ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

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

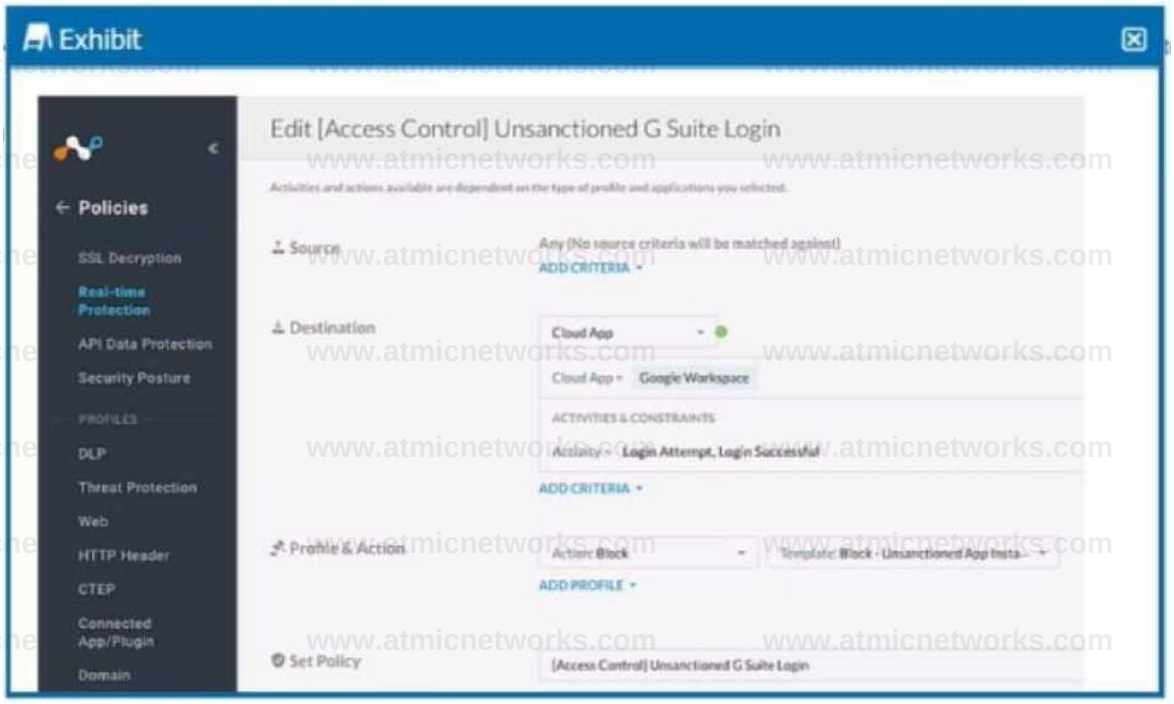
Answer: ABD

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: 2

Review the exhibit.



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

Answer: B

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: 3

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.

Answer: BD

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: 4

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.

Answer: A

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: 5

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)

Answer: C

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: 6

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.

Answer: AC

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: 7

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

A. DLP profile

B. File profile

C. Domain profile

D. User profile

Answer: B

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: 8

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.

Answer: BC

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: 9

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.

Answer: A

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: 10

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.

