# Netskope

## Exam Questions NSK300

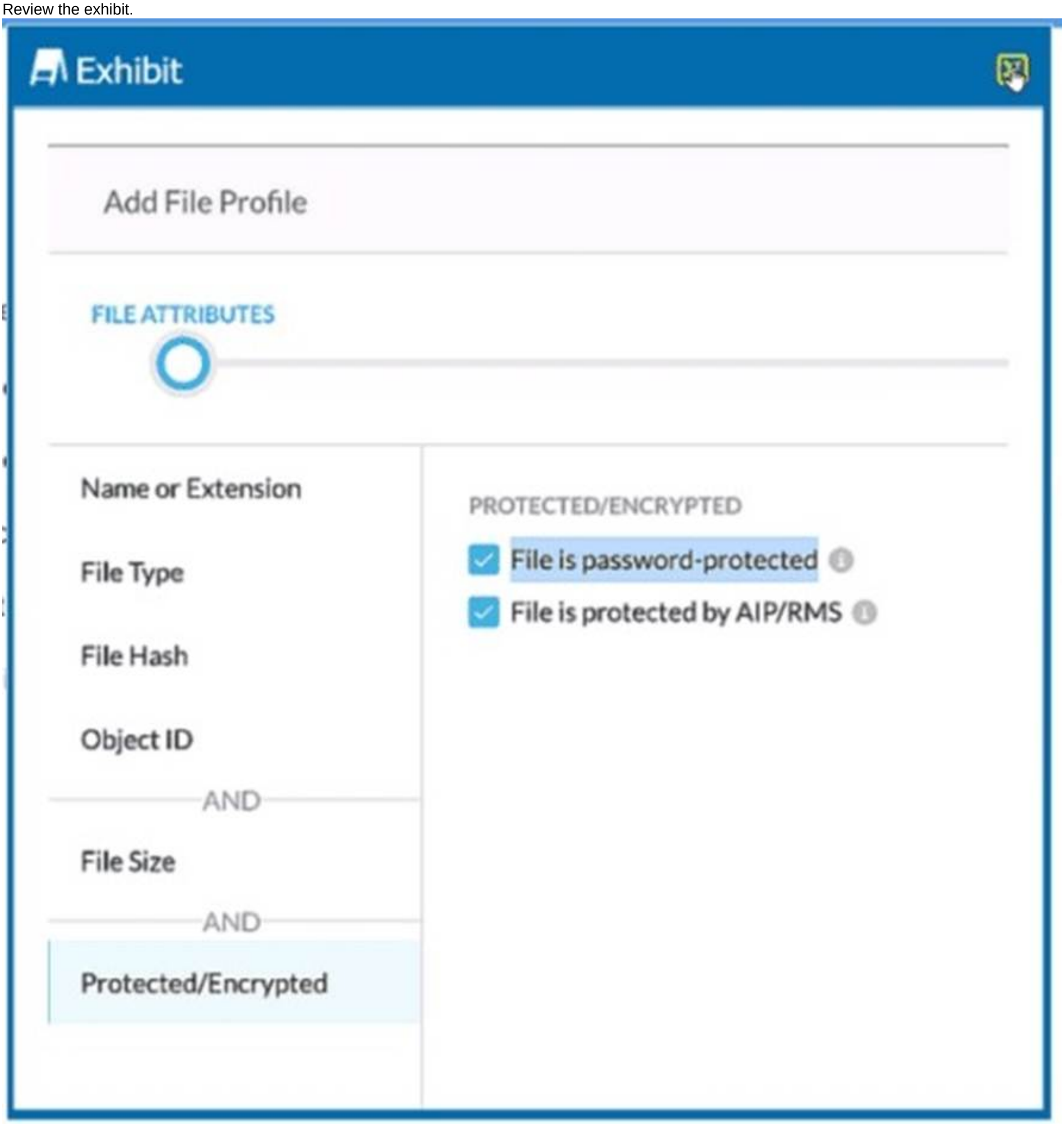
Netskope Certified Cloud Security Architect Exam

**NEW QUESTION 1**
Users at your company's branch office in San Francisco report that their clients are connecting, but websites and SaaS applications are slow When troubleshooting, you notice that the users are connected to a Netskope data plane in New York where your company's headquarters is located.
What is a valid reason for this behavior?

