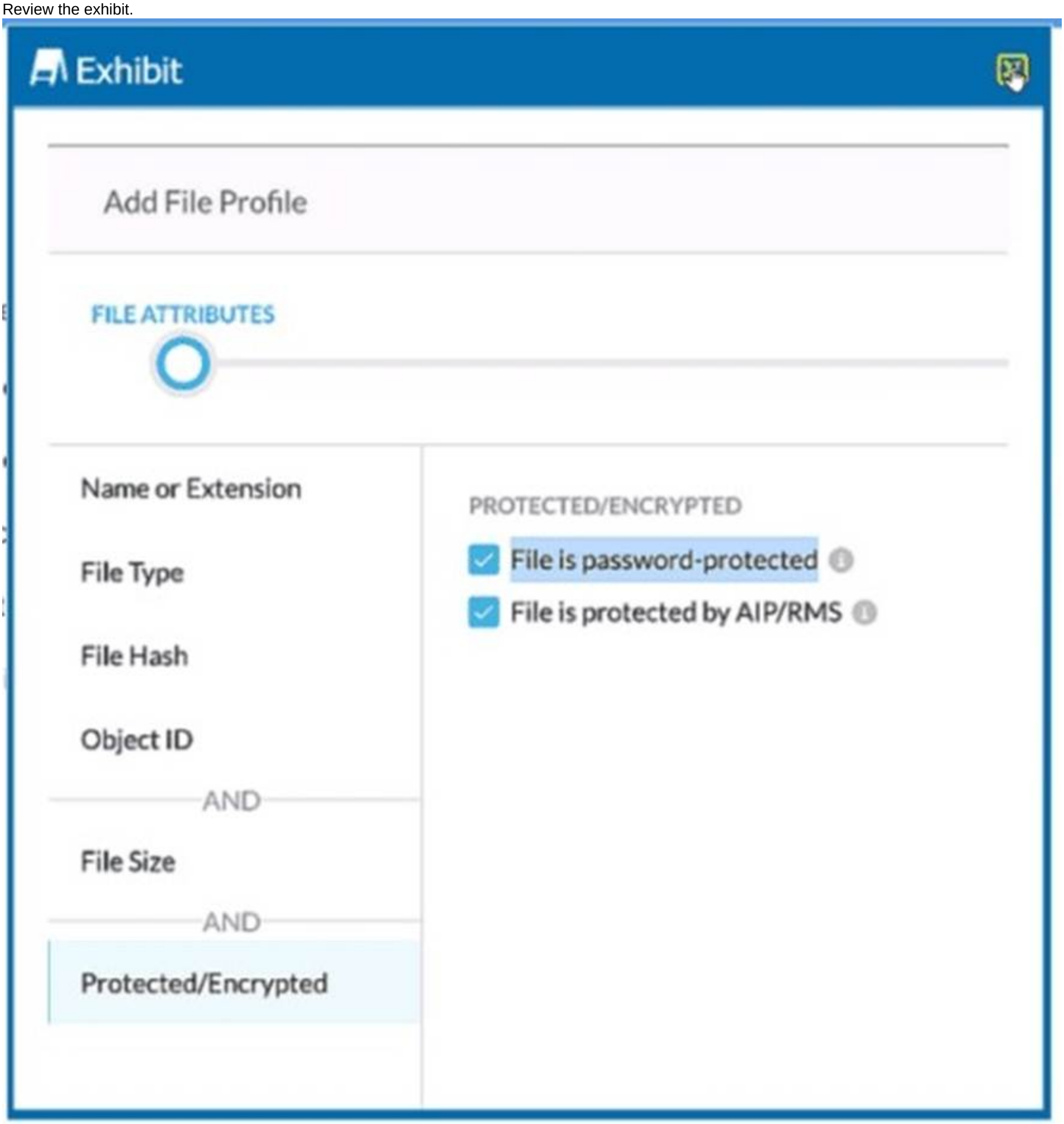
# Netskope

## Exam Questions NSK300

Netskope Certified Cloud Security Architect Exam

**NEW QUESTION 1**
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 2**
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

