Netskope.NSK200.by.Pano.39q

Number: NSK200
Passing Score: 800
Time Limit: 120
File Version: 4.0

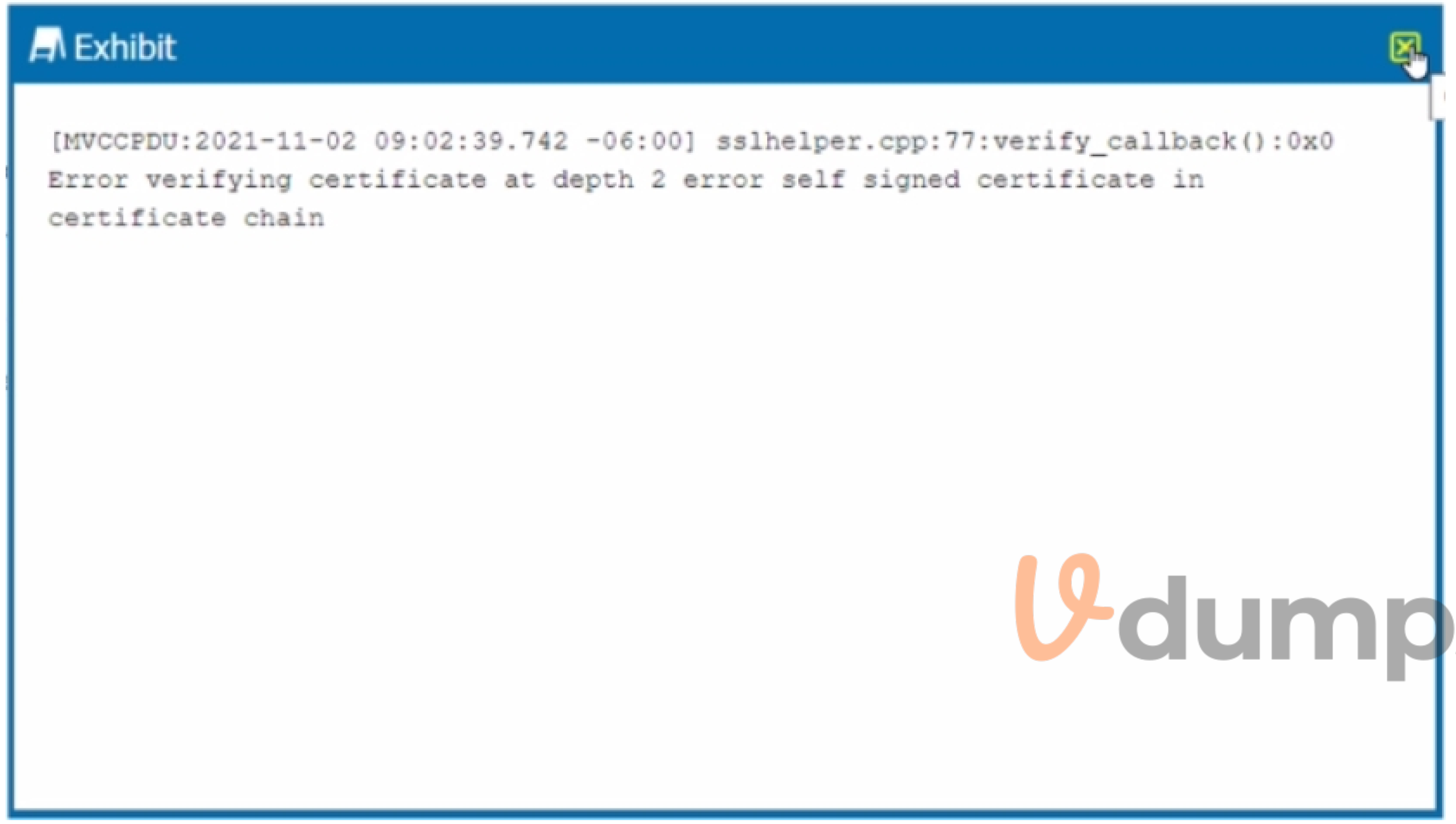
Exam Code: NSK200

Exam Name: Netskope Certified Cloud Security Integrator

Exam A

QUESTION 1

Review the exhibit.



```
[MVCCPDU:2021-11-02 09:02:39.742 -06:00] sslhelper.cpp:77:verify_callback():0x0
Error verifying certificate at depth 2 error self signed certificate in
certificate chain
```

While diagnosing an NPA connectivity issue, you notice an error message in the Netskope client logs.
Referring to the exhibit, what does this error represent?

A. The Netskope client has been load-balanced to a different data center.

B. The primary publisher is unavailable or cannot be reached.

C. There Is an EDNS or LDNS resolution error.

D. There Is an upstream device trying to intercept the NPA TLS connection.

Correct Answer: D
Section:
Explanation:
The error message in the exhibit represents that there is an upstream device trying to intercept the NPA TLS connection. The error message is ''ERROR SSL certificate verification failed: self signed certificate in certificate chain''. This means that the Netskope client is receiving a certificate that is not issued by Netskope, but by a device that is intercepting and decrypting the traffic between the client and the Netskope cloud.This can cause the client to fail to establish a secure connection to the NPA service and access the private applications4.To solve this problem, you need to either bypass or trust the upstream device that is performing SSL decryption, such as a firewall or proxy5. Therefore, option D is correct and the other options are incorrect.Reference:Troubleshooting Netskope Client - Netskope Knowledge Portal,Netskope Client Troubleshooting Guide - The Netskope Community

QUESTION 2

You have deployed Netskope Secure Web Gateway (SWG). Users are accessing new URLs that need to be allowed on a daily basis. As an SWG administrator, you are spending a lot of time updating Web policies. You want to automate this process without having to log into the Netskope tenant
Which solution would accomplish this task?

A. You can use Cloud Log Shipper.
B. You can minimize your work by sharing URLs with Netskope support.
C. You can use Cloud Risk Exchange.
D. You can use REST API to update the URL list.

Correct Answer: D
Section:
Explanation:
To automate the process of updating Web policies without having to log into the Netskope tenant, you can use REST API to update the URL list.REST API is a feature that allows you to use an auth token to make authorized calls to the Netskope API and access resources via URI paths1.You can use REST API to update a URL list with new values by providing the name of an existing URL list and a comma-separated list of URLs or IP addresses2. This can help you automate or script the management of your URL lists and keep them up-to-date. Therefore, option D is correct and the other options are incorrect.Reference:REST API v2 Overview - Netskope Knowledge Portal,Update a URL List - Netskope Knowledge Portal

QUESTION 3
A customer wants to use Netskope to prevent PCI data from leaving the corporate sanctioned OneDrive instance. In this scenario. which two solutions would assist in preventing data exfiltration? (Choose two.)

A. API Data Protection
B. Cloud Firewall (CFW)
C. SaaS Security Posture Management (SSPM)
D. Real-time Protection

Correct Answer: A, D
Section:
Explanation:
To prevent PCI data from leaving the corporate sanctioned OneDrive instance, the customer can use API Data Protection and Real-time Protection. API Data Protection is a feature that allows you to discover, classify, and protect data that is already resident in your cloud services, such as OneDrive. You can create a policy that matches the PCI data based on criteria such as users, content, activity, or DLP profiles.Then, you can choose an action to prevent the PCI data from being shared or exfiltrated, such as remove external collaborators, remove public links, or quarantine3. Real-time Protection is a feature that allows you to inspect and control data in transit between your users and cloud services, such as OneDrive. You can create a policy that matches the PCI data based on criteria such as users, devices, locations, categories, or DLP profiles.Then, you can choose an action to prevent the PCI data from being uploaded or downloaded, such as block, alert, encrypt, or watermark4. Therefore, options A and D are correct and the other options are incorrect.Reference:API Data Protection - Netskope Knowledge Portal,Real-time Protection - Netskope Knowledge Portal

QUESTION 4
Your customer is concerned about malware in their AWS S3 buckets. What two actions would help with this scenario? (Choose two.)

A. Create a real-time policy to block malware uploads to their AWS instances.
B. Enable Threat Protection (Malware Scan) for all of their AWS instances to Identify malware.
C. Create an API protection policy to quarantine malware in their AWS S3 buckets.
D. Create a threat profile to quarantine malware in their AWS S3 buckets.

Correct Answer: B, C
Section:
Explanation:
To help the customer with the scenario of malware in their AWS S3 buckets, two actions that would help are B. Enable Threat Protection (Malware Scan) for all of their AWS instances to identify malware and C. Create an API protection policy to quarantine malware in their AWS S3 buckets. Threat Protection (Malware Scan) is a feature that allows you to scan files in your cloud services, such as AWS S3, for malware using Netskope's advanced

threat protection engine.You can enable Threat Protection (Malware Scan) for all of your AWS instances in the Netskope tenant by going to Settings > Cloud Services > AWS > Threat Protection and selecting the Enable Malware Scan option1. This will help you identify malware in your AWS S3 buckets and generate alerts for further action. An API protection policy is a rule that specifies the actions and notifications that Netskope applies to the data that is already resident in your cloud services, such as AWS S3, based on various criteria.You can create an API protection policy to quarantine malware in your AWS S3 buckets by going to Policies > API Protection > New Policy and selecting the AWS service, the Malware Scan data identifier, and the Quarantine action in the policy page2. This will help you isolate malware in your AWS S3 buckets and prevent it from spreading or being accessed by unauthorized users. Therefore, options B and C are correct and the other options are incorrect.Reference:Threat Protection (Malware Scan) - Netskope Knowledge Portal,Add a Policy for API Protection - Netskope Knowledge Portal

QUESTION 5
What are three methods to deploy a Netskope client? (Choose three.)