A. The Netskope Client's on-premises detection check failed.
B. The Netskope Client's default DNS over HTTPS call is failing.
C. The closest Netskope data plane to San Francisco is unavailable.
D. The Netskope Client's DNS call to Secure Forwarder is failing

**Answer:** C

**NEW QUESTION 2**
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 3**
A company wants to capture and maintain sensitive Pll data in a relational database to help their customers. There are many employees and contractors that need access to sensitive customer data to perform their duties The company wants to prevent the exfiltration of sensitive customer data by their employees and contractors.
In this scenario. what would satisfy this requirement?

A. fingerprinting
B. exact data match
C. regular expression
D. machine learning

**Answer:** B

**NEW QUESTION 4**
Your company has a large number of medical forms that are allowed to exit the company when they are blank. If the forms contain sensitive data, the forms must not leave any company data centers, managed devices, or approved cloud environments. You want to create DLP rules for these forms.
Which first step should you take to protect these forms?

A. Use Netskope Secure Forwarder to create EDM hashes of all forms.
B. Use Netskope Secure Forwarder to create an MIP tag for all forms.
C. Use Netskope Secure Forwarder to create fingerprints of all forms.
D. Use Netskope Secure Forwarder to create an ML Model of all forms

**Answer:** C

**Explanation:**
The first step to protect the medical forms containing sensitive data is to create fingerprints of all forms © using Netskope Secure Forwarder. Fingerprints are unique identifiers that can be used to detect when a form contains sensitive data. By creating fingerprints, you can set up DLP (Data Loss Prevention) rules that will allow blank forms to exit the company but will prevent forms with sensitive data from leaving the protected environments. This method ensures that only forms without sensitive information are allowed to be shared externally.
[: The process of creating fingerprints for DLP rules is a common practice in data security to protect sensitive information. It is part of the DLP capabilities provided by Netskope, as outlined in their documentation on data protection and loss prevention1., ]

**NEW QUESTION 5**
You deployed IPsec tunnels to steer on-premises traffic to Netskope. You are now experiencing problems with an application that had previously been working. In an attempt to solve the issue, you create a Steering Exception in the Netskope tenant tor that application: however, the problems are still occurring
Which statement is correct in this scenario?

A. You must create a private application to steer Web application traffic to Netskope over an IPsec tunnel.
B. Exceptions only work with IP address destinations
C. Steering bypasses for IPsec tunnels must be applied at your edge network device.
D. You must deploy a PAC file to ensure the traffic is bypassed pre-tunnel

**Answer:** C

**Explanation:**
In the scenario where you have deployed IPsec tunnels to steer on-premises traffic to Netskope and are experiencing issues with an application, the correct statement is C: Steering bypasses for IPsec tunnels must be applied at your edge network device . This means that to effectively bypass the steering for a specific application, the configuration must be done on the network device that is establishing the IPsec tunnel, such as a firewall or router. This device controls the traffic before it enters the tunnel, so applying the bypass there ensures that the application??s traffic does not get directed through the tunnel and can reach its destination directly.
[: The solution is based on standard practices for IPsec tunnel configuration and steering exceptions as described in Netskope??s documentation on traffic steering and IPsec configuration12., ]

**NEW QUESTION 6**
You want to verify that Google Drive is being tunneled to Netskope by looking in the nsdebuglog file. You are using Chrome and the Netskope Client to steer traffic. In this scenario, what would you expect to see in the log file?
A)

```
2022/01/0 01:00:00.001010 stAgentNE p752b t28da7 info tunnel.cpp:712 nsTunnel TLS [sessId 502] Tunneling flow from addr:
1.0.0.1:64000, process: google drive to host: play.googleapis.com, addr: 172.217.4.46:443 to nsProxy
```

B)

```
2022/01/0 01:00:00.001010 stAgentNE p752b t28da7 info tunnel.cpp:712 nsTunnel TLS [sessId 502] Tunneling flow from addr:
1.0.0.1:63720, process: google chrome helper to host: drive.google.com, addr: 172.217.4.46:443 to nsProxy
```

C)

```
2022/01/0 01:00:00.001010 stAgentNE p752b t28da7 info bypassAppMgr.cpp:538 BypassAppMgr Bypassing UDP flow to process
google chrome helper ip: 172.217.4.46, Port: 443, host: drive.google.com
```

D)

```
2022/01/0 01:00:00.001010 stAgentNE p752b t28da7 info AppProxyProvider.mm:303 main New UDP flow: Process = google chrome
helper, IP:Port = [8.8.8.8:53]
```

A. Option A
B. Option B
C. Option C

D. Option D

**Answer:** B

**NEW QUESTION 7**
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 8**
You have enabled CASB traffic steering using the Netskope Client, but have not yet enabled a Real-time Protection policy. What is the default behavior of the traffic in this scenario?