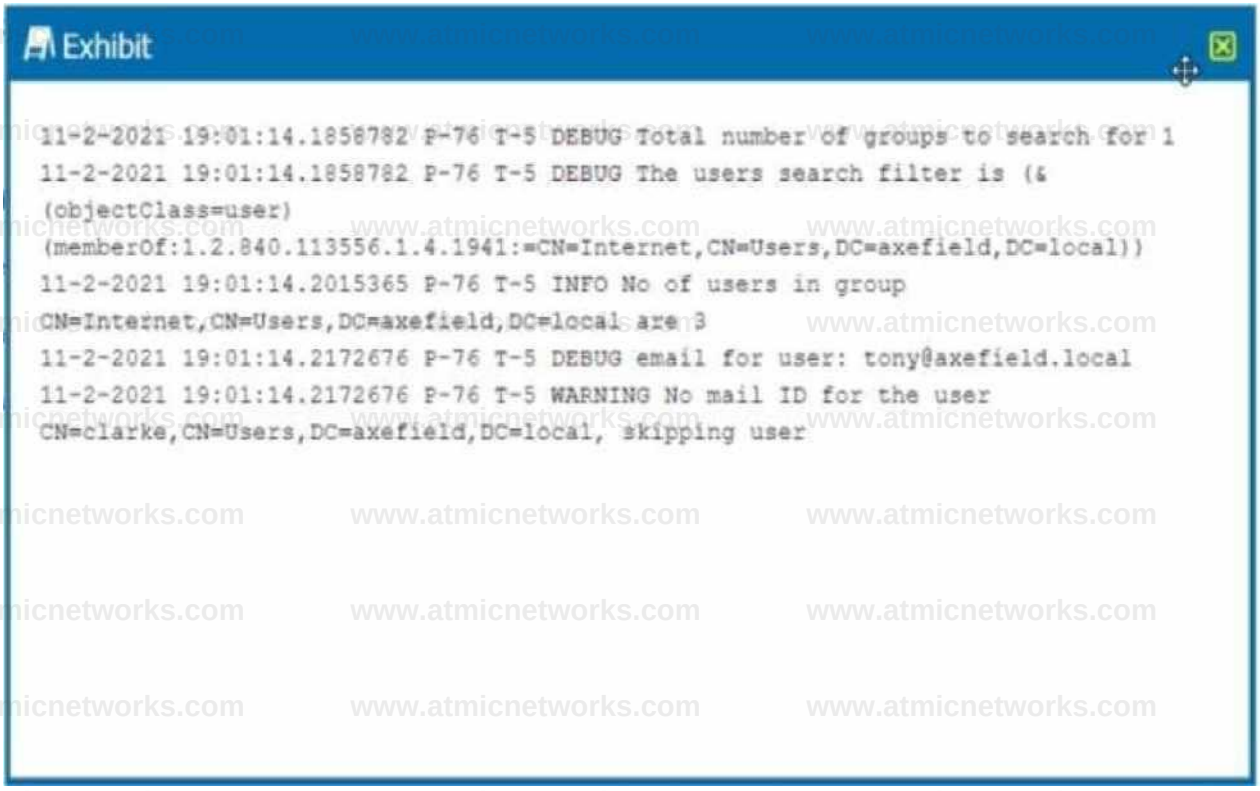
Answer: B

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: 11

Review the exhibit.



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.

Answer: B

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: 12

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

Answer: B

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: 13

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.

Answer: B

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: 14

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.

Answer: B

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: 15

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.

Answer: AB

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: 16

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).

Answer: A

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: 17

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 aDo NotDecrypt Policy using User Group and Domain in the policy page.

B. Create aDo NotDecrypt Policy using Application in the policy page and a Steering Exception for Group

C. Create aDo NotDecrypt Policy using Destination IP and Application in the policy page.

D. Create aDo NotDecrypt Policy using Source IP and Application in the policy page.

Answer: A

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: 18

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.

Answer: D

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: 19

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.

Answer: ABC

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: 20

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

Answer: B

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: 21

Recently your company implemented Zoom for collaboration purposes and you are attempting to inspect the traffic with Netskope. Your initial attempt reveals that you are not seeing traffic from the Zoom client that is used by all users. You must ensure that this traffic is visible to Netskope.

In this scenario, which two steps must be completed to satisfy this requirement? (Choose two.)

A. Create a steering exception for Zoom to ensure traffic is reaching Netskope.

B. Create a Do Not Decrypt SSL policy for the Zoom application suite.

C. Remove the Zoom certificate-pinned application from the default steering configuration.

D. Remove the default steering exception for the Web Conferencing Category.

Answer: CD

Explanation:

To ensure that the traffic from the Zoom client is visible to Netskope, you need to remove the Zoom certificate-pinned application from the default steering configuration and remove the default steering exception for the Web Conferencing Category. A certificate-pinned application is an

application that validates the server certificates against the hardcoded ones in the application. This is a security technique used to prevent man-in-the-middle attacks and secure access to the application. By default, Netskope bypasses the traffic from certificate-pinned applications and does not decrypt or inspect it3. Zoom is one of the predefined certificate-pinned applications that Netskope supports4. To enable Netskope to inspect the traffic from Zoom, you need to remove it from the steering configuration that applies to your users5. Additionally, you need to remove the default steering exception for the Web Conferencing Category, which includes Zoom and other similar applications. A steering exception is a rule that specifies the traffic that you want to bypass Netskope and go directly to the destination6. By removing this exception, you allow Netskope to steer and analyze the traffic from web conferencing applications. Therefore, options C and D are correct and the other options are incorrect. Reference: Certificate Pinned Applications - Netskope Knowledge Portal, Certificate Pinned App (CPA) - The Netskope Community, Steering Configuration - Netskope Knowledge Portal, Steering Exceptions - Netskope Knowledge Portal

Question: 22

Which statement describes how Netskope's REST API, v1 and v2, handles authentication?

A. Both REST API v1 and v2 require the use of tokens to make calls to the API

B. Neither REST API v1 nor v2 require the use of tokens.

C. REST API v2 requires the use of a token to make calls to the API. while API vI does not.

D. REST API v1 requires the use of a token to make calls to the API. while API v2 does not.

Answer: A

Explanation:

The statement that describes how Netskope's REST API, v1 and v2, handles authentication is A. Both REST API v1 and v2 require the use of tokens to make calls to the API. A token is a unique string that identifies the user or application that is making the API request. The token must be included in the HTTP header of every API call as an authorization parameter1. The token can be generated from the Netskope UI or from the Netskope Platform API2. The token can also be revoked or refreshed as needed3. Therefore, option A is correct and the other options are incorrect. Reference: REST API v1 Overview - Netskope Knowledge Portal, Netskope Platform API Endpoints for REST API v1 - Netskope Knowledge Portal, REST API v2 Overview - Netskope Knowledge Portal

Question: 23

You are provisioning Netskope users from Okta with SCIM Provisioning, and users are not showing up in the tenant. In this scenario, which two Netskope components should you verify first In Okta for accuracy? (Choose two.)