A. Deploy Netskope client using SCCM.
B. Deploy Netskope client using REST API v2.
C. Deploy Netskope client using email invite.
D. Deploy Netskope client using REST API v1.
E. Deploy Netskope client using IdP.

Correct Answer: A, C, E
Section:
Explanation:
Three methods to deploy a Netskope client are A. Deploy Netskope client using SCCM, C. Deploy Netskope client using email invite, and E. Deploy Netskope client using IdP.These are some of the methods that Netskope supports for packaging and installing the Netskope client on the user's device1.SCCM is a Microsoft tool that allows you to push the Netskope client silently to the user's device without requiring user intervention or local admin privileges2. Email invite is a method that sends an email to the user with a unique link to download and install the Netskope client.This method is quick and easy, but requires the user to initiate the installation and have local admin privileges3. IdP is a method that uses an identity provider (such as Azure AD or Okta) to authenticate the user and enroll the Netskope client.This method requires the UPN of the logged in user to match the directory, or use SAML/SSO as an alternative4. Therefore, options A, C, and E are correct and the other options are incorrect.Reference:Deploy the Netskope Client - Netskope Knowledge Portal,Deploying with Microsoft Endpoint Configuration Manager / SCCM - Netskope Knowledge Portal,Deploying with Email Invite - Netskope Knowledge Portal,Deploying with IdP - Netskope Knowledge Portal

QUESTION 6
Your small company of 10 people wants to deploy the Netskope client to all company users without requiring users to be imported using Active Directory, LDAP, or an IdP.

A. Deploy the Netskope client using SCCM.
B. Deploy the Netskope client using JAMF.
C. Deploy the Netskope client using Microsoft GPO.
D. Deploy the Netskope client using an email invitation.

Correct Answer: D
Section:
Explanation:
Deploying the Netskope client using an email invitation allows smaller companies to onboard users easily without relying on integration with AD, LDAP, or an IdP. This method is efficient for smaller teams that need a quick deployment without complex setup.

QUESTION 7
While most Web and SaaS traffic is decrypted for inspection, you are asked to prevent a certain host on the network from SSL decryption for privacy purposes.

A. Create a steering exception for the host.
B. Create a Real-time Protection policy, select the host, and choose to block SSL decryption.
C. Create a Source Network Location for a Do Not Decrypt SSL policy.
D. Add the host to the certificate-pinned application list.

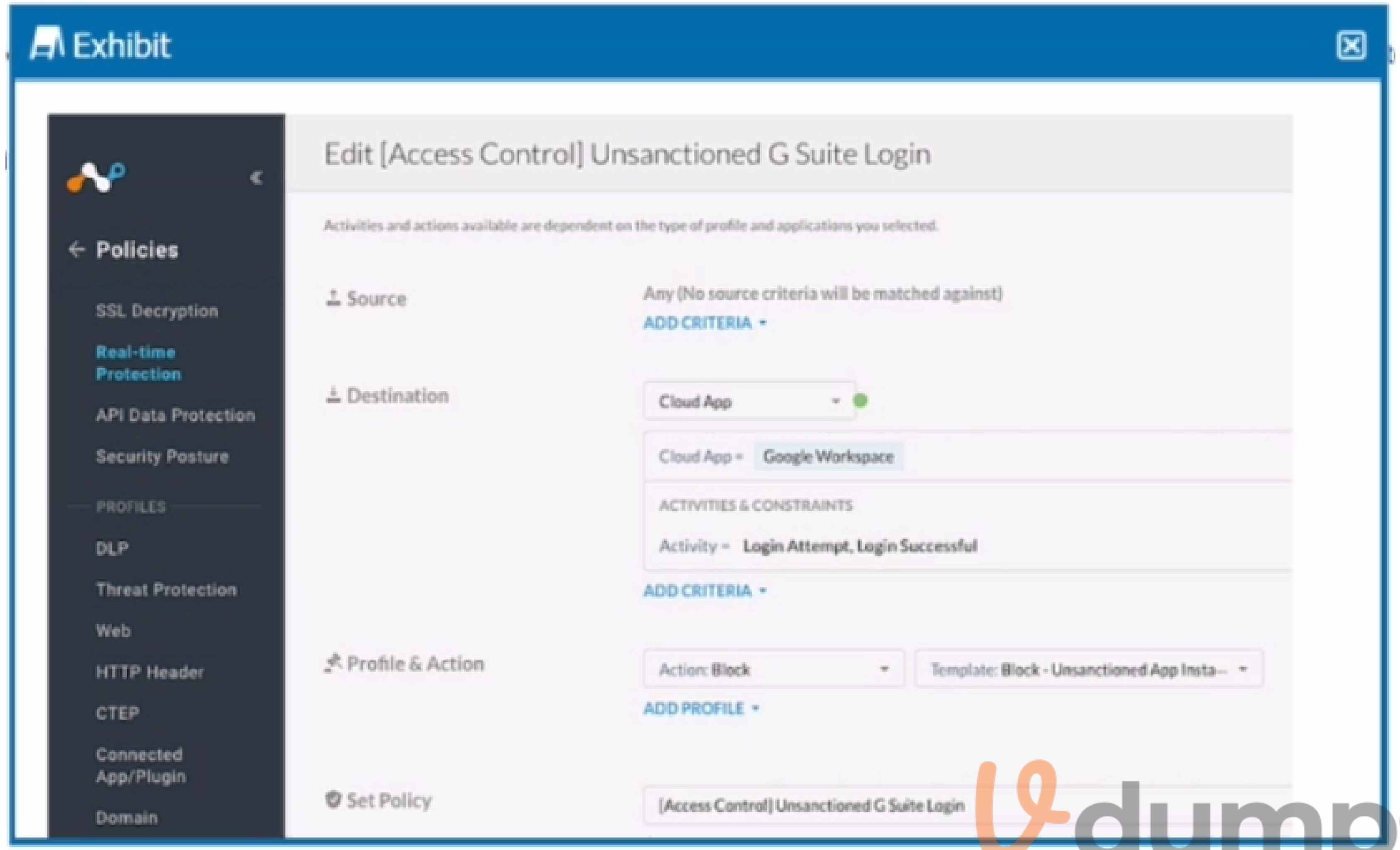
Correct Answer: A
Section:
Explanation:
Creating a steering exception for the host is the appropriate action to prevent SSL decryption on specific network traffic. Steering exceptions allow you to bypass decryption for designated hosts, which is useful for privacy-sensitive scenarios.

QUESTION 8
To which three event types does Netskope's REST API v2 provide access? (Choose three.)

A. application
B. alert
C. client
D. infrastructure
E. user

Correct Answer: A, B, D
Section:
Explanation:
Netskope's REST API v2 provides access to various event types via URI paths. The event types include application, alert, infrastructure, audit, incident, network, and page. These event types can be used to retrieve data from Netskope's cloud security platform. The event types client and user are not supported by the REST API v2.Reference:REST API v2 Overview,Cribl Netskope Events and Alerts Integration,REST API Events and Alerts Response Descriptions

QUESTION 9
Review the exhibit.



Edit [Access Control] Unsanctioned G Suite Login

Activities and actions available are dependent on the type of profile and applications you selected.

Source: Any (No source criteria will be matched against)

Destination: Cloud App

Cloud App = Google Workspace

ACTIVITIES & CONSTRAINTS

Activity = Login Attempt, Login Successful

Profile & Action: Action: Block | Template: Block - Unsanctioned App Insta...

Set Policy: [Access Control] Unsanctioned G Suite Login

Your company uses Google as the corporate collaboration suite; however, corporate policy restricts the use of personal Google services. The exhibit provides a partially completed policy to ensure that users cannot log into their personal account.
What should be added to achieve the desired outcome in this scenario?

A. Google Gmail app
B. User Constraint
C. DLP profile
D. Device classification

Correct Answer: B
Section:
Explanation:
In order to restrict users from logging into their personal Google accounts, the policy should include a user constraint. This will ensure that only users with corporate accounts can access the corporate collaboration suite. The user constraint can be added by selecting the ''User'' option in the ''Source'' field and then choosing the appropriate user group or identity provider. The other options are not relevant for this scenario.Reference: [Creating a Policy to Block Personal Google Services], [Policy Creation], [User Constraint]

QUESTION 10
You have deployed a development Web server on a public hosting service using self-signed SSL certificates. After some troubleshooting, you determined that when the Netskope client is enabled, you are unable to access the Web server over SSL. The default Netskope tenant steering configuration is in place.
In this scenario, which two settings are causing this behavior? (Choose two.)