A. Traffic will be blocked and logged.
B. Traffic will be allowed and logged.
C. Traffic will be blocked, but not logged.
D. Traffic will be allowed, but not logged.

**Answer:** B

**NEW QUESTION 9**
You successfully configured Advanced Analytics to identify policy violation trends Upon further investigation, you notice that the activity is NULL. Why is this happening in this scenario?

A. The SSPM policy was not configured during setup.
B. The REST API v1 token has expired.
C. A policy violation was identified using API Protection.
D. A user accessed a static Web page.

**Answer:** D

**Explanation:**
The reason for the activity being NULL in this scenario is likely because a user accessed a static Web page . In Netskope??s Advanced Analytics, when the activity is reported as NULL, it often indicates that there was no dynamic interaction or transaction to record, which is typical when a static web page is accessed 1 . Static web pages do not generate the kind of events or activities that are tracked by policies, hence they appear as NULL in the activity field.
[: This explanation is supported by the Netskope Knowledge Portal, which mentions that applications fields with null values indicate incidents generated from web traffic, such as accessing static web pages2. Further information on interpreting NULL values in Advanced Analytics reports can be found in the Netskope documentation1., , In Advanced Analytics, the Activity field is populated only when Netskope can identify a specific app activity (e.g., upload, download, edit, share, delete)., When the traffic is simply generic web browsing — especially static web pages (HTML, images, CSS, JS) — Netskope cannot map the request to an application-level activity, so the Activity field becomes:, ?? NULL, This is expected behavior for traffic that is:, Not associated with a sanctioned/unsanctioned cloud app, Does not contain a user action like upload/download, Classified only as generic web content (static website), Why other options are incorrect, A. The SSPM policy was not configured during setupSSPM configuration does not impact the Activity field in Analytics for inline events., B. The REST API v1 token has expiredAPI token expiration would impact API logs collection, not inline event Activity values., C. A policy violation was identified using API ProtectionAPI Protection events always include an activity type (e.g., ??Download via API??), so they wouldn??t show NULL., , ]

**NEW QUESTION 10**
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 10**
Your CISO asks that you to provide a report with a visual representation of the top 10 applications (by number of objects) and their risk score. As the administrator, you decide to use a Sankey visualization in Advanced Analytics to represent the data in an efficient manner.
In this scenario, which two field types are required to produce a Sankey Tile in your report? (Choose two.)