A. IdP Entity ID

B. OAuth token

C. Netskope SAML certificate

D. SCIM server URL

Answer: BD

Explanation:

To provision Netskope users from Okta with SCIM Provisioning, and users are not showing up in the tenant, the two Netskope components that you should verify first in Okta for accuracy are B. OAuth token and D. SCIM server URL. The OAuth token is a credential that allows Okta to authenticate with the Netskope SCIM server and perform user provisioning operations4. The SCIM server URL is the endpoint that Okta uses to communicate with the Netskope SCIM

server and send user data5. Both of these components must be configured correctly in Okta for the SCIM Provisioning to work. You can find them in the Netskope UI under Settings > Tools > Directory Tools > SCIM Integration6. Therefore, options B and D are correct and the other options are incorrect. Reference: SCIM-Based User Provisioning - Netskope Knowledge Portal, Netskope + Okta Use Case: Provisioning Users and Managing Groups Using SCIM - Netskope, Netskope Partner Okta - Netskope

Question: 24

You are given an MD5 hash of a file suspected to be malware by your security incident response team. They ask you to offer insight into who has encountered this file and from where was the threat initiated. In which two Skope IT events tables would you search to find the answers to these questions? (Choose two.)

A. Application Events

B. Network Events

C. Alerts

D. Page Events

Answer: AC

Explanation:

To find the answers to the questions posed by the security incident response team, you need to search in the Application Events and Alerts tables in Skope IT. The Application Events table shows the details of the cloud application activities performed by the users, such as upload, download, share, etc. You can filter the Application Events table by the MD5 hash of the file to find out who has encountered this file and from which cloud service it was downloaded1. The Alerts table shows the details of the policy violations triggered by the users, such as DLP, threat protection, anomaly detection, etc. You can filter the Alerts table by the MD5 hash of the file to find out if this file was detected as malware by Netskope and what action was taken2. Therefore, options A and C are correct and the other options are incorrect. Reference: Application Events - Netskope Knowledge Portal, Alerts - Netskope Knowledge Portal

Question: 25

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)

Answer: C

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: 26

Review the exhibit.

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.

Answer: B

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: 27

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

Answer: AD

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: 28

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.

Answer: BD

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: 29

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.

Answer: ACE

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: 30

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

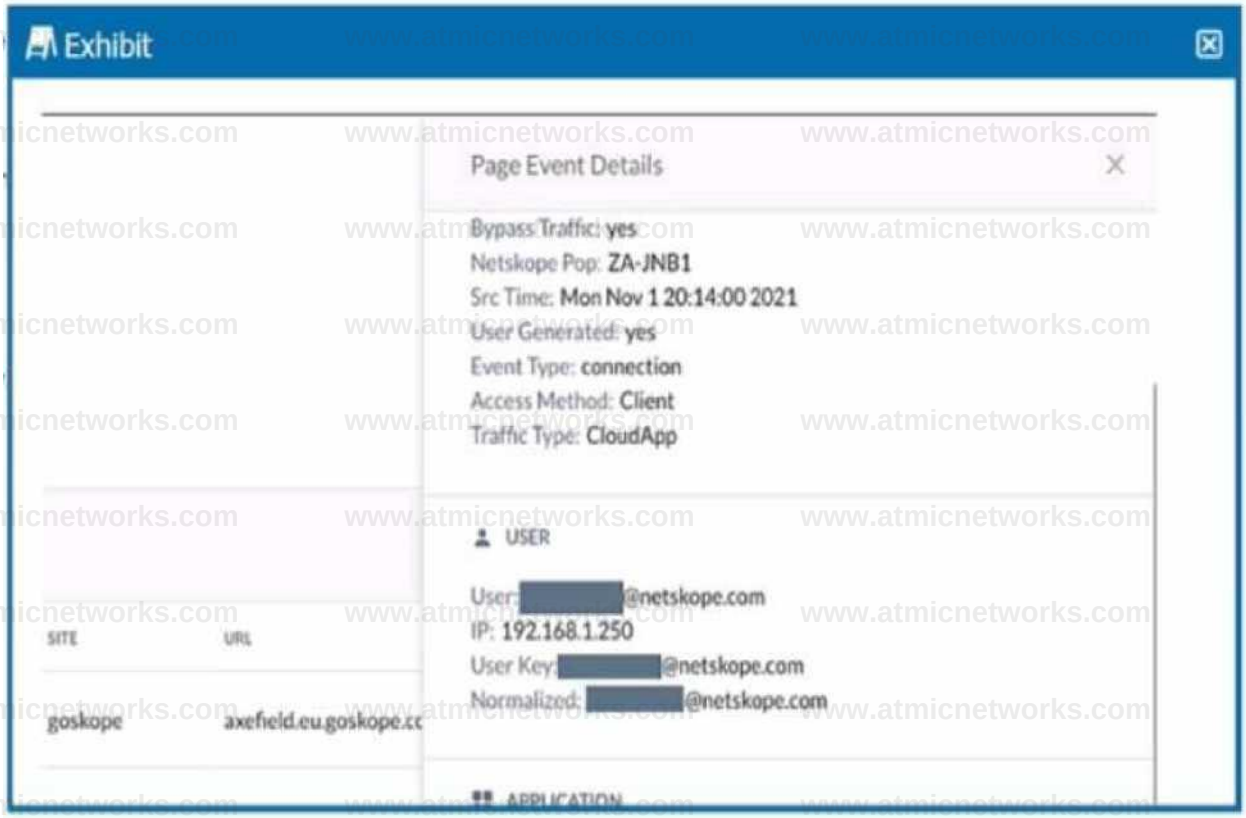
Answer: A

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: 31

Review the exhibit.