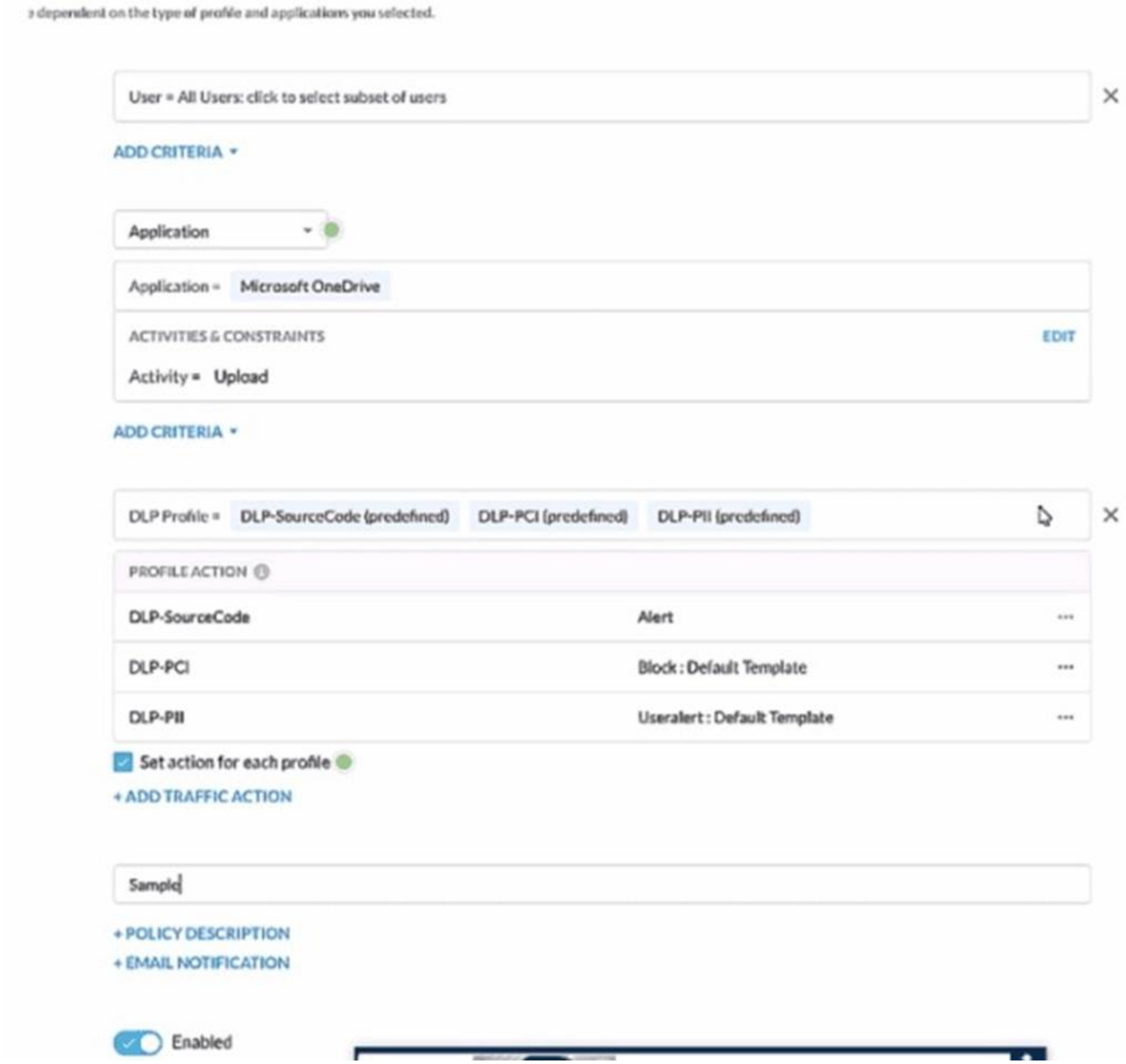
**NEW QUESTION 3**
Your company has a large number of medical forms that are allowed to exit the company when they are blank. If the forms contain sensitive data, the forms must not leave any company data centers, managed devices, or approved cloud environments. You want to create DLP rules for these 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 4**
Review the exhibit.




A user has attempted to upload a file to Microsoft OneDrive that contains source code with Pll and PCI data.
Referring to the exhibit, which statement Is correct?

A. The user will be blocked and a single Incident will be generated referencing the DLP- PCI profile.
B. The user will be blocked and a single Incident will be generated referencing all of the matching DLP profiles
C. The user will be blocked and a separate incident will be generated for each of the matching DLP profiles.
D. The user will be alerted and a single incident will be generated referencing the DLP-PII profile.

**Answer:** C

**NEW QUESTION 5**
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 6**
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 7**
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 8**
You want to see all instances of malware that were detected by the Netskope Cloud Sandbox.
Which process would you use to achieve this task in the Netskope tenant UI?