A. SSL pinned certificates are blocked.
B. Untrusted root certificates are blocked.

C. Incomplete certificate trust chains are blocked.

D. Self-signed server certificates are blocked.

Correct Answer: B, D
Section:
Explanation:
The default Netskope tenant steering configuration blocks untrusted root certificates and self-signed server certificates. These settings are intended to prevent man-in-the-middle attacks and ensure the validity of the SSL connection. However, they also prevent the access to the development Web server that uses self-signed SSL certificates. To allow access to the Web server, the settings need to be changed or an exception needs to be added for the Web server domain.

QUESTION 11
Your customer currently only allows users to access the corporate instance of OneDrive using SSO with the Netskope client. The users are not permitted to take their laptops when vacationing, but sometimes they must have access to documents on OneDrive when there is an urgent request. The customer wants to allow employees to remotely access OneDrive from unmanaged devices while enforcing DLP controls to prohibit downloading sensitive files to unmanaged devices.
Which steering method would satisfy the requirements for this scenario?

A. Use a reverse proxy integrated with their SSO.

B. Use proxy chaining with their cloud service providers integrated with their SSO.

C. Use a forward proxy integrated with their SSO.

D. Use a secure forwarder integrated with an on-premises proxy.

Correct Answer: A
Section:
Explanation:
A reverse proxy integrated with their SSO would satisfy the requirements for this scenario. A reverse proxy intercepts requests from users to cloud apps and applies policies based on user identity, device posture, app, and data context. It can enforce DLP controls to prohibit downloading sensitive files to unmanaged devices. It can also integrate with the customer's SSO provider to authenticate users and allow access only to the corporate instance of OneDrive. The other steering methods are not suitable for this scenario because they either require the Netskope client or do not provide granular control over cloud app activities.

QUESTION 12
An engineering firm is using Netskope DLP to identify and block sensitive documents, including schematics and drawings. Lately, they have identified that when these documents are blocked, certain employees may be taking screenshots and uploading them. They want to block any screenshots from being uploaded.
Which feature would you use to satisfy this requirement?

A. exact data match (EDM)

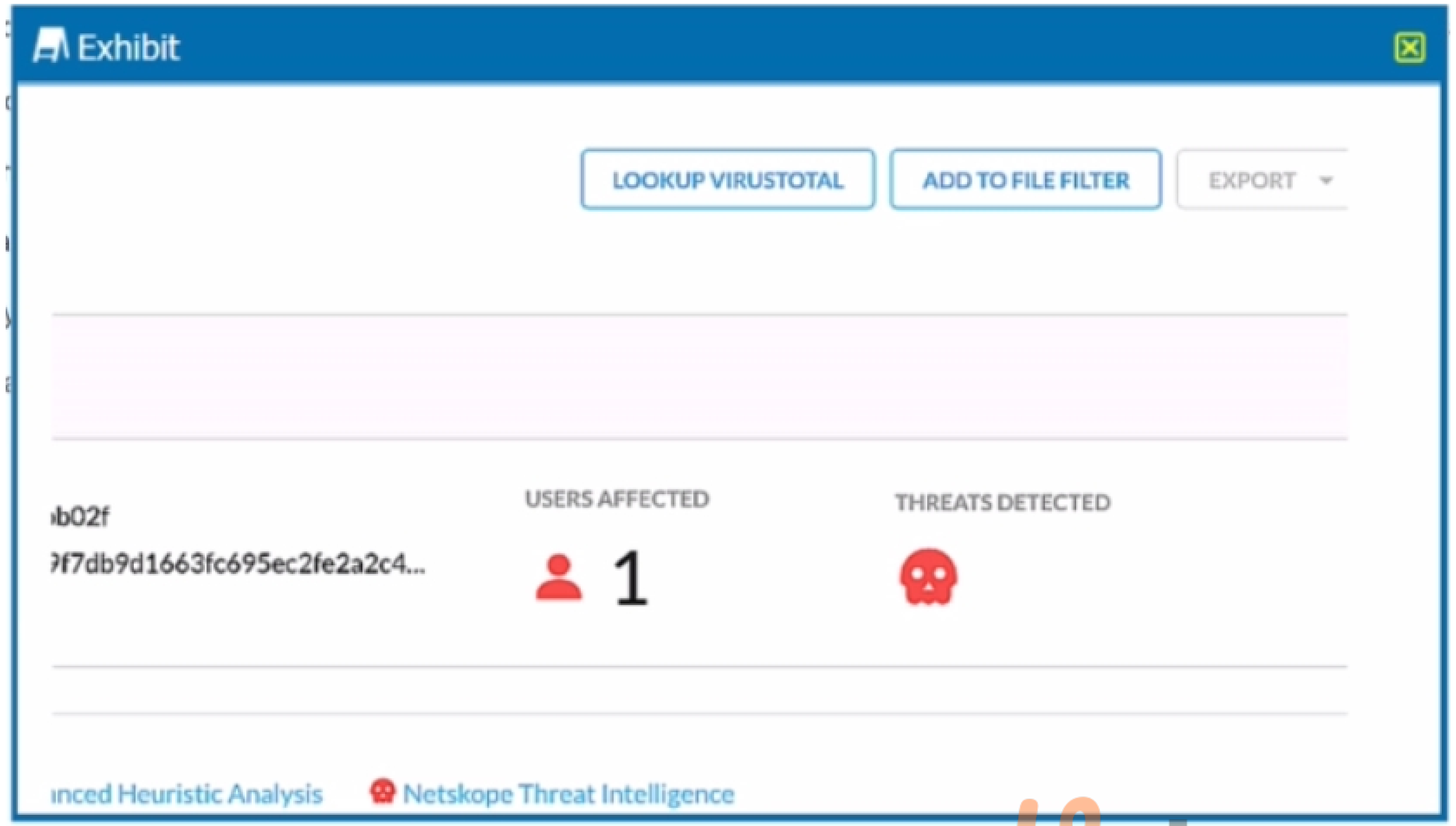
B. document fingerprinting

C. ML image classifier

D. optical character recognition (OCR)

Correct Answer: C
Section:
Explanation:
To block any screenshots from being uploaded, the engineering firm should use the ML image classifier feature of Netskope DLP. This feature uses machine learning to detect sensitive information within images, such as screenshots, whiteboards, passports, driver's licenses, etc. The firm can create a DLP policy that blocks any image upload that matches the screenshot classifier. This will prevent employees from circumventing the DLP controls by taking screenshots of sensitive documents.Reference:Improved DLP Image Classifiers,Netskope Data Loss Prevention,The Importance of a Machine Learning-Based Source Code Classifier

QUESTION 13
Review the exhibit.



You are at the Malware Incident page. A virus was detected by the Netskope Heuristics Engine. Your security team has confirmed that the virus was a test data file You want to allow the security team to use this file Referring to the exhibit, which two statements are correct? (Choose two.)

A. Click the 'Add To File Filter button to add the IOC to a file list.
B. Contact the CrowdStrike administrator to have the file marked as safe.
C. Click the ''Lookup VirusTotal' button to verify if this IOC is a false positive.
D. Create a malware detection profile and update the file hash list with the IOC.

Correct Answer: A, C
Section:
Explanation:
To allow the security team to use the test data file that was detected as a virus by the Netskope Heuristics Engine, the following two steps are correct:
Click the ''Add To File Filter'' button to add the IOC to a file list. This will exclude the file from future malware scans and prevent false positive alerts.The file list can be managed in the Settings > File Filter page1.
Click the ''Lookup VirusTotal'' button to verify if this IOC is a false positive. This will open a new tab with the VirusTotal report for the file hash. VirusTotal is a service that analyzes files and URLs for viruses, worms, trojans, and other kinds of malicious content.The report will show how many antivirus engines detected the file as malicious and provide additional information about the file2.
https://docs.netskope.com/en/netskope-help/admin-console/incidents/

QUESTION 14
Which object would be selected when creating a Malware Detection profile?

A. DLP profile
B. File profile
C. Domain profile
D. User profile

Correct Answer: B
Section:
Explanation:
A file profile is an object that contains a list of file hashes that can be used to create a malware detection profile. A file profile can be configured as an allowlist or a blocklist, depending on whether the files are known to be benign or malicious.A file profile can be created in the Settings > File Profile page1. A malware detection profile is a set of rules that define how Netskope handles malware incidents.A malware detection profile can be created in the Policies > Threat Protection > Malware Detection Profiles page2. To create a malware detection profile, one needs to select a file profile as an allowlist or a blocklist, along with the Netskope malware scan option. The other options are not objects that can be selected when creating a malware detection profile.

QUESTION 15
Your learn is asked to Investigate which of the Netskope DLP policies are creating the most incidents. In this scenario, which two statements are true? (Choose two.)

A. The Skope IT Applications tab will list the top five DLP policies.
B. You can see the top Ave DLP policies triggered using the Analyze feature
C. You can create a report using Reporting or Advanced Analytics.
D. The Skope IT Alerts tab will list the top five DLP policies.

