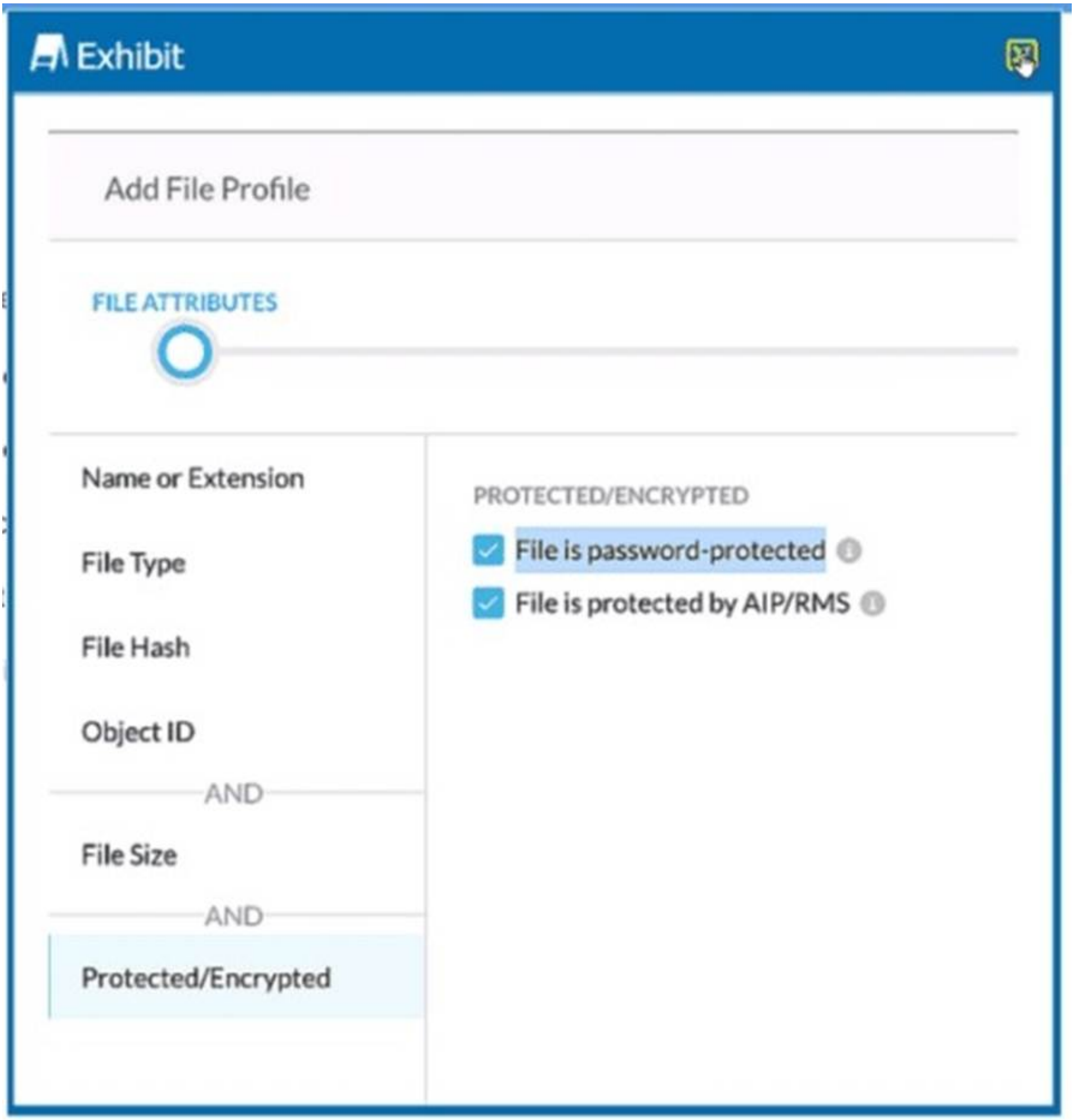
Answer: A

NEW QUESTION 2
You jus! deployed and registered an NPA publisher for your first private application and need to provide access to this application for the Human Resources (HR) users group only. How would you accomplish this task?