A. Go to Incidents > Malicious Sites, and perform the detection_engine eq ??Advanced Detection?? query.
B. Go to Incidents > Malware and perform the detection_engine eq ??Netskope Cloud Sandbox?? query.
C. Go to Skope IT > Alerts, switch to Query Mode and perform the detection_engine eq ??Netskope Cloud Sandbox?? query.
D. Go to Skope IT > Page Events, switch to Query Mode and perform the detection_engine eq ??Netskope Cloud Sandbox?? query.

**Answer:** B

**NEW QUESTION 9**
You configured a pair of IPsec funnels from the enterprise edge firewall to a Netskope data plane. These tunnels have been implemented to steer traffic for a set of defined HTTPS SaaS applications accessed from end-user devices that do not support the Netskope Client installation. You discover that all applications steered through this tunnel are non- functional.
According to Netskope. how would you solve this problem?

A. Restart the tunnel to stop the tunnel from flapping.
B. Downgrade from IKE v2 to IKE v1.
C. Install the Netskope root and intermediate certificates on the end-user devices.
D. Disable Perfect Forward Secrecy on the tunnel configuration.

**Answer:** C

**NEW QUESTION 10**
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 are implementing Netskope Cloud Exchange in your company lo include functionality provided by third-party partners. What would be a reason for using Netskope Cloud Risk Exchange in this scenario?

A. to ingest events and alerts from a Netskope tenant
B. to feed SOC with detection and response services
C. to map multiple scores to a normalized range
D. to automate service tickets from alerts of interest

**Answer:** D

**Explanation:**
The reason for using Netskope Cloud Risk Exchange in this scenario is to automate service tickets from alerts of interest . Netskope Cloud Risk Exchange (CRE) is designed to ingest user, device, and application risk scores, creating a dashboard view of contributors to your company??s overall risk score and trend. One of the key functionalities of CRE is to trigger risk-reducing actions through business rules that are tuned to a weighted score. Automating service tickets from alerts of interest is a part of this functionality, as it allows for the automatic creation of tickets in response to specific alerts, streamlining the process of addressing potential security issues 1 2 .
[: The use cases for Netskope Cloud Risk Exchange, including the automation of service tickets, can be found in the official Netskope resources1. Further information on how to integrate and utilize Netskope Cloud Risk Exchange for automating service tickets can be found in the Netskope Knowledge Portal3., ]

**NEW QUESTION 14**
You are deploying the Netskope Client in a multi-user VDI environment and need to determine the command to deploy the MSI.
Which three parameters are required in this scenario? (Choose three.)