Correct Answer: B, C
Section:
Explanation:
To investigate which of the Netskope DLP policies are creating the most incidents, the following two statements are true:
You can see the top five DLP policies triggered using the Analyze feature. The Analyze feature allows you to create custom dashboards and widgets to visualize and explore your data.You can use the DLP Policy widget to see the top five DLP policies that generated the most incidents in a given time period3.
You can create a report using Reporting or Advanced Analytics. The Reporting feature allows you to create scheduled or ad-hoc reports based on predefined templates or custom queries.You can use the DLP Incidents by Policy template to generate a report that shows the number of incidents per DLP policy4. The Advanced Analytics feature allows you to run SQL queries on your data and export the results as CSV or JSON files.You can use the DLP_INCIDENTS table to query the data by policy name and incident count5.
The other two statements are not true because:
The Skope IT Applications tab will not list the top five DLP policies. The Skope IT Applications tab shows the cloud app usage and risk summary for your organization.It does not show any information about DLP policies or incidents6.
The Skope IT Alerts tab will not list the top five DLP policies. The Skope IT Alerts tab shows the alerts generated by various policies and profiles, such as DLP, threat protection, IPS, etc.It does not show the number of incidents per policy, only the number of alerts per incident7.

QUESTION 16
You want to secure Microsoft Exchange and Gmail SMTP traffic for DLP using Netskope. Which statement is true about this scenario when using the Netskope client?

A. Netskope can inspect outbound SMTP traffic for Microsoft Exchange and Gmail.
B. Enable Cloud Firewall to Inspect Inbound SMTP traffic for Microsoft Exchange and Gmail.
C. Netskope can inspect inbound and outbound SMTP traffic for Microsoft Exchange and Gmail.
D. Enable REST API v2 to Inspect inbound SMTP traffic for Microsoft Exchange and Gmail.

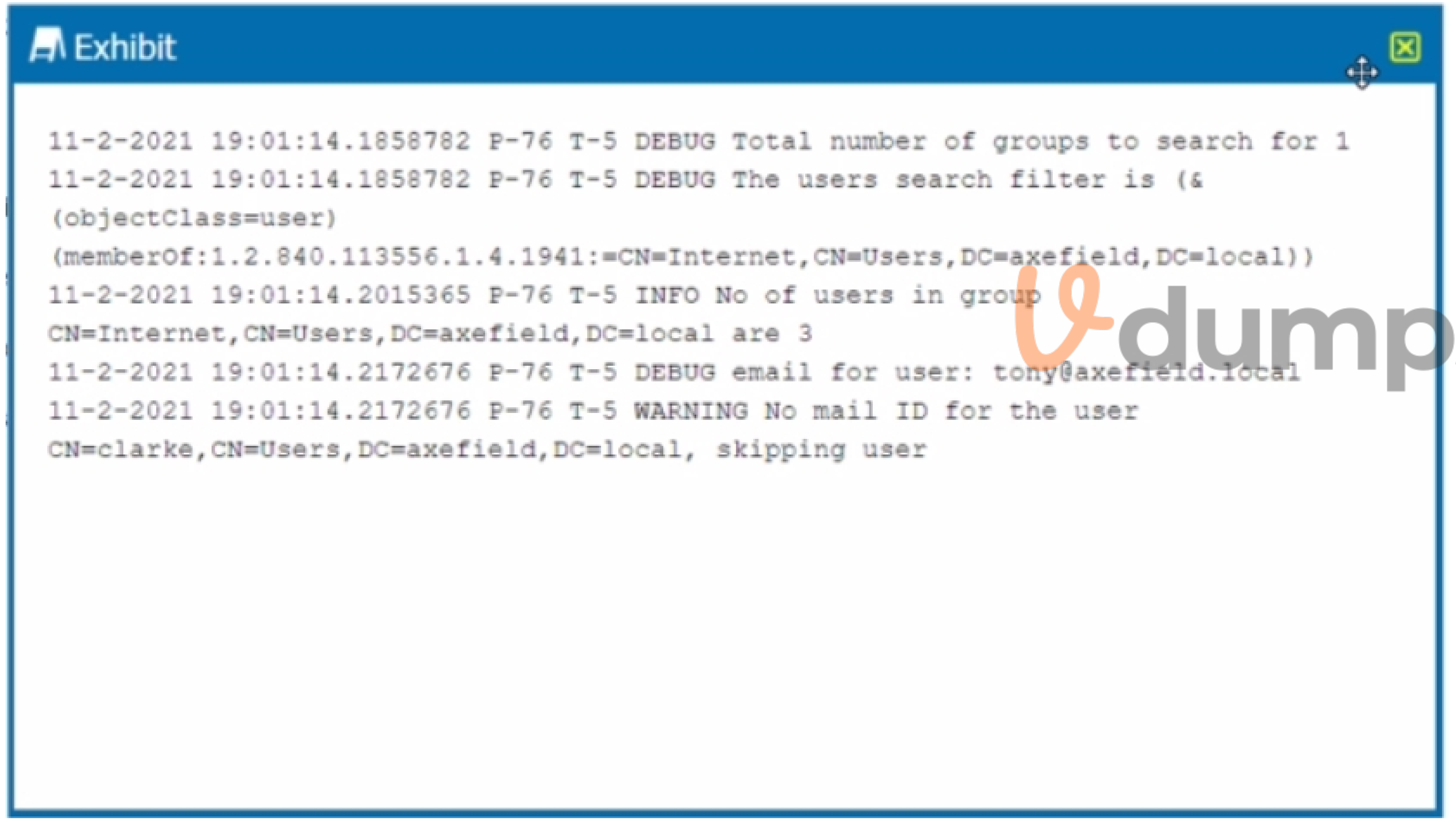
Correct Answer: A
Section:
Explanation:
Netskope can inspect outbound SMTP traffic for Microsoft Exchange and Gmail using the Netskope client. The Netskope client intercepts the SMTP traffic from the user's device and forwards it to the Netskope cloud for DLP scanning. The Netskope client does not inspect inbound SMTP traffic, as this is handled by the cloud email service or the MTA. Therefore, option A is correct and the other options are incorrect.Reference:Configure Netskope SMTP Proxy with Microsoft O365 Exchange,Configure Netskope SMTP Proxy with Gmail,SMTP DLP,Best Practices for Email Security with SMTP proxy

QUESTION 17
Your company needs to keep quarantined files that have been triggered by a DLP policy. In this scenario, which statement Is true?

A. The files are stofed remotely In your data center assigned In the Quarantine profile.
B. The files are stored In the Netskope data center assigned in the Quarantine profile.
C. The files are stored In the Cloud provider assigned In the Quarantine profile.
D. The files are stored on the administrator console PC assigned In the Quarantine profile.

Correct Answer: B
Section:
Explanation:
When a policy flags a file to be quarantined, that file is placed in a quarantine folder and a tombstone file is put in the original location in its place. The quarantine folder is located in the Netskope data center assigned in the Quarantine profile. The Quarantine profile is configured in Settings > Threat Protection > API-enabled Protection. The quarantined file is zipped and protected with a password to prevent users from inadvertently downloading the file.Netskope then notifies the admin specified in the profile1. Therefore, option B is correct and the other options are incorrect.Reference:Quarantine - Netskope Knowledge Portal,Threat Protection - Netskope Knowledge Portal

QUESTION 18
Review the exhibit.



```
11-2-2021 19:01:14.1858782 P-76 T-5 DEBUG Total number of groups to search for 1
11-2-2021 19:01:14.1858782 P-76 T-5 DEBUG The users search filter is (&
(objectClass=user)
(memberOf:1.2.840.113556.1.4.1941:=CN=Internet,CN=Users,DC=axefield,DC=local))
11-2-2021 19:01:14.2015365 P-76 T-5 INFO No of users in group
CN=Internet,CN=Users,DC=axefield,DC=local are 3
11-2-2021 19:01:14.2172676 P-76 T-5 DEBUG email for user: tony@axefield.local
11-2-2021 19:01:14.2172676 P-76 T-5 WARNING No mail ID for the user
CN=clarke,CN=Users,DC=axefield,DC=local, skipping user
```

You are troubleshooting a Netskope client for user Clarke which remains in a disabled state after being installed. After looking at various logs, you notice something which might explain the problem. The exhibit is an excerpt from the nsADImporterLog.log.
Referring to the exhibit, what is the problem?

A. The client was not Installed with administrative privileges.
B. The Active Directory user is not synchronized to the Netskope tenant.
C. This is normal; it might take up to an hour to be enabled.
D. The client traffic is decrypted by a network security device.

Correct Answer: B

Section:
Explanation:
The problem is B. The Active Directory user is not synchronized to the Netskope tenant. This is evident from the log message ''WARNING No mail ID for the user: Clarke, Daxmeifield, DC=local, skipping use''. This means that the user Clarke does not have a valid email address in the Active Directory, which is required for the Netskope client to work. The Netskope client uses the email address of the user to authenticate and enable the client. Therefore, option B is correct and the other options are incorrect.

QUESTION 19
You are having issues with fetching user and group Information periodically from the domain controller and posting that information to your tenant instance in the Netskope cloud. To begin the troubleshooting process, what would you Investigate first in this situation?