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

Answer: D

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

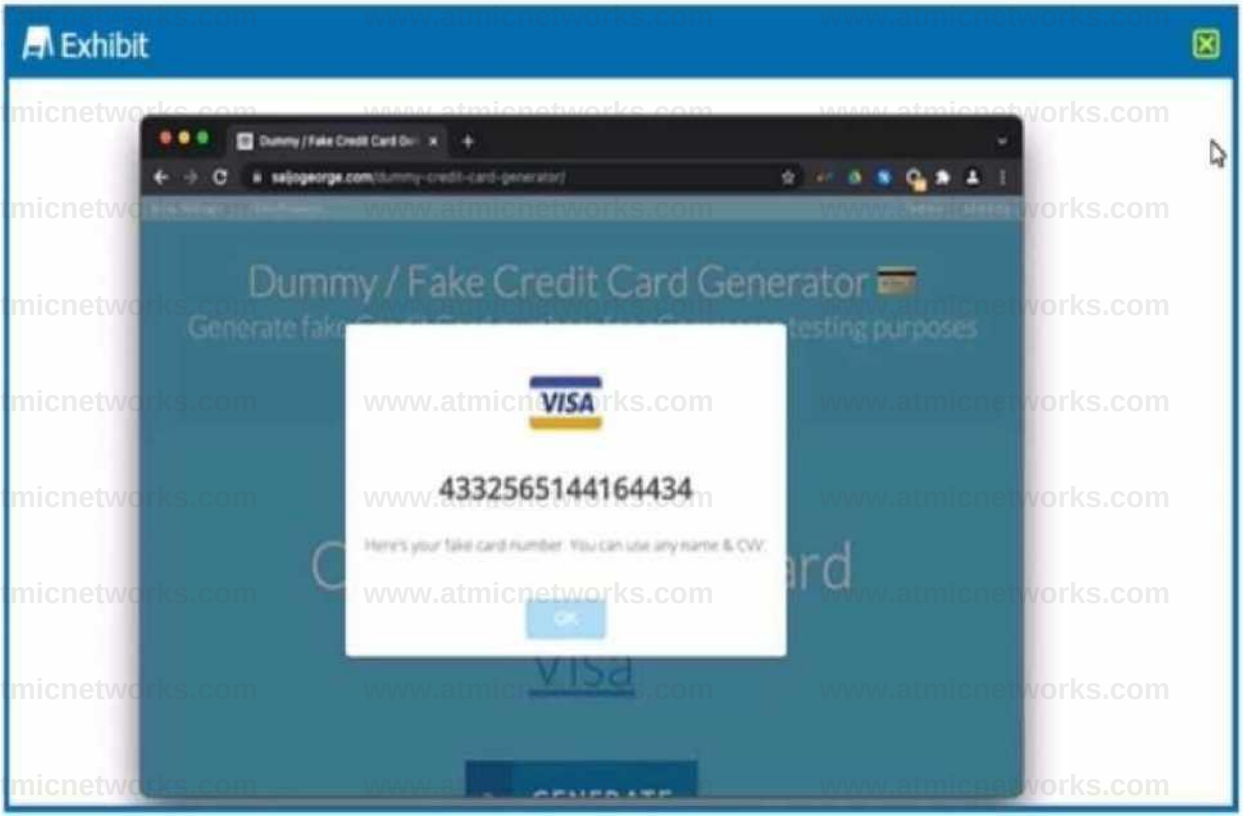
"Netskope" value of "yes". This means that the traffic was steered to Netskope but not decrypted or inspected2.

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

Question: 32

Review the exhibit.



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

Answer: C

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)

Answer: B

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.

Answer: B

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 NP

A. 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.

Answer: BC

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.

Answer: AC

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.

Answer: D

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

Review the exhibit.

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.

Answer: D

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: 39

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.

Answer: D

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: 40

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

Answer: AD

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: 41

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.

Answer: BC

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: 42

Which statement describes a requirement for deploying a Netskope Private Application (NPA) Publisher?

A. The publisher must be deployed in a public cloud environment, such as AWS.

B. The publisher must be deployed in a private data center.

C. The publisher must be deployed on the network where the private application will be accessed.

D. The publisher's name must match the name of the application process that it will access.

Answer: C

Explanation:

The statement that describes a requirement for deploying a Netskope Private Application (NPA) Publisher is C. The publisher must be deployed on the network where the private application will be accessed. A NPA Publisher is a software component that enables Netskope to discover resources that users will connect to via NPA. A NPA Publisher must be deployed on the same network as the private application that it will publish, such as a public cloud environment (AWS, Azure, GCP) or a private data center3. This ensures that the NPA Publisher can communicate with the private application and relay its traffic to the NPA service in the Netskope cloud. Therefore, option C is correct and the other options are incorrect. Reference: Deploy a Publisher - Netskope Knowledge Portal

Question: 43

The director of IT asks for confirmation If your organization's Web traffic would be blocked when the Netskope client fails. In this situation, what would confirm the fail close status?