A. 1. Enable private app steering in the Steering Configuration assigned to the HR group.* 2. Create a new Private App.* 3. Create a new Real-time Protection policy as follows;Source = HR user group Destination = Private App Action = Allow
B. 1. Create a new private app and assign it to the HR user group.* 2. Create a new Real-time Protection policy as follows:Source = HR user group Destination = Private App Action = Allow.
C. 1. Enable private app steering in Tenant Steering Configuration.* 2. Create a new private app and assign it to the HR user group.
D. 1. Enable private app steering in the Steering Configuration assigned to the HR group.* 2. Create a new private app and assign it to the HR user group* 3. Create a new Real-time Protection policy as follows:Source = HR user group Destination = Private App Action = Allow

Answer: A

NEW QUESTION 3
Review the exhibit.



You are attempting to block uploads of password-protected files. You have created the file profile shown in the exhibit.
Where should you add this profile to use in a Real-time Protection policy?

A. Add the profile to a DLP profile that is used in a Real-time Protection policy.
B. Add the profile to a Malware Detection profile that is used in a Real-time Protection policy.
C. Add the profile directly to a Real-time Protection policy as a Constraint.
D. Add the profile to a Constraint profile that is used in a Real-time Protection policy.

Answer: A

NEW QUESTION 4
Review the exhibit.

You are the proxy administrator for a medical devices company. You recently changed a pilot group of users from cloud app steering to all Web traffic. Pilot group

users have started to report that they receive the error shown in the exhibit when attempting to access the company intranet site that is publicly available. During troubleshooting, you realize that this site uses your company's internal certificate authority for SSL certificates.
Which three statements describe ways to solve this issue? (Choose three.)

A. Import the root certificate for your internal certificate authority into Netskope.
B. Bypass SSL inspection for the affected site(s).
C. Create a Real-time Protection policy to allow access.
D. Change the SSL Error Settings from Block to Bypass in the Netskope tenant.
E. Instruct the user to proceed past the error message

Answer: ABD

NEW QUESTION 5
You are attempting to merge two Advanced Analytics reports with DLP incidents: Report A with 3000 rows and Report B with 6000 rows. Once merged, you notice that the merged report is missing a significant number of rows.
What is causing this behavior?

A. Netskope automatically deduplicates data in merged reports.
B. Missing data is due to viewing limits.
C. Filters are applied differently to dimensions and measures
D. Visualizations have a system limit of 5000 rows.

Answer: B

Explanation:
When merging two Advanced Analytics reports in Netskope, if the merged report is missing rows, it is likely due to viewing limits within the system. Netskope??s Advanced Analytics platform has limitations on the number of rows that can be viewed at once, which can result in missing data when dealing with large reports. This viewing limit ensures performance and manageability of the data within the system.
[: The behavior of data viewing limits in Netskope Advanced Analytics is discussed in the Netskope Knowledge Portal, which provides insights into how data is explored and managed within the platform1,]

NEW QUESTION 6
You are implementing a solution to deploy Netskope for machine traffic in an AWS account across multiple VPCs. You want to deploy the least amount of tunnels while providing connectivity for all VPCs.
How would you accomplish this task?

A. Use IPsec tunnels from the AWS Virtual Private Gateway.
B. Use GRE tunnels from the AWS Transit Gateway.
C. Use GRE tunnels from the AWS Virtual Private Gateway
D. Use IPsec tunnels from the AWS Transit Gateway.

Answer: D

NEW QUESTION 7
You deployed Netskope Cloud Security Posture Management (CSPM) using pre-defined benchmark rules to monitor your cloud posture in AWS, Azure, and GCP. You are asked to assess if you can extend the Netskope CSPM solution by creating custom rules for each environment.
Which statement is correct?