A. mode=peruserconfig
B. host=
C. installmode=IDP
D. token=
E. autoupdate=on

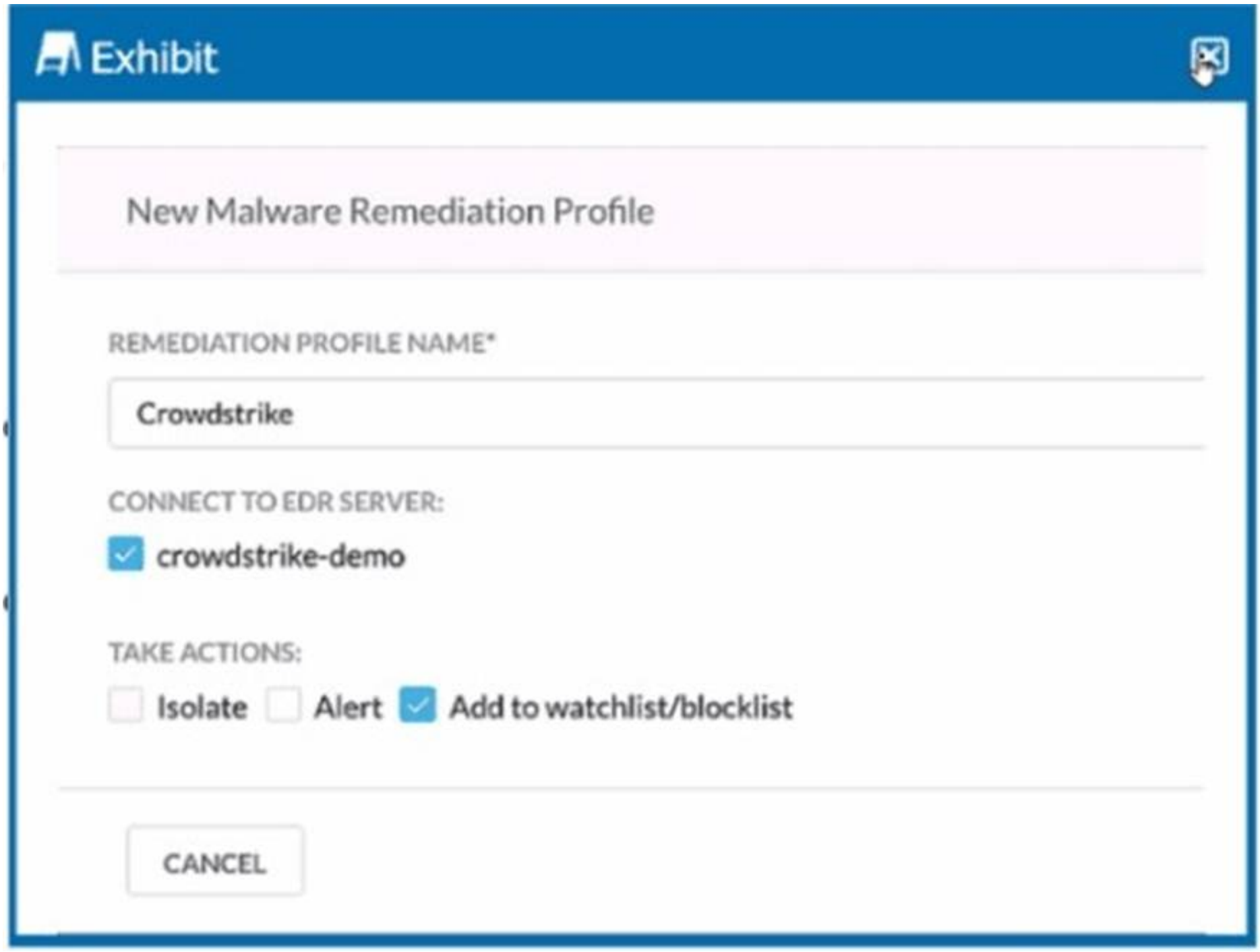
**Answer:** ABD

**NEW QUESTION 19**
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 24**
Review the exhibit.




You are asked to integrate Netskope with Crowdstrike EDR. You added the Remediation profile shown in the exhibit.
Which action will this remediation profile take?

A. The endpoint will be isolated.
B. The malware hash will be added as an IOC in Crowdstrike.
C. The malware will be quarantined.
D. The malware hash will be added as an IOC in Netskope.