A. On-Premises Log Parser
B. Directory Importer
C. DNS Connector
D. AD Connector

Correct Answer: B
Section:
Explanation:
The Directory Importer is a component of the Netskope Adapters that connects to the domain controller and periodically fetches user and group information to post that info to your tenant instance in the Netskope cloud1. If you are having issues with this process, the first thing you should investigate is the Directory Importer itself.You can check the status of the Directory Importer service, the configuration file, the logs, and the connectivity to the domain controller and the Netskope cloud2. Therefore, option B is correct and the other options are incorrect.Reference:Configure Directory Importer - Netskope Knowledge Portal,Troubleshooting Directory Importer - Netskope Knowledge Portal

QUESTION 20
You are troubleshooting an issue with Microsoft where some users complain about an issue accessing OneDrive and SharePoint Online. The configuration has the Netskope client deployed and active for most users, but some Linux machines are routed to Netskope using GRE tunnels. You need to disable inspection for all users to begin troubleshooting the issue.
In this scenario, how would you accomplish this task?

A. Create a Real-time Protection policy to isolate Microsoft 365.
B. Create a Do Not Decrypt SSL policy for the Microsoft 365 App Suite.
C. Create a steering exception for the Microsoft 365 domains.
D. Create a Do Not Decrypt SSL policy for OneDrive.

Correct Answer: B
Section:
Explanation:
To disable inspection for all users accessing Microsoft 365, you need to create a Do Not Decrypt SSL policy for the Microsoft 365 App Suite.This policy will prevent Netskope from decrypting and analyzing the traffic for any Microsoft 365 app, regardless of the access method (Netskope client or GRE tunnel)3.This policy will also allow SNI-based policies to apply, but no deep analysis performed via Real-time Protection policies4. Therefore, option B is correct and the other options are incorrect.Reference:Add a Policy for SSL Decryption - Netskope Knowledge Portal,Default Microsoft appsuite SSL do not decrypt rule - Netskope Community

QUESTION 21
Your company has many users that are remote and travel often. You want to provide the greatest visibility into their activities, even while traveling. Using Netskope. which deployment method would be used in this scenario?

A. Use proxy chaining.
B. Use a Netskope client.
C. Use an IPsec tunnel.
D. Use a GRE tunnel.

Correct Answer: B
Section:
Explanation:
The best deployment method for remote and traveling users is to use a Netskope client.The Netskope client is a lightweight software agent that runs on the user's device and steers web and cloud traffic to the Netskope cloud for real-time inspection and policy enforcement1.The Netskope client provides an always-on end user remote access experience and avoids backhauling (or hairpinning) remote users through the corporate network to access applications in public cloud environments2.The Netskope client also supports offline mode, which allows users to work offline and sync their policies when they reconnect to the internet

QUESTION 22
Your company has Microsoft Azure ADFS set up as the Identity Provider (idP). You need to deploy the Netskope client to all company users on Windows laptops without user intervention.
In this scenario, which two deployment options would you use? (Choose two.)

A. Deploy the Netskope client with SCCM.
B. Deploy the Netskope client with Microsoft GPO.
C. Deploy the Netskope client using IdP.
D. Deploy the Netskope client using an email Invitation.

Correct Answer: A, B
Section:
Explanation:
To deploy the Netskope client to all company users on Windows laptops without user intervention, you can use either SCCM or GPO.These are two methods of packaging the application and pushing it silently to the user's device using Microsoft tools4. These methods do not require the user to have local admin privileges or to initiate the installation themselves. They also allow enforcing the use of the client through company policy.The Netskope client can authenticate the user using Azure ADFS as the identity provider, as long as the UPN of the logged in user matches the directory5

QUESTION 23
What is the purpose of the file hash list in Netskope?

A. It configures blocklist and allowlist entries referenced in the custom Malware Detection profiles.
B. It is used to allow and block URLs.
C. It provides the file types that Netskope can inspect.
D. It provides Client Threat Exploit Prevention (CTEP).

Correct Answer: A
Section:
Explanation:
The purpose of the file hash list in Netskope is to configure blocklist and allowlist entries referenced in the custom Malware Detection profiles. A file hash list is a collection of MD5 or SHA-256 hashes that represent files that you want to allow or block in your organization.You can create a file hash list when adding a file profile and use it as an allowlist or blocklist for files in your organization1.You can then select the file hash list when creating a Malware Detection profile2.

QUESTION 24
The risk team at your company has determined that traffic from the sales team to a custom Web application should not be inspected by Netskope. All other traffic to the Web application should continue to be inspected. In this scenario, how would you accomplish this task?

A. Create a Do Not Decrypt Policy using User Group and Domain in the policy page.
B. Create a Do Not Decrypt Policy using Application in the policy page and a Steering Exception for Group
C. Create a Do Not Decrypt Policy using Destination IP and Application in the policy page.
D. Create a Do Not Decrypt Policy using Source IP and Application in the policy page.

Correct Answer: A

Section:
Explanation:
To prevent traffic from the sales team to a custom Web application from being inspected by Netskope, you need to create a Do Not Decrypt Policy using User Group and Domain in the policy page.A Do Not Decrypt Policy allows you to specify the traffic you want to leave encrypted and not further analyzed by Netskope via the Real-time Protection policies3. You can use the User Group criteria to match the sales team members and the Domain criteria to match the custom Web application. This way, only the traffic from the sales team to the custom Web application will be exempted from decryption, while all other traffic to the Web application will continue to be inspected.

QUESTION 25
Your organization has a homegrown cloud application. You are required to monitor the activities that users perform on this cloud application such as logins, views, and downloaded files. Unfortunately, it seems Netskope is unable to detect these activities by default.
How would you accomplish this goal?

A. Enable access to the application with Netskope Private Access.
B. Ensure that the cloud application is added as a steering exception.
C. Ensure that the application is added to the SSL decryption policy.
D. Create a new cloud application definition using the Chrome extension.

Correct Answer: D
Section:
Explanation:
To monitor the activities that users perform on a homegrown cloud application, you need to create a new cloud application definition using the Chrome extension.The Chrome extension is a tool that allows you to record the traffic and activities of any web-based application and create a custom app definition that can be imported into your Netskope tenant1. This way, you can enable Netskope to detect and analyze the activities of your homegrown cloud application and apply policies accordingly. Therefore, option D is correct and the other options are incorrect.Reference:Creating a Cloud App Definition - Netskope Knowledge Portal

QUESTION 26
You are implementing tenant access security and governance controls for privileged users. You want to start with controls that are natively available within the Netskope Cloud Security Platform and do not require external or third-party integration.
Which three access controls would you use in this scenario? (Choose three.)

A. IP allowlisting to control access based upon source IP addresses.
B. Login attempts to set the number of failed attempts before the admin user is locked out of the UI.
C. Applying predefined or custom roles to limit the admin's access to only those functions required for their job.
D. Multi-factor authentication to verify a user's authenticity.
E. History-based access control based on past security actions.

Correct Answer: A, B, C
Section:
Explanation:
To implement tenant access security and governance controls for privileged users, you can use the following access controls that are natively available within the Netskope Cloud Security Platform and do not require external or third-party integration:
IP allowlisting to control access based upon source IP addresses.This allows you to specify the IP addresses that are allowed to access your Netskope tenant2. This can prevent unauthorized access from unknown or malicious sources.
Login attempts to set the number of failed attempts before the admin user is locked out of the UI.This allows you to configure how many times an admin can enter an incorrect password before being locked out for a specified period of time3. This can prevent brute-force attacks or password guessing attempts.
Applying predefined or custom roles to limit the admin's access to only those functions required for their job.This allows you to assign different levels of permissions and access rights to different admins based on their roles and responsibilities4. This can enforce the principle of least privilege and reduce the risk of misuse or abuse of admin privileges. Therefore, options A, B, and C are correct and the other options are incorrect.Reference:Secure Tenant Configuration and Hardening - Netskope Knowledge Portal,Admin Settings - Netskope Knowledge Portal,Create Roles - Netskope Knowledge Portal

QUESTION 27
You want to prevent a document stored in Google Drive from being shared externally with a public link. What would you configure in Netskope to satisfy this requirement?