A. Custom rules using Domain Specific Language are only available when using SSPM.
B. You will need to evaluate SaaS Security Posture Management (SSPM) in addition to CSPM so that rules applied to GCP will align with Google Workspace
C. With Netskope CSPM, you can create custom rules using Domain Specific Language for AW
D. Azure, but not for GCP.
E. With Netskope CSPM, you can create custom rules using Domain Specific Language for AW
F. Azure, and GCP

Answer: D

Explanation:
Netskope Cloud Security Posture Management (CSPM) allows for the creation of custom rules using Domain Specific Language (DSL) for all three major cloud platforms: AWS, Azure, and GCP. This capability is integral to CSPM and enables organizations to tailor their security posture assessments to their specific needs across different cloud environments.
[: The ability to create custom rules using DSL within Netskope CSPM for AWS, Azure, and GCP is documented in the Netskope Knowledge Portal.It provides detailed instructions on how to build custom rules under Policies > Security Posture > Profiles & Rules for security assessment of resources across these cloud platforms,]

NEW QUESTION 8
Your organization's software deployment team did the initial install of the Netskope Client with SCCM. As the Netskope administrator, you will be responsible for all up-to-date upgrades of the client.
Which two actions would be required to accomplish this task9 (Choose two.)

A. In the Client Configuration, set Upgrade Client Automatically to Latest Release.
B. Set the installmode-IDP flag during the original Install.
C. Set the autoupdate-on flag during the original Install.
D. In the Client Configuration, set Upgrade Client Automatically to Specific Golden Release.

Answer: AC

NEW QUESTION 9

You are building an architecture plan to roll out Netskope for on-premises devices. You determine that tunnels are the best way to achieve this task due to a lack of support for explicit proxy in some instances and IPsec is the right type of tunnel to achieve the desired security and steering.
What are three valid elements that you must consider when using IPsec tunnels in this scenario? (Choose three.)

A. cipher support on tunnel-initiating devices
B. bandwidth considerations
C. the categories to be blocked
D. the impact of threat scanning performance
E. Netskope Client behavior when on-premises

Answer: ABD

NEW QUESTION 10
A company needs to block access to their instance of Microsoft 365 from unmanaged devices. They have configured Reverse Proxy and have also created a policy that blocks login activity for the AD group "marketing-users" for the Reverse Proxy access method. During UAT testing, they notice that access from unmanaged devices to Microsoft 365 is not blocked for marketing users. What is causing this issue?

A. There is a missing group name in the SAML response.
B. The username in the name ID field is not in the format of the e-mail address.
C. There is an invalid certificate in the SAML response.
D. The username in the name ID field does not have the "marketing-users" group name.

Answer: A

NEW QUESTION 10
You recently began deploying Netskope at your company. You are steering all traffic, but you discover that the Real-time Protection policies you created to protect Microsoft OneDrive are not being enforced.
Which default setting in the Ul would you change to solve this problem?

A. Disable the default Microsoft appsuite SSL rule.
B. Disable the default certificate-pinned application
C. Remove the default steering exception for domains.
D. Remove the default steering exception for Cloud Storage.

Answer: C

NEW QUESTION 14
What are three valid Instance Types for supported SaaS applications when using Netskope's API-enabled Protection? (Choose three.)

A. Forensic
B. API Data Protection
C. Behavior Analytics
D. DLP Scan
E. Quarantine

Answer: ABE

NEW QUESTION 16
You have deployed Netskope to all users of the organization and you are now ready to begin ingesting all events, alerts, and Web transactions into your SIEM as a part of your requirements.
What are three ways in which you would accomplish this task? (Choose three.)

A. Use custom API calls to ingest to a data lake and then into your SIEM.
B. Use the Netskope Publisher to a stream syslog to your SIEM.
C. Use syslog directly to Splunk.
D. Use Cloud Log Shipper to an IaaS storage repository and then into your SIEM.