**Answer:** B

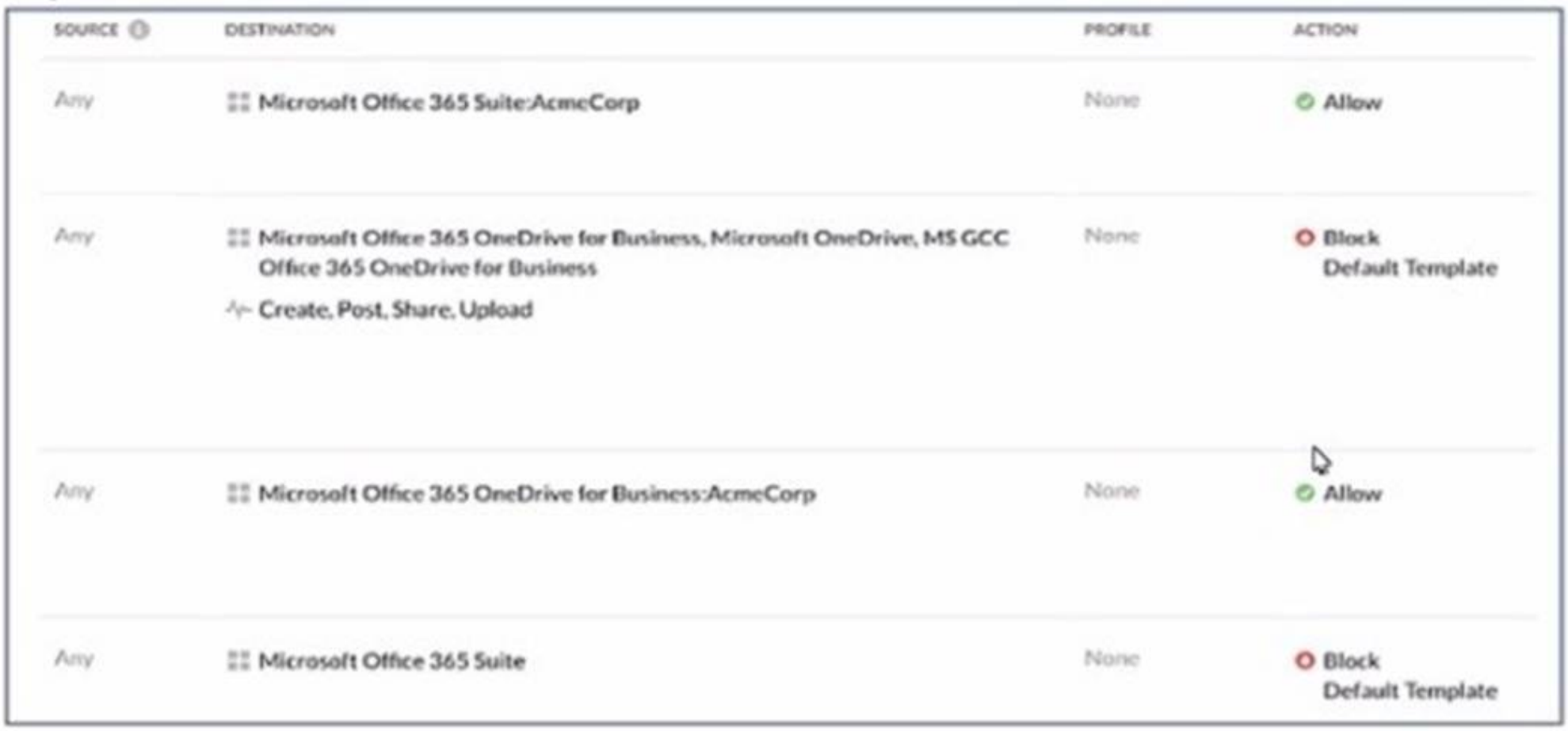
**NEW QUESTION 29**
You do not want a scheduled Advanced Analytics dashboard to be automatically updated when Netskope makes improvements to that dashboard. In this scenario, what would you do to retain the original dashboard?

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 34**
Review the exhibit.

1




2


3


4


AcmeCorp has recently begun using Microsoft 365. The organization is concerned that employees will start using third-party non-AcmeCorp OneDrive instances to store company data. The CISO asks you to use Netskope to create a policy that ensures that no data is being uploaded to non-AcmeCorp instances of OneDrive. Referring to the exhibit, which two policies would accomplish this posture? (Choose two.)

A. 4
B. 3
C. 2
D. 1

**Answer:** BC

**Explanation:**
To ensure that no data is uploaded to non-AcmeCorp instances of OneDrive, the policies that would accomplish this are:
Policy B : This policy allows traffic only for AcmeCorp??s OneDrive and blocks all other Microsoft 365 Suite traffic. It ensures that data is not uploaded to non-AcmeCorp OneDrive instances by restricting access to only the corporate instance of OneDrive.
Policy C : This policy allows traffic for AcmeCorp??s Microsoft 365 Suite but blocks all other OneDrive for Business traffic. It achieves the same outcome by permitting corporate suite usage while preventing uploads to any OneDrive for Business instances that are not part of AcmeCorp.
These policies are designed to provide granular control over the data flow, ensuring that company data remains within the corporate environment and is not transferred to external or personal storage solutions.
[: The policies are based on Netskope??s capabilities for real-time protection and data security, which allow organizations to enforce granular access and control policies.The information aligns with the best practices for setting up such policies as described in Netskope??s documentation and resources, , ]

**NEW QUESTION 38**
Your customer is currently using Directory Importer with Active Directory (AD) to provision users to Nelskope. They have recently acquired three new companies (A. B. and C) and want to onboard users from the companies onto the NetsKope platform. Information about the companies is shown below.
- Company A uses Active Directory.
-- Company B uses Azure AD.
-- Company C uses Okta Universal Directory. Which statement is correct in this scenario?

A. Users from Company B and Company C cannot be provisioned because the customer is already using AD Importer.
B. Either Company B or Company C users cannot be provisioned because integration with only one SCIM solution is allowed.
C. Users from Companies
D. B, and C can be provisioned to Netskope by deploying additional AD Importers and integrating more than one SCIM solution.
E. Company A users cannot be provisioned to Netskope because the customer is already using AD Importer to import users from another Active Directory environment.