A. Threat Protection policy
B. API Data Protection policy
C. Real-time Protection policy
D. Quarantine

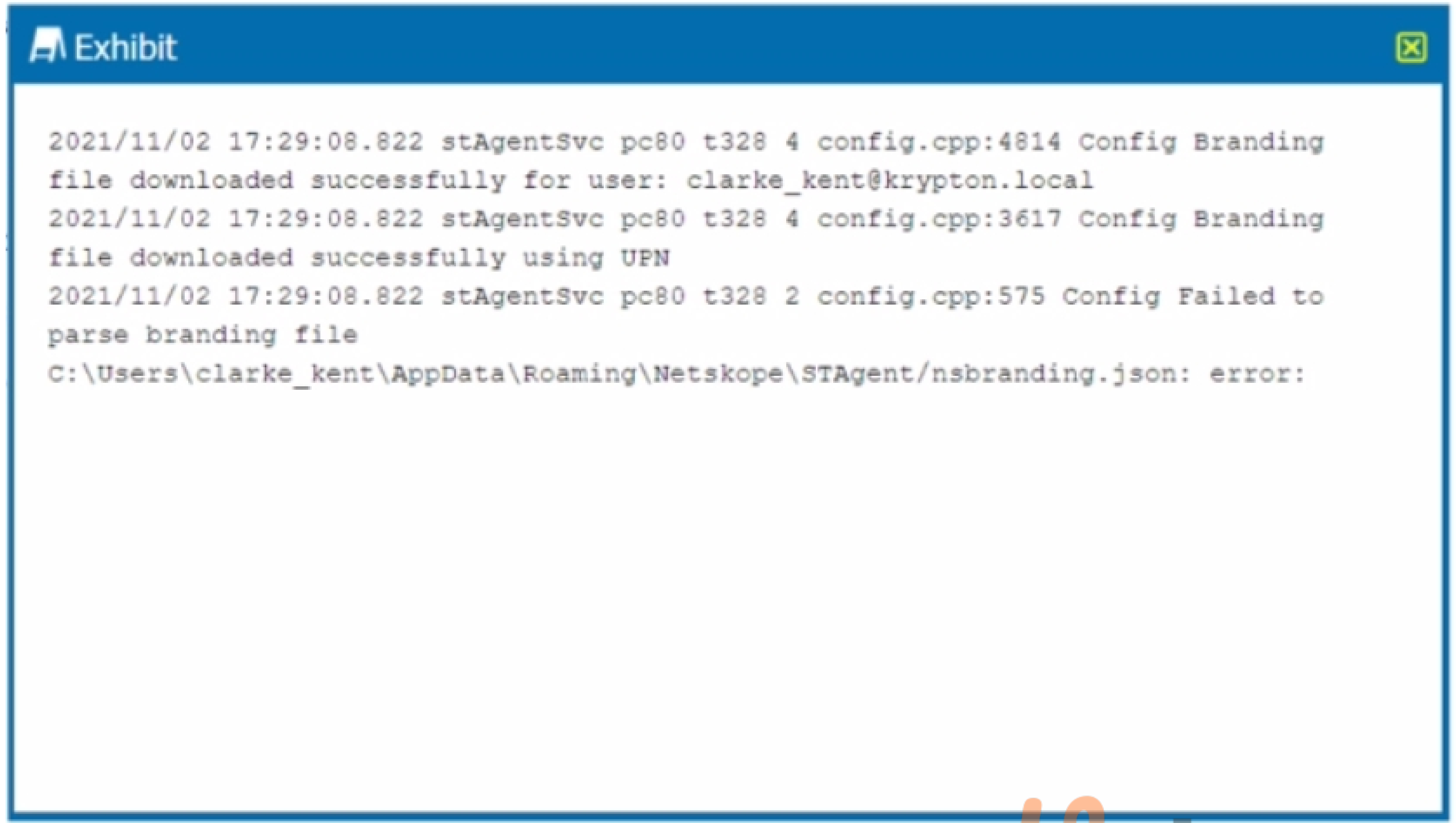
Correct Answer: B
Section:
Explanation:
To prevent a document stored in Google Drive from being shared externally with a public link, you need to configure an API Data Protection policy in Netskope.An API Data Protection policy allows you to discover, classify, and protect data that is already resident in your cloud services, such as Google Drive1. You can create a policy that matches the documents you want to protect based on criteria such as users, content, activity, or DLP profiles.Then, you can choose an action to prevent the documents from being shared externally, such as remove external collaborators, remove public links, or quarantine2. Therefore, option B is correct and the other options are incorrect.Reference:API Data Protection - Netskope Knowledge Portal,Add a Policy for API Data Protection - Netskope Knowledge Portal

QUESTION 28
A city uses many types of forms, including permit applications. These forms contain personal and financial information of citizens. Remote employees download these forms and work directly with the citizens to complete them. The city wants to be able to identify and monitor the specific forms and block the employees from downloading completed forms.
Which feature would you use to accomplish this task?

A. exact data match (EDM)
B. regular expressions (regex)
C. document fingerprinting
D. optical character recognition (OCR)

Correct Answer: C
Section:
Explanation:
To identify and monitor the specific forms used by the city and block the employees from downloading completed forms, you need to use document fingerprinting. Document fingerprinting is a feature that allows you to create a unique signature for a document based on its content and structure.You can then use this signature to match other documents that are similar or identical to the original document3.You can create a document fingerprinting profile in Netskope by uploading a sample document or selecting one from your cloud services4.You can then use this profile in your data protection policies to apply actions such as block, alert, or quarantine to the documents that match the fingerprint5. Therefore, option C is correct and the other options are incorrect.Reference:Document Fingerprinting - Netskope Knowledge Portal,Create a Document Fingerprinting Profile - Netskope Knowledge Portal,Add a Policy for Data Protection - Netskope Knowledge Portal

QUESTION 29
Review the exhibit.



```
2021/11/02 17:29:08.822 stAgentSvc pc80 t328 4 config.cpp:4814 Config Branding
file downloaded successfully for user: clarke_kent@krypton.local
2021/11/02 17:29:08.822 stAgentSvc pc80 t328 4 config.cpp:3617 Config Branding
file downloaded successfully using UPN
2021/11/02 17:29:08.822 stAgentSvc pc80 t328 2 config.cpp:575 Config Failed to
parse branding file
C:\Users\clarke_kent\AppData\Roaming\Netskope\STAgent/nsbranding.json: error:
```

You receive a service request from a user who indicates that their Netskope client is in a disabled state. The exhibit shows an excerpt (rom the affected client nsdebuglog.log.
What is the problem in this scenario?

A. User authentication failed during IdP-based enrollment.
B. The Netskope client connection is being decrypted.
C. Custom installation parameters are incorrectly specified
D. The user's account has not been provisioned into Netskope.

Correct Answer: B
Section:
Explanation:
The problem in this scenario is that the Netskope client connection is being decrypted by a network security device. This is evident from the log message ''ERROR SSL certificate verification failed: self signed certificate in certificate chain''. This means that the Netskope client is receiving a certificate that is not issued by Netskope, but by a device that is intercepting and decrypting the traffic between the client and the Netskope cloud.This can cause the client to fail to download the required configuration and remain in a disabled state1. Therefore, option B is correct and the other options are incorrect.Reference:Troubleshooting Netskope Client - Netskope Knowledge Portal,Using Netskope Client - Netskope Knowledge Portal

QUESTION 30
Your customer is migrating all of their applications over to Microsoft 365 and Azure. They have good practices and policies in place (or their inline traffic, but they want to continuously detect reconfigurations and enforce compliance standards.
Which two solutions would satisfy their requirements? (Choose two.)

A. Netskope SaaS Security Posture Management
B. Netskope Cloud Confidence Index
C. Netskope Risk Insights

D. Netskope Continuous Security Assessment

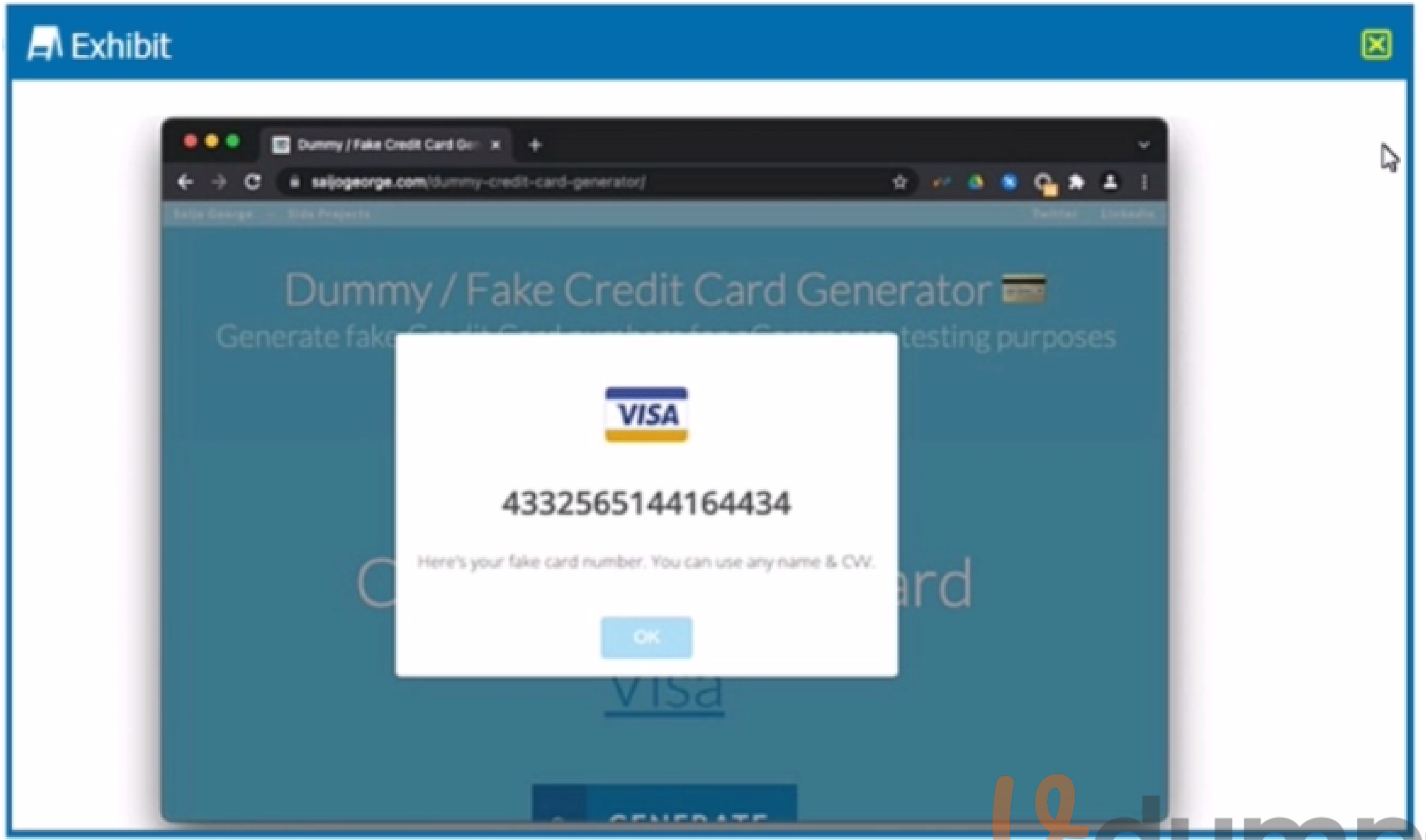
Correct Answer: A, D
Section:
Explanation:
To continuously detect and enforce compliance standards for their Microsoft 365 and Azure applications, the customer needs to use Netskope SaaS Security Posture Management (SSPM) and Netskope Continuous Security Assessment (CSA). Netskope SSPM allows the customer to monitor, assess, and act on security, permission, and access related issues in their SaaS environment, such as Microsoft 365. Netskope SSPM continuously checks security posture by comparing SaaS app settings with security policies and industry benchmarks (CIS, PCI-DSS, NIST, HIPAA, CSA, GDPR, AIPCA, ISO, and more).It also provides visibility and control over third-party apps that are connected to the managed apps1. Netskope CSA allows the customer to discover, audit, and remediate misconfigurations in their IaaS environment, such as Azure. Netskope CSA continuously monitors and audits cloud configurations against industry standards, CIS benchmarks, and regulatory frameworks.It also provides real-time inline protection to secure public clouds from threats and data loss2. Therefore, options A and D are correct and the other options are incorrect.Reference:SaaS Security Posture Management - Netskope,Public Cloud Security Solutions - Netskope