A. Perform a right-click on the Netskope client icon using your mouse.

B. Review the nsdebuglog.log.

C. View Application events.

D. Review user settings.

Answer: B

Explanation:

The method that would confirm the fail close status is B. Review the nsdebuglog.log. The nsdebuglog.log is a log file that contains information about the Netskope client's status, configuration, events, errors, etc. You can review the nsdebuglog.log file to confirm the fail close status by looking for a line that says "failCloseStatus":"1". This indicates that the fail close option is enabled for the Netskope client4. The fail close option is a feature that allows you to block all web traffic when the Netskope client fails or loses connection to the Netskope cloud5. Therefore, option B is correct and the other options are incorrect. Reference: Troubleshooting Netskope Client - Netskope Knowledge Portal, Client Configuration - Netskope Knowledge Portal

Question: 44

Your company asks you to use Netskope to integrate with Endpoint Detection and Response (EDR) vendors such as CrowdStrike. In this scenario, what is a requirement for a successful Integration and sharing of threat data?

A. API Client ID

B. device classification

C. custom log parser

D. user endpoint

Answer: A

Explanation:

To integrate Netskope with EDR vendors such as CrowdStrike and share threat data, a requirement for a successful integration is A. API Client ID. An API Client ID is a unique identifier that is used to authenticate and authorize requests to the EDR vendor's API. You need to obtain an API Client ID from the EDR vendor and enter it in the Netskope tenant settings under Threat Protection > Integration. This will allow Netskope to communicate with the EDR vendor and exchange threat intelligence and remediation actions1. Therefore, option A is correct and the other options are incorrect. Reference: Integrating CrowdStrike for EDR - Netskope Knowledge Portal

Question: 45

You are integrating Netskope tenant administration with an external identity provider. You need to implement role-based access control. Which two statements are true about this scenario? (Choose two.)

A. The roles you want to assign must be present in the Netskope tenant.

B. You do not need to define the administrators locally in the Netskope tenant after It Is integrated with IdP.

C. You need to define the administrators locally in the Netskope tenant.

D. Once integrated with IdP. you must append the "locallogin" URL to log in using IdP

Answer: AC

Explanation:

To implement role-based access control when integrating Netskope tenant administration with an external identity provider (IdP), two statements that are true about this scenario are A. The roles you want to assign must be present in the Netskope tenant and C. You need to define the administrators locally in the Netskope tenant. Role-based access control (RBAC) is a feature that allows you to assign different levels of permissions and access to the Netskope tenant based on the user's role. You can use RBAC to integrate Netskope tenant administration with an external IdP such as Azure AD or Okta and delegate administrative tasks to different users or groups1. To do this, you need to ensure that the roles you want to assign are present in the Netskope tenant. You can use the predefined roles such as SYSADMIN, AUDITOR, or OPERATOR, or create custom roles with specific privileges2. You also need to define the administrators locally in the Netskope tenant by creating local user accounts and

assigning them roles. You can use the same email address as the IdP user account for the local user account3. Therefore, options A and C are correct and the other options are incorrect. Reference: Role-Based Access Control - Netskope Knowledge Portal, Roles - Netskope Knowledge Portal, Integrate with Azure AD - Netskope Knowledge Portal

Question: 46

Your organization has three main locations with 30.000 hosts in each location. You are planning to deploy Netskope using iPsec tunnels for security.

What are two considerations to make a successful connection in this scenario? (Choose two.)