Answer: ACD

NEW QUESTION 18
A company's architecture includes a server subnet that is logically isolated from the rest of the network with no Internet access, no default gateway, and no access to DNS. New resources can only be provisioned on virtual resources in that segment and there is a firewall that is tunnel-capable securing the perimeter of the segment. The only requirement is to have content filtering for any server that might access the Internet using a browser.
Which two Netskope deployment methods would achieve this requirement? (Choose two.)

A. Deploy a mobile profile on the servers.
B. Deploy Data Plane on Premises (DPoP) with a proxy configuration on the servers.
C. Deploy IPsec or GRE tunnels in the segment to steer traffic from the servers to Netskope.
D. Install the Netskope Client on the servers

Answer: BC

NEW QUESTION 20
You have multiple networking clients running on an endpoint and client connectivity is a concern. You are configuring co-existence with a VPN solution in this scenario, what is recommended to prevent potential routing issues?

A. Configure the VPN to split tunnel traffic by adding the Netskope IP and Google DNS ranges and set to Exclude in the VPN configuration.

B. Modify the VPN to operate in full tunnel mode at Layer 3. so that the Netskope agent will always see the traffic first.
C. Configure the VPN to full tunnel traffic and add an SSL Do Not Decrypt policy to the VPN configuration for all Netskope traffic.
D. Configure a Network Location with the VPN IP ranges and add it as a Steering Configuration exception.

Answer: B

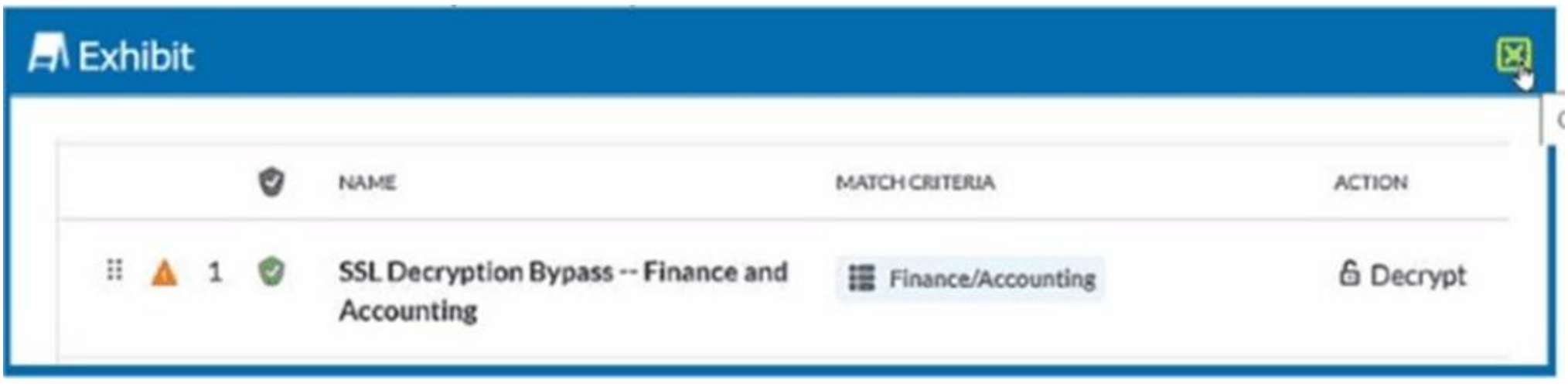
Explanation:
To prevent potential routing issues and ensure that the Netskope agent consistently sees the traffic first, it is recommended tomodify the VPN to operate in full tunnel mode at Layer 3.
In full tunnel mode, all traffic from the endpoint is routed through the VPN, including traffic destined for Netskope. This ensures that the Netskope agent can inspect and apply policies to all traffic, regardless of the destination.
Layer 3 full tunnel mode provides better visibility and control over the traffic flow, reducing the risk of routing conflicts or bypassing the Netskope inspection.References:
The answer is based on general knowledge of VPN configurations and their impact on traffic routing.