QUESTION 31
You are an administrator writing Netskope Real-time Protection policies and must determine proper policy ordering.
Which two statements are true in this scenario? (Choose two.)

A. You must place Netskope private access malware policies in the middle.
B. You do not need to create an 'allow all' Web Access policy at the bottom.
C. You must place DLP policies at the bottom.
D. You must place high-risk block policies at the top.

Correct Answer: B, D
Section:
Explanation:
To determine proper policy ordering for Netskope Real-time Protection policies, you need to follow these two statements: B. You do not need to create an ''allow all'' Web Access policy at the bottom. D. You must place high-risk block policies at the top.These statements are based on the best practices for policy ordering recommended by Netskope3. An ''allow all'' Web Access policy at the bottom is not necessary because any traffic that does not match any policy will be allowed by default.However, you can create a ''monitor all'' Web Access policy at the bottom if you want to log all the traffic that is not matched by any other policy4. High-risk block policies at the top are important because they prevent any traffic that poses a serious threat or violates a critical compliance standard from reaching its destination.These policies should have higher priority than other policies that may allow or modify the traffic5. Therefore, options B and D are correct and the other options are incorrect.Reference:Real-time Protection Policies - Netskope Knowledge Portal,Create a Real-time Protection Policy for Web Categories - Netskope Knowledge Portal,Best Practices: Real-time Protection Policies (1 of 2) - Netskope

QUESTION 32
Review the exhibit.



Exhibit

Dummy / Fake Credit Card Generator

saijogeorge.com/dummy-credit-card-generator/

Dummy / Fake Credit Card Generator

Generate fake ... testing purposes

VISA

4332565144164434

Here's your fake card number. You can use any name & CVV.

You are asked to create a DLP profile that will ensure that the data shown in the exhibit cannot be uploaded to a user's personal Google Drive.
What must be used to accomplish this task?

A. document fingerprinting
B. ML image classifier
C. optical character recognition
D. INTL-PAN-Name rule

Correct Answer: C
Section:
Explanation:
To create a DLP profile that will ensure that the data shown in the exhibit cannot be uploaded to a user's personal Google Drive, you need to use optical character recognition (OCR). OCR is a feature that allows you to detect and extract text from images and scanned documents.You can use OCR in your DLP profiles to identify sensitive data that is embedded or hidden in images1. In the exhibit, we can see that the data is a credit card number, which is a type of sensitive data that can be easily identified by OCR. You can create a DLP profile that uses OCR and matches the credit card number data identifier or a custom regex expression.You can then apply an action such as block, alert, or quarantine to prevent the data from being uploaded to Google Drive2. Therefore, option C is correct and the other options are incorrect.Reference:Optical Character Recognition (OCR) - Netskope Knowledge Portal,Add a Policy for Data Protection - Netskope Knowledge Portal

QUESTION 33
Your customer implements Netskope Secure Web Gateway to secure all Web traffic. While they have created policies to block certain categories, there are many new sites available dally that are not yet categorized. The customer's users need quick access and cannot wait to put in a request to gain access requiring a policy change or have the site's category changed.
To solve this problem, which Netskope feature would provide quick, safe access to these types of sites?

A. Netskope Cloud Firewall (CFW)
B. Netskope Remote Browser Isolation (RBI)

C. Netskope Continuous Security Assessment (CSA)
D. Netskope SaaS Security Posture Management (SSPM)

Correct Answer: B
Section:
Explanation:
To solve the problem of providing quick, safe access to uncategorized and risky websites, the Netskope feature that the customer should use is Netskope Remote Browser Isolation (RBI). Netskope RBI is a part of the Netskope Secure Web Gateway offering that intercepts a user's browsing session to a website, acting as a proxy that fetches the content for that user and renders the content in an isolated browsing instance. The rendered content is delivered to the user's browser as a safe stream of pixels.This safely silos the end user's device and the enterprise network and systems, separating it from their browsing activity and restricting the ability of an attacker to establish control and / or breach other systems and exfiltrate data1.Netskope RBI can be easily invoked with an 'isolate' policy action within the Netskope Security Cloud for any website category or domain2. Therefore, option B is correct and the other options are incorrect.Reference:Remote Browser Isolation - Netskope Knowledge Portal,Netskope Remote Browser Isolation - Netskope

QUESTION 34
You are creating an API token to allow a DevSecOps engineer to create and update a URL list using REST API v2. In this scenario, which privilege(s) do you need to create in the API token?

A. Provide read and write access for the '/events' endpoint.
B. Provide read and write access for the '/urllist' endpoint.
C. Provide only read access for the '/urllist' endpoint.
D. Provide only write access for the '/urllist' endpoint.

Correct Answer: B
Section:
Explanation:
To create an API token to allow a DevSecOps engineer to create and update a URL list using REST API v2, you need to provide read and write access for the ''/urllist'' endpoint. The ''/urllist'' endpoint is the API endpoint that allows you to manage URL lists in your Netskope tenant.You can use this endpoint to perform operations such as create, update, delete, or list URL lists3.To create an API token with this privilege, you need to go to Settings > Tools > REST API v2 > New Token, enter a token name and expiration time, add the ''/urllist'' endpoint, and select Read+Write as the privilege4. This will allow the DevSecOps engineer to use the API token in their requests to create and update URL lists. Therefore, option B is correct and the other options are incorrect.Reference:REST API v2 Overview - Netskope Knowledge Portal,Manage URL Lists - Netskope Knowledge Portal

QUESTION 35
You are asked to grant access for a group of users to an application using NPA. So far, you have created and deployed the publisher and created a private application using the Netskope console. Which two steps must also be completed to enable your users access to the application? (Choose two.)

A. Create an inbound firewall rule to permit network traffic to reach the publisher
B. Enable traffic steering for private applications.
C. Create a Real-time Protection policy that allows your users to access the application.
D. Define an application instance name in Skope IT.

Correct Answer: B, C
Section:
Explanation:
To enable your users access to the application using NPA, you need to complete these two steps: B. Enable traffic steering for private applications and C. Create a Real-time Protection policy that allows your users to access the application. Traffic steering is the process of directing the user's traffic to the Netskope cloud platform for inspection and policy enforcement.You need to enable traffic steering for private applications in your traffic steering profile to allow the Netskope client to tunnel the traffic to the private application through the Netskope cloud1. A Real-time Protection policy is a rule that specifies the actions and notifications that Netskope applies to the user's traffic based on various criteria.You need to create a Real-time Protection policy that allows your users to access the private application by selecting the application name, the user group, and the allow action in the policy page2. Therefore, options B and C are correct and the other options are incorrect.Reference:Traffic Steering Profile - Netskope Knowledge Portal,Add a Policy for Real-time Protection - Netskope Knowledge Portal

QUESTION 36

A customer wants to deploy the Netskope client on all their employee laptops to protect all Web traffic when users are working from home. However, users are required to work from their local offices at least one day per week. Management requests that users returning to the office be able to transparently leverage the local security stack without any user intervention.
Which two statements are correct in this scenario? (Choose two.)