A. browsers in use

B. operating systems

C. redundant POPs

D. number of hosts

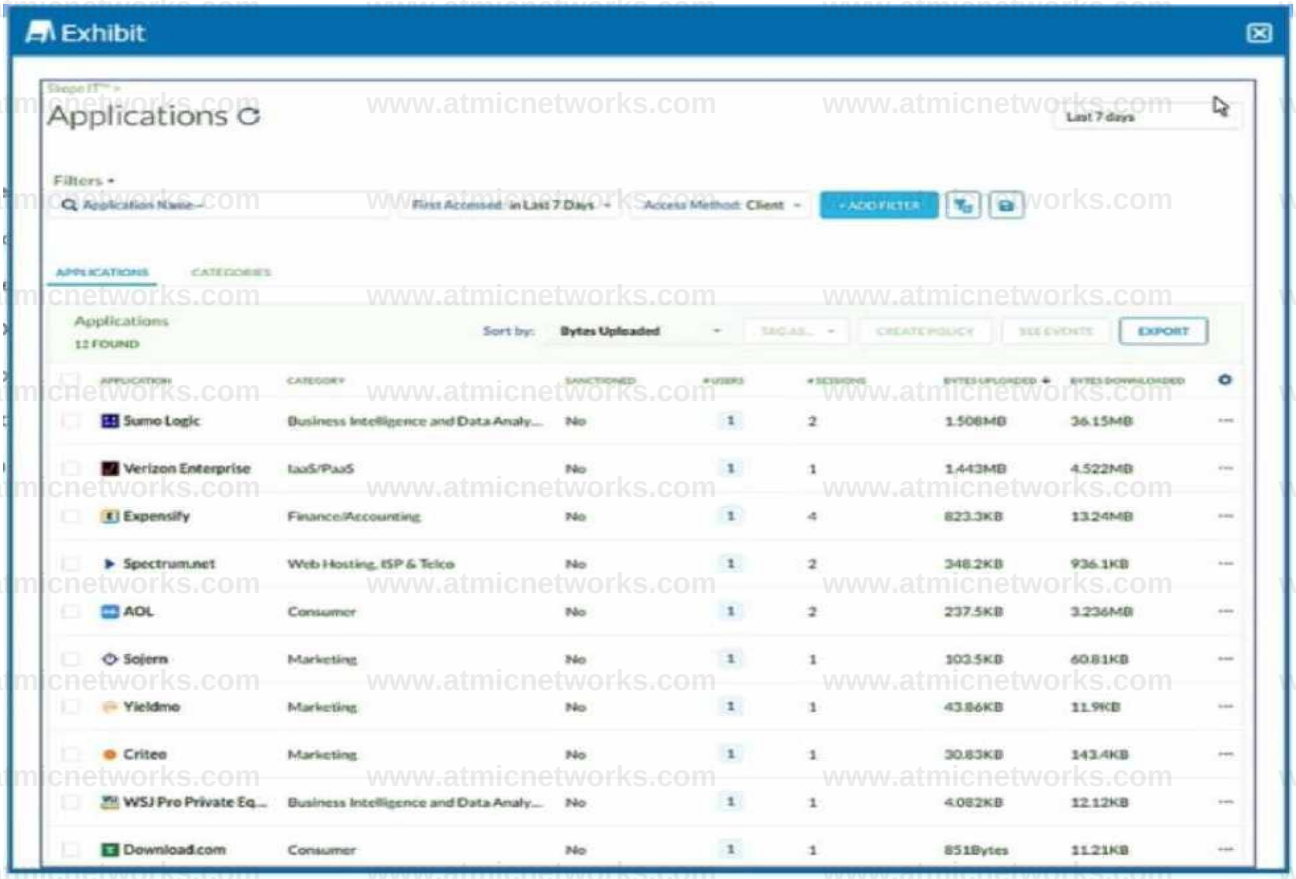
Answer: CD

Explanation:

To deploy Netskope using IPSec tunnels for security in this scenario, two considerations to make a successful connection are C. redundant POPs and D. number of hosts. Redundant POPs are Points of Presence that are geographically distributed data centers that host the Netskope cloud platform. You need to consider redundant POPs to ensure high availability and resiliency of your IPSec tunnels in case of a failure or outage in one of the POPs. You can configure multiple IPSec tunnels from your network to different POPs and use dynamic routing protocols such as BGP to load balance and failover the traffic1. Number of hosts is the number of devices or endpoints that will use the IPSec tunnels to access the cloud services. You need to consider the number of hosts to estimate the bandwidth and throughput requirements of your IPSec tunnels and choose the appropriate POPs that can handle the traffic volume. You can use the Netskope Bandwidth Calculator tool to estimate the bandwidth and throughput based on the number of hosts, locations, and cloud services2. Therefore, options C and D are correct and the other options are incorrect. Reference: IPSec - Netskope Knowledge Portal, Netskope Bandwidth Calculator

Question: 47

Review the exhibit.



You want to discover new cloud applications in use within an organization.

Referring to the exhibit, which three methods would accomplish this task? (Choose three.)

A. Set up API-enabled Protection instances for SaaS applications.

B. Deploy an On-Premises Log Parser (OPLP).

C. Use forward proxy steering methods to direct cloud traffic to Netskope

D. View "All Apps" within the Cloud Confidence Index (CCI) In the Netskope UI.

E. Upload firewall or proxy logs directly into the Netskope platform.

Answer: BCE

Explanation:

To discover new cloud applications in use within an organization, three methods that would accomplish this task are B. Deploy an On-Premises Log Parser (OPLP), C. Use forward proxy steering methods to direct cloud traffic to Netskope, and E. Upload firewall or proxy logs directly into the Netskope platform. An On-Premises Log Parser (OPLP) is a software component that allows you to parse logs from your on-premises firewall or proxy devices and send them to the Netskope cloud for analysis and reporting. You can deploy an OPLP on a Linux server in your network and configure it to connect to your log sources and upload logs periodically or in real time3. A forward proxy steering method is a way of directing your web traffic from your users' devices or browsers to the Netskope cloud for inspection and policy enforcement. You can use forward proxy steering methods such as PAC file, VPN, or inline proxy to steer traffic to Netskope and discover new cloud applications in use4. Uploading firewall or proxy logs directly into the Netskope platform is a way of manually sending logs from your log sources to the Netskope cloud for analysis and reporting. You can upload firewall or proxy logs directly into the Netskope platform by going to SkopeIT > Settings > Log Upload > New Log Upload and selecting the log source type, file format, log file, and time zone5. Therefore, options B, C, and E are correct and the other options are incorrect. Reference: On-Premises Log Parser - Netskope Knowledge Portal, Traffic Steering - Netskope Knowledge Portal, Upload Firewall or Proxy Logs Directly into the Platform - Netskope Knowledge Portal

Question: 48

You notice that your Netskope client icon has a red dot and see "Disabled due to error" when hovering the mouse over the icon. What are two reasons for this message? (Choose two.)