NEW QUESTION 23
A hospital has a patient form that they share with their patients over Gmail. The blank form can be freely shared among anyone. However, if the form has any information filled out. the document is considered confidential.
Which rule type should be used in the DLP profile to match such a document?

A. Use fingerprint classification.
B. Use a dictionary rule for all your patient names.
C. Use Exact Match with patient names
D. Use predefined DLP Rule(s) that match the patient name.

Answer: A

NEW QUESTION 25
Review the exhibit.



You created an SSL decryption policy to bypass the inspection of financial and accounting Web categories. However, you still see banking websites being inspected.
Referring to the exhibit, what are two possible causes of this behavior? (Choose two.)

A. The policy is in a "disabled" state.
B. An incorrect category has been selected
C. The policy is in a "pending changes" state.
D. An incorrect action has been specified.

Answer: BD

NEW QUESTION 26
You need to extract events and alerts from the Netskope Security Cloud platform and push it to a SIEM solution. What are two supported methods to accomplish this task? (Choose two.)

A. Use Cloud Ticket Orchestrator.
B. Use Cloud Log Shipper.
C. Stream directly to syslog.
D. Use the REST API.

Answer: BD

NEW QUESTION 31
You built a number of DLP profiles for different sensitive data types. If a file contains any of this sensitive data, you want to take the most restrictive policy action but also create incident details for all matching profiles.
Which statement is correct in this scenario?

A. Create a Real-time Protection policy for each DLP profile; each matched profile will generate a unique DLP incident.
B. Create a Real-time Protection policy for each DLP profile; all matched profiles will show up in a single DLP incident
C. Create a single Real-time Protection policy and include all of the DLP profiles; each matched profile will generate a unique DLP incident
D. Create a single Real-time Protection policy and include all of the DLP profiles; all matched profiles will show up in a single DLP incident.

Answer: D

NEW QUESTION 33

You created a Real-time Protection policy that blocks all activities to non-corporate S3 buckets, but determine that the policy is too restrictive. Specifically, users are complaining that normal websites have stopped rendering properly.
How would you solve this problem?

A. Create a Real-time Protection policy to allow the Browse activity to the Amazon S3 application.
B. Create a Real-time Protection policy to allow the Browse activity to the Cloud Storage category
C. Create a Real-time Protection policy to allow the Download activity to the Cloud Storage category
D. Create a Real-time Protection policy to allow the Download activity to the Amazon S3 application

Answer: B

NEW QUESTION 36
You are designing a Netskope deployment for a company with a mixture of endpoints, devices, and services.
In this scenario, what would be two considerations for using IPsec as part of the design? (Choose two.)

A. guest Wi-Fi network users
B. corporate-managed Mac computers
C. remote unmanaged Windows PCs
D. Internet-connected IoT devices

Answer: AD

NEW QUESTION 38
You are troubleshooting an issue with users who are unable to reach a financial SaaS application when their traffic passes through Netskope. You determine that this is because of IP restrictions in place with the SaaS vendor. You are unable to add Netskope's IP ranges at this time, but need to allow the traffic.
How would you allow this traffic?

A. Use NPAto implement Source IP anchonng so the traffic will egress from the corporate data center.
B. Use Explicit Proxy Over Tunnel (EPoT) so the traffic will egress from the corporate data center.
C. Use Cloud Explicit Proxy so the traffic will egress from the corporate data center
D. Use an IPsec tunnel to forward traffic so it will egress from the corporate data center

Answer: B

NEW QUESTION 42
You want to integrate with a third-party DLP engine that requires ICAP. In this scenario, which Netskope platform component must be configured?

A. On-Premises Log Parser (OPLP)
B. Secure Forwarder
C. Netskope Cloud Exchange
D. Netskope Adapter

Answer: B

NEW QUESTION 47
You are currently designing a policy for AWS S3 bucket scans with a custom DLP profile Which policy action(s) are available for this policy?