A. Dimension
B. Measure
C. Pivot Ranks
D. Period of Type

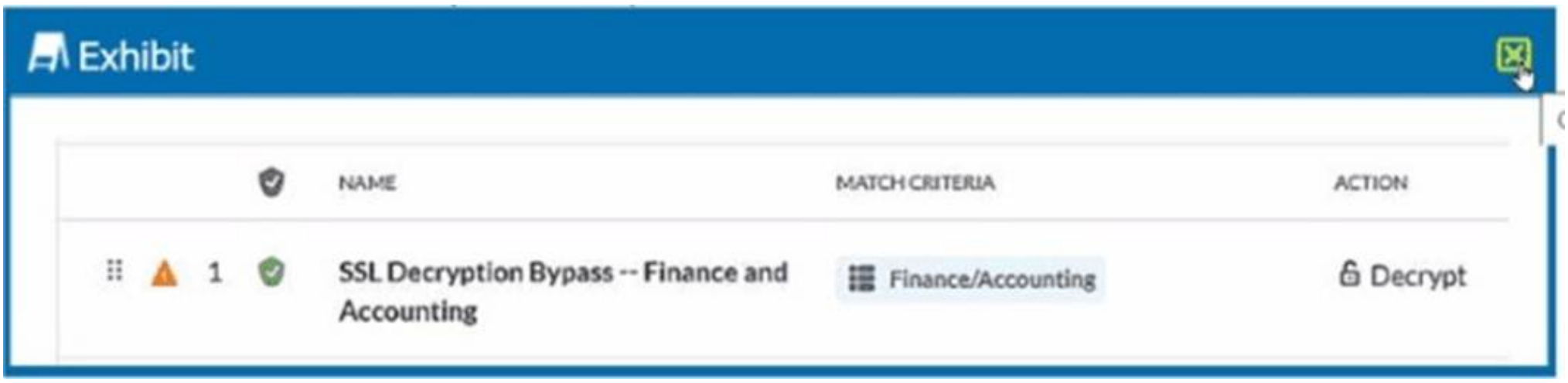
**Answer:** AB

**NEW QUESTION 14**
You do not want a scheduled Advanced Analytics dashboard to be automatically updated when Netskope makes improvements to that dashboard. In this scenario, what would you do to retain the original dashboard?

A. Create a new dashboard from scratch that mimics the Netskope dashboard you want to use.
B. Copy the dashboard into your Group or Personal folders and schedule from these folders.
C. Ask Netskope Support to provide the dashboard and import into your Personal folder.
D. Download the dashboard you want and Import from File into your Group or Personal folder.

**Answer:** B

**NEW QUESTION 19**
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 22**
Your client is an NG-SWG customer. They are going to use the Explicit Proxy over Tunnel (EPoT) steering method. They have a specific list of domains that they do not want to steer to the Netskope Cloud.
What would accomplish this task"

A. Define exception domains in the PAC file.
B. Define exceptions in the Netskope steering configuration
C. Create a real-time policy with a bypass action.
D. Use an SSL decryption policy.

**Answer:** A

**NEW QUESTION 27**
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 28**
You are consuming Audit Reports as part of a Salesforce API integration. Someone has made a change to a Salesforce account record field that should not have been made and you are asked to venfy the previous value of the structured data field. You have the approximate date and time of the change, user information, and the new field value.
How would you accomplish this task?

A. Create a classic report and apply a query that filters on the changed field value.
B. Use the Application Events Data Collection within Advanced Analytics and filter on the changed field value.
C. Query Skope IT Page Events and look for the specific Page URL that was called under the Application section.

D. Query Skope IT for an Access Method of API Connector and search Application Event Details for the Old Value field using the User details and Edit Activity.

**Answer:** D

**Explanation:**
To verify the previous value of a structured data field in Salesforce after an unauthorized change, you would use Skope IT with an Access Method of API Connector. This method allows you to search the Application Event Details for the ??Old Value?? field. By filtering with the user details and the edit activity, you can pinpoint the exact change and retrieve the original value of the field.
[: The approach is consistent with the Netskope Cloud Security Architect??s guidelines for using API Data Protection with Salesforce.The documentation provides a detailed procedure for configuring Salesforce for API Data Protection, which includes the use of Netskope Audit Reports and the ability to track changes through the ??Old Value?? field, ]

**NEW QUESTION 32**
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 37**
Your company just had a new Netskope tenant provisioned and you are asked to create a secure tenant configuration. In this scenario, which two default settings should you change? {Choose two.)

A. Change Safe Search to Disabled
B. Change Untrusted Root Certificate to Block.
C. Change the No SNI setting to Block.
D. Change "Disallow concurrent logins by an Admin" to Enabled.

**Answer:** BD

**NEW QUESTION 41**
Your company purchased Netskope's Next Gen Secure Web Gateway You are working with your network administrator to create GRE tunnels to send traffic to Netskope Your network administrator has set up the tunnel, keepalives. and a policy-based route on your corporate router to send all HTTP and HTTPS traffic to Netskope. You want to validate that the tunnel is configured correctly and that traffic is flowing.
In this scenario, which two statements are correct? (Choose two.)

A. You can use your local router or network device to verify that keepalives are being received and traffic is flowing to Netskope.
B. You must use your own monitoring tools to verify that the tunnel is up.
C. You can verify that the tunnel is up and receiving traffic in the Netskope Ul under Settings > Security Cloud Platform > GRE.
D. You can verify that the tunnel is up in the Netskope Trust portal at https://trust netskope.com/.

**Answer:** AC

**NEW QUESTION 46**
.....

# 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