A. You must enable On-premises Detection in the client configuration.
B. You must allow users to unenroll In the client configuration.
C. You must disable Dynamic Steering in the traffic steering profile.
D. You must configure IPsec/GRE tunnels on the local network to steer traffic to Netskope.

Correct Answer: A, C
Section:
Explanation:
To allow users to transparently leverage the local security stack when they return to the office, you need to follow these two statements: A. You must enable On-premises Detection in the client configuration and C. You must disable Dynamic Steering in the traffic steering profile. On-premises Detection is a feature that allows the Netskope client to detect whether it is on-premises or off-premises based on a DNS or HTTP probe.You need to enable On-premises Detection in the client configuration and specify a domain name or an HTTP address that is only accessible from your local network3. Dynamic Steering is a feature that allows you to steer different types of traffic differently based on various criteria such as user group, location, category, etc.You need to disable Dynamic Steering in the traffic steering profile or create an exception for your local network to bypass Netskope and use your local security stack4. Therefore, options A and C are correct and the other options are incorrect.Reference:Client Configuration - Netskope Knowledge Portal,Dynamic Steering - Netskope Knowledge Portal

QUESTION 37
You are using the Netskope DLP solution. You notice that valid credit card numbers in a file that you just uploaded to an unsanctioned cloud storage solution are not triggering a policy violation. You can see the Skope IT application events for this traffic but no DLP alerts.
Which statement is correct in this scenario?

A. Netskope client is not enabled.
B. You have set the severity threshold to a higher value.
C. Netskope client is enabled, but API protection for the SaaS application is not configured.
D. Credit card numbers are entered with a space or dash separator and not as a 16-digit consecutive number.

Correct Answer: D
Section:
Explanation:
The statement that is correct in this scenario is D. Credit card numbers are entered with a space or dash separator and not as a 16-digit consecutive number. This is one of the possible reasons why valid credit card numbers in a file are not triggering a policy violation by Netskope DLP. Netskope DLP uses data identifiers to detect sensitive data in files and network traffic.Data identifiers are predefined or custom rules that match data patterns based on regular expressions, checksums, keywords, etc1.The credit card number data identifier matches 16-digit consecutive numbers that pass the Luhn algorithm check2. If the credit card numbers are entered with a space or dash separator, such as 1234-5678-9012-3456 or 1234 5678 9012 3456, they will not match the data identifier and will not trigger a policy violation.To solve this problem, you can either remove the separators from the credit card numbers or create a custom data identifier that matches the credit card numbers with separators3. Therefore, option D is correct and the other options are incorrect.Reference:Data Identifiers - Netskope Knowledge Portal,Credit Card Number - Netskope Knowledge Portal,Create a Custom Data Identifier - Netskope Knowledge Portal

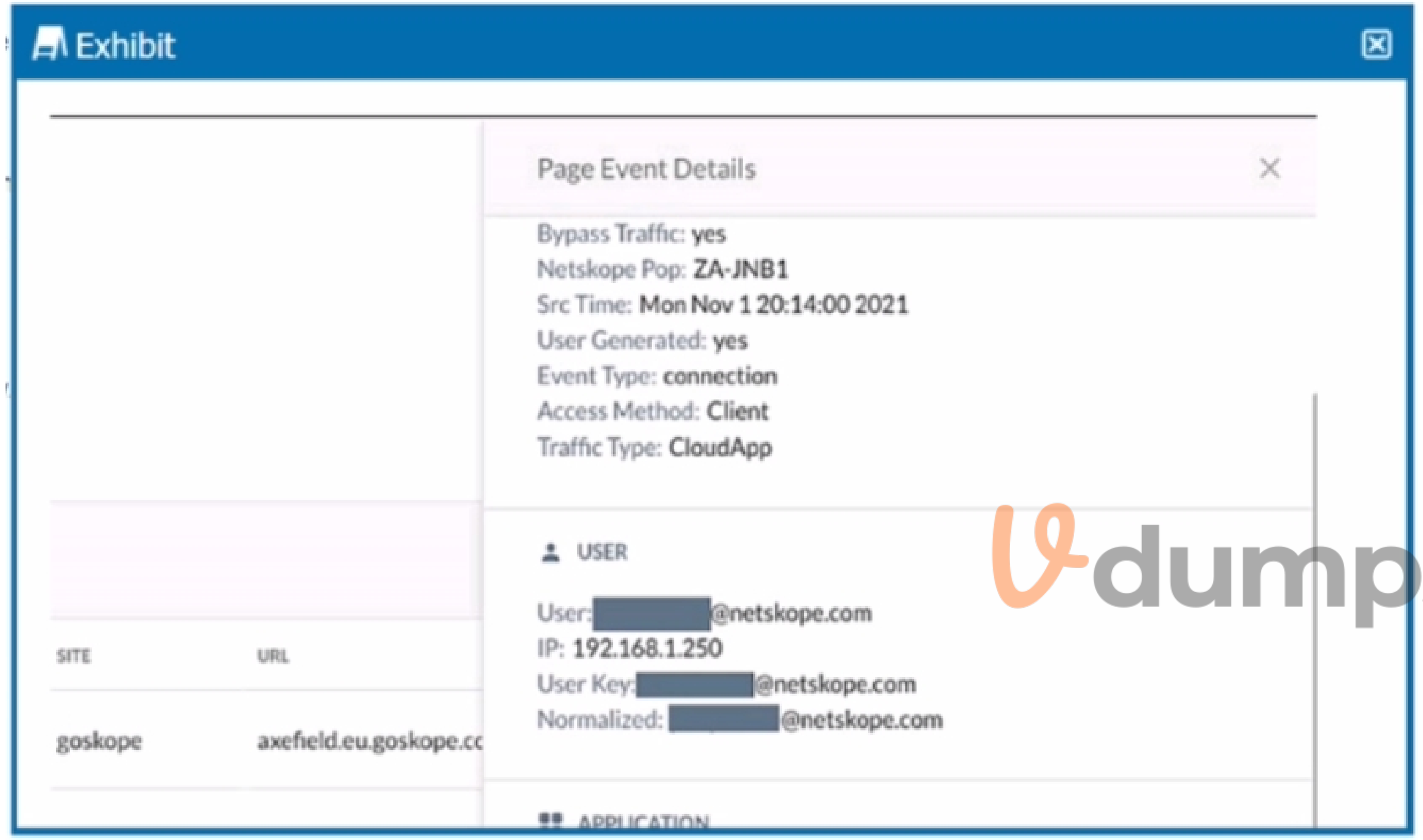
QUESTION 38
Netskope is being used as a secure Web gateway. Your organization's URL list changes frequently. In this scenario, what makes It possible for a mass update of the URL list in the Netskope platform?

A. REST API v2
B. Assertion Consumer Service URL
C. Cloud Threat Exchange
D. SCIM provisioning

Correct Answer: A
Section:

Explanation:
The method that makes it possible for a mass update of the URL list in the Netskope platform is A. REST API v2.REST API v2 is a feature that allows you to use an auth token to make authorized calls to the Netskope API and access resources via URI paths5.You can use REST API v2 to update a URL list with new values by providing the name of an existing URL list and a comma-separated list of URLs or IP addresses6. This can help you automate or script the management of your URL lists and keep them up-to-date. Therefore, option A is correct and the other options are incorrect.Reference:REST API v2 Overview - Netskope Knowledge Portal,Update a URL List - Netskope Knowledge Portal

QUESTION 39
Review the exhibit.



Exhibit

Page Event Details

Bypass Traffic: yes
Netskope Pop: ZA-JNB1
Src Time: Mon Nov 1 20:14:00 2021
User Generated: yes
Event Type: connection
Access Method: Client
Traffic Type: CloudApp

USER

User:[redacted]@netskope.com
IP: 192.168.1.250
User Key:[redacted]@netskope.com
Normalized: [redacted]@netskope.com

APPLICATION

SITE	URL
goskope	axefield.eu.goskope.cc

You are asked to restrict users from accessing YouTube content tagged as Sport. You created the required real-time policy; however, users can still access the content, referring to the exhibit, what is the problem?

A. The website is in a steering policy exception.
B. The policy changes have not been applied.
C. The YouTube content cannot be controlled.
D. The traffic matched a Do Not Decrypt policy

Correct Answer: D
Section:
Explanation:
The problem in this scenario is that the traffic matched a Do Not Decrypt policy.A Do Not Decrypt policy is a rule that specifies the traffic that you want to leave encrypted and not further analyzed by Netskope via the Real-time Protection policies1. In the exhibit, we can see that the traffic from the user to YouTube has a ''Bypass Traffic'' value of ''yes'' and a ''Netskope'' value of ''yes''.This means that the traffic was steered to Netskope but not decrypted or inspected2. Therefore, the real-time policy that was created to restrict users from accessing YouTube content tagged as Sport did not apply, and users could still access the content.To solve this problem, you need to either remove or modify the Do Not Decrypt policy that matches the traffic to YouTube, or create an exception for the Sport category in the policy3. Therefore, option D is correct and the other options are incorrect.Reference:Page Events - Netskope Knowledge Portal,Add a Policy for SSL Decryption - Netskope Knowledge Portal,YouTube Content Control - Netskope Knowledge Portal