**Answer:** C

**NEW QUESTION 43**
Users in your network are attempting to reach a website that has a self-signed certificate using a GRE tunnel to Netskope. They are currently being blocked by Netskope with an SSL error. How would you allow this traffic?

A. Configure a Do Not Decrypt SSL Decryption rule to allow traffic to pass.
B. Configure a Real-time Protection policy with the action set to Allow.
C. Set the No SNI setting in Netskope to Bypass.
D. Ensure that the users add the self-signed certificate to their local certificate store.

**Answer:** A

**Explanation:**
To allow traffic from a website with a self-signed certificate that is being blocked by Netskope with an SSL error, the correct action is to configure a Do Not Decrypt SSL Decryption rule . This rule will allow the traffic to pass without being decrypted, thus bypassing the SSL error caused by the self-signed certificate. This is a common practice for handling traffic from trusted internal applications or specific external sites that use self-signed certificates 1 .
[: The Netskope Community Forum discusses the application of exceptions for sites with self-signed certificates and the use of SSL decryption policies to bypass the blocking1. Additionally, the Netskope Knowledge Portal provides information on managing error settings and configuring SSL decryption rules2., ]

**NEW QUESTION 47**
You are already using Netskope CSPM to monitor your AWS accounts for compliance. Now you need to allow access from your company-managed devices running the Netskope Client to only Amazon S3 buckets owned by your organization. You must ensure that any current buckets and those created in the future will be allowed
Which configuration satisfies these requirements?

A. Steering: Cloud Apps Only, All Traffic Policy type: Real-time Protection Constraint: Storag
B. Bucket Does Not Match -ALLAccounts Action: Block
C. Steering: Cloud Apps Only Policy type: Real-time ProtectionConstraint: Storag
D. Bucket Does Not Match *@myorganization.com Action: Block
E. Steering: Cloud Apps Onl
F. All Traffic Policy type: Real-time Protection Constraint: Storag
G. Bucket Does Match -ALLAccounts Action: Allow
H. Steering: All Web Traffic Policy type: API Data ProtectionConstraint: Storage, Bucket Does Match *@myorganization.com Action: Allow

**Answer:** A

**NEW QUESTION 50**
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 53**
You have users connecting to Netskope from around the world You need a way for your NOC to quickly view the status of the tunnels and easily visualize where the tunnels are located Which Netskope monitoring tool would you use in this scenario?

A. Network Steering in Digital Experience Management
B. Network Events in Skope IT
C. Web Usage Summary in Advanced Analytics
D. Alerts in Skope IT

**Answer:** A

**Explanation:**
Network Steering in Digital Experience Management is the appropriate Netskope monitoring tool for this scenario. It allows the Network Operations Center (NOC) to quickly view the status of the tunnels and provides an easy way to visualize the locations of the tunnels. This tool is designed to give a clear overview of network health and performance, which is essential for managing global connectivity and ensuring the reliability of the service.
[: The use of Network Steering in Digital Experience Management for monitoring tunnel status and location visualization is supported by Netskope??s documentation on secure web gateway use cases and best practices for deployment and validation of IPSec/GRE tunnels, ]

**NEW QUESTION 57**
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 59**
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 61**
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 64**
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 UI 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 69**
You are the network architect for a company using Netskope Private Access. Multiple users are reporting that they are unable to access an application using Netskope Private Access that was working previously. You have verified that the Real-time Protection policy allows access to the application, private applications are steered for the users, and the application is reachable from internal machines. You must verify that the application is reachable through Netskope Publisher
In this scenario, which two tools in the Netskope UI would you use to accomplish this task? (Choose two.)

A. Reachability Via Publisher in the App Definitions page
B. Troubleshooter tool in the App Definitions page
C. Applications in Skope IT
D. Clear Private App Auth under Users in Skope IT

**Answer:** AB

**NEW QUESTION 71**
Given the following:

```
user eq 'user@company.com' and access_method eq 'Client' and activity eq 'Download' or activity eq 'Upload' and site eq 'Amazon S3'
```

Which result does this Skope IT query provide?

A. The query returns all events of user@company.com downloading or uploading to or from the site 'Amazon S3" using the Netskope Client.
B. The query returns all events of an IP address downloading or uploading to or from Amazon S3 using the Netskope Client.
C. The query returns all events of everyone except user@company.com downloading or uploading to or from the site "Amazon S3" using the Netskope Client.
D. The query returns all events of user@company.com downloading or uploading to or from the application "Amazon S3" using the Netskope Client.

**Answer:** A

**NEW QUESTION 74**
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 75**
.....

# 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