A. Alert, Quarantin
B. Block, User Notification
C. Alert, User Notification
D. Alert only
E. Alert, Quarantine

Answer: D

Explanation:
When designing a policy for AWS S3 bucket scans with a custom DLP profile in Netskope, the available policy actions are Alert and Quarantine . These actions allow you to be notified when a policy violation occurs and to quarantine sensitive data to prevent potential data loss or exposure. The Alert action will notify the designated personnel or system when a match to the DLP profile is found during the scan. The Quarantine action will move the offending file to a secure location where it can be reviewed and dealt with appropriately 1 .
[: The information about policy actions for AWS S3 bucket scans is available in the Netskope documentation, which provides guidance on creating API Data Protection policies for scanning S3 buckets and the actions that can be taken when a policy is triggered1.,]

NEW QUESTION 52
You want to enable the Netskope Client to automatically determine whether it is on- premises or off-premises. Which two options in the Netskope Ul would you use to accomplish this task? (Choose two.)

A. the All Traffic option in the Steering Configuration section of the Ul
B. the New Exception option in the Traffic Steering options of the Ul
C. the Enable Dynamic Steering option in the Steering Configuration section of the Ul
D. the On Premises Detection option under the Client Configuration section of the Ul

Answer: CD

Explanation:
To enable the Netskope Client to automatically determine whether it is on-premises or off-premises, you can use the following options in the Netskope UI:
Enable Dynamic Steering:
This option is available in theSteering Configurationsection of the UI.

By enabling dynamic steering, the Netskope Client can intelligently determine the appropriate data plane (on-premises or cloud) based on the user??s location and network conditions.
It ensures that traffic is directed to the optimal data plane for improved performance and security.
[Reference: Netskope Documentation on Dynamic Steering, On Premises Detection:, This option is available under theClient Configurationsection of the UI., By configuring on-premises detection, the Netskope Client can identify whether it is connected to the local network (on-premises) or accessing resources from outside (off-premises)., It helps in applying relevant policies and steering traffic accordingly., Reference: Netskope Documentation on Client Configuration,]

NEW QUESTION 53
You are asked to ensure that a Web application your company uses is both reachable and decrypted by Netskope. This application is served using HTTPS on port 6443. Netskope is configured with a default Cloud Firewall configuration and the steering configuration is set for All Traffic.
Which statement is correct in this scenario?

A. Create a Firewall App in Netskope along with the corresponding Real-time Protection policy to allow the traffic.
B. Nothing is required since Netskope is steering all traffic.
C. Enable "Steer non-standard ports" in the steering configuration and add the domain and port as a new non-standard port
D. Enable "Steer non-standard ports" in the steering configuration and create a corresponding Real-time Protection policy to allow the traffic

Answer: C

NEW QUESTION 56
You are architecting a Netskope steering configuration for devices that are not owned by the organization The users could be either on-premises or off-premises and the architecture requires that traffic destined to the company's instance of Microsoft 365 be steered to Netskope for inspection.
How would you achieve this scenario from a steering perspective?

A. Use IPsec and GRE tunnels.
B. Use reverse proxy.
C. Use explicit proxy and the Netskope Client
D. Use DPoP and Secure Forwarder

Answer: B

NEW QUESTION 57
You are asked to create a Real-time Protection policy to inspect outbound e-mail for DLP violations. You must prevent sensitive e-mail from leaving the corporate mail relay.
In this scenario, which Real-time Protection policy action must be specified?

A. Alert
B. Block
C. Forward to Proxy
D. Add SMTP Header

Answer: D

NEW QUESTION 59
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSK300 Practice Exam Features:

* NSK300 Questions and Answers Updated Frequently

* NSK300 Practice Questions Verified by Expert Senior Certified Staff

* NSK300 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSK300 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year