A. The client service is manually stopped.

B. The steering exceptions are incorrect.

C. The client health check has failed.

D. The client traffic is directed over iPsec.

Answer: AC

Explanation:

Two reasons for the message "Disabled due to error" when hovering the mouse over the Netskope client icon are A. The client service is manually stopped and C. The client health check has failed. The client service is a background process that runs the Netskope client on the user's device and communicates with the Netskope cloud. If the client service is manually stopped by the user or by another program, the Netskope client will be disabled and show a red dot on the icon1. The client health check is a feature that monitors the status of the Netskope client and performs self-repair actions if any issues are detected. If the client health check has failed, it means that the Netskope client has encountered a critical error that cannot be fixed automatically, such as corrupted files or registry entries. In this case, the Netskope client will be disabled and show a red dot on the icon2. Therefore, options A and C are correct and the other options are incorrect. Reference: Troubleshooting Netskope Client - Netskope Knowledge Portal, Client Health Check - Netskope

Knowledge Portal

Question: 49

After deploying the Netskope client to a number of devices, users report that the Client status indicates "Admin Disabled". User and gateway information is displayed correctly in the client configuration dialog

Why are clients installing in an "Admin Disabled" state in this scenario?

A. All devices were previously disabled by the administrator.

B. The user's identity is not synchronized to Netskope.

C. The user's password was incorrect during enrollment.

D. The user's account has no mail ID attribute In Active Directory.

Answer: A

Explanation:

The Netskope client can be disabled by the administrator from the Netskope console. This is useful for troubleshooting or maintenance purposes. When the client is disabled by the administrator, it shows the status as “Admin Disabled” and does not apply any policies or steer any traffic. The user cannot enable the client unless the administrator enables it from the console. The other options are not valid reasons for the client to be in an “Admin Disabled” state. Reference: Netskope Client Status 1, Enable or Disable Netskope Client 2

Question: 50

Netskope support advised you to enable DTLS for belter performance. You added firewall rules to allow UDP port 443 traffic. These settings are part of which configuration element when enabled in the Netskope tenant?

A. Real-time Protection policies

B. SSL decryption policies

C. steering configuration

D. client configuration

Answer: D

Explanation:

DTLS (Datagram Transport Layer Security) is a protocol that provides secure communication over UDP. It is an option that can be enabled in the client configuration settings in the Netskope tenant. Enabling DTLS can improve the performance of the Netskope client, especially in high latency or packet loss scenarios. DTLS is not related to Real-time Protection policies, SSL decryption policies, or steering configuration, which are different configuration elements in the Netskope tenant. Reference: Client Configuration Settings 3, Netskope Client Performance 4

Question: 51

You are comparing the behavior of Netskope's Real-time Protection policies to API Data Protection policies. In this Instance, which statement is correct?

A. All real-time policies are enforced, regardless of sequential order, while API policies are analyzed sequentially from top to bottom and stop once a policy Is matched.

B. Both real-time and API policies are analyzed sequentially from top to bottom and stop once a policy Is matched.

C. All API policies are enforced, regardless of sequential order, while real-time policies are analyzed sequentially from top to bottom and stop once a policy Is matched.

D. Both real-time and API policies are all enforced, regardless of sequential order.

Answer: C

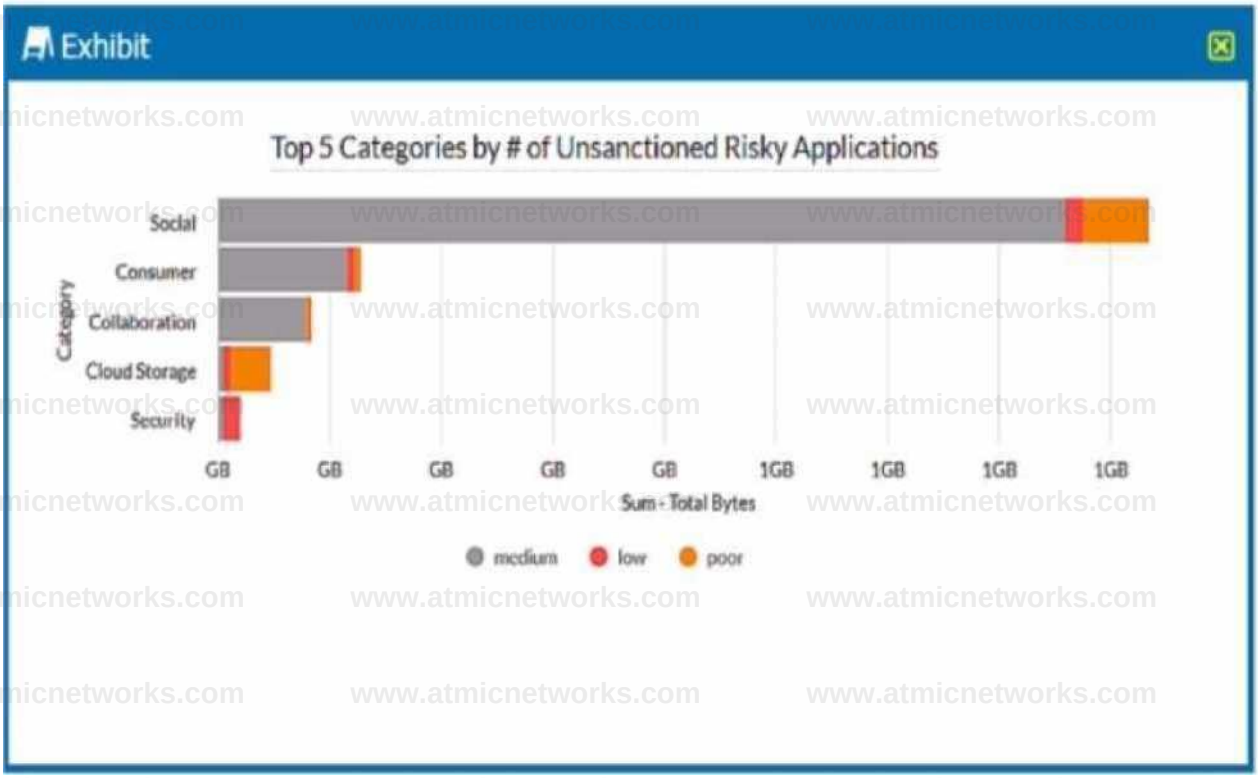
Explanation:

Netskope's Real-time Protection policies and API Data Protection policies have different ways of applying actions based on the policy order. Real-time Protection policies are analyzed sequentially from top to bottom and stop once a policy is matched. This means that only one policy action is applied per transaction. API Data Protection policies are all enforced, regardless of sequential order. This means that multiple policy actions can be applied per file or email. Therefore, the correct statement is that all API policies are enforced, regardless of sequential order, while real-time policies are analyzed

sequentially from top to bottom and stop once a policy is matched. Reference: Real[time Protection Policies1, API Data Protection Policies2]

Question: 52

Review the exhibit.



A security analyst needs to create a report to view the top five categories of unsanctioned applications accessed in the last 90 days. Referring to the exhibit, what are two data collections in Advanced Analytics that would be used to create this report? (Choose two.)

A. Alerts

B. Application Events

C. Page Events

D. Network Events

Answer: BD

Explanation:

To create a report to view the top five categories of unsanctioned applications accessed in the last 90 days, the security analyst would need to use two data collections in Advanced Analytics: Application Events and Network Events. Application Events provide information about the cloud applications and websites accessed by users, such as app name, app category, app risk score, app instance, app version, and more. Network Events provide information about the network traffic generated by users, such as source IP, destination IP, protocol, port, bytes sent, bytes received, and more. By combining these two data collections, the security analyst can filter the events by app category, app risk score, and time range to create a report that shows the top five categories of unsanctioned applications accessed in the last 90 days. Alerts and Page Events are not relevant for this report. Alerts provide information about the alerts triggered by Real-time Protection or API Data Protection policies, such as alert type, alert severity, alert status, alert description, and more. Page Events provide information about the web pages visited by users, such as page title, page URL, page category, page risk score, page content type, and more. Reference: Advanced Analytics

Question: 53

You want to provision users and groups to a Netskope tenant. You have Microsoft Active Directory servers hosted in two different forests. Which statement is true about this scenario?

A. You can use the Netskope Adapter Tool for user provisioning.

B. You can use the Netskope virtual appliance for user provisioning

C. You cannot provision users until you migrate to Azure AD or Okta.

D. You can use SCIM version 2 for user provisioning.

Answer: D

Explanation:

You can use SCIM version 2 for user provisioning in this scenario. SCIM (System for Cross-domain Identity Management) is a standard protocol for exchanging identity information across different cloud applications. Netskope supports SCIM version 2 and can integrate with identity providers (IdPs) that follow the same standard, such as Microsoft Azure AD, Okta, OneLogin, and Ping Identity. You can use SCIM to provision users and groups from multiple Active Directory forests to a Netskope tenant. The other options are not valid for this scenario. The Netskope Adapter Tool and the Netskope virtual appliance are used for user identification, not provisioning. They can only connect to one Active Directory forest at a time. You do not need to migrate to Azure AD or Okta to provision users, as Netskope supports other IdPs that use SCIM as well. Reference: Provisioning Users for Netskope Client1, SCIM Integration2

Question: 54

Your customer has some managed Windows-based endpoints where they cannot add any clients or agents. For their users to have secure access to their SaaS application, you suggest that the customer use Netskope's Explicit Proxy.

Which two configurations are supported for this use case? (Choose two.)

A. Endpoints can be configured to directly use the Netskope proxy.

B. Endpoints must have separate steering configurations in the tenant settings.

C. Endpoints must be configured in the device section of the tenant to interoperate with all proxies.

D. Endpoints can be configured to use a Proxy Auto Configuration (PAC) file.

Answer: AD

Explanation:

For the use case of managed Windows-based endpoints where no clients or agents can be added, you can suggest that the customer use Netskope's Explicit Proxy. Explicit Proxy is a method for steering traffic from any device to the Netskope Cloud using a proxy server. There are two supported configurations for this use case: Endpoints can be configured to directly use the Netskope proxy by setting the proxy settings in the browser or the operating system to point to the explicit proxy destination provided by Netskope. Endpoints can be configured to use a Proxy Auto Configuration (PAC) file by downloading a PAC file template from Netskope and modifying it according to the customer's needs. The PAC file can be hosted on-premises or on the cloud and distributed to the endpoints. The other options are not valid for this use case. Endpoints do not need separate steering configurations in the tenant settings, as they can use the same explicit proxy destination and port. Endpoints do not need to be configured in the device section of the tenant to interoperate with all proxies, as this is only required for reverse proxy mode. Reference: Explicit Proxy3, [Explicit Proxy over IPSec and GRE Tunnels]

Question: 55

You are using the Netskope DLP solution. You notice flies containing test data for credit cards are not triggering DLP events when uploaded to Dropbox. There are corresponding page events. Which two scenarios would cause this behavior? (Choose two.)

A. The Netskope client Is not steering Dropbox traffic.

B. The DLP rule has the severity threshold set to a value higher than the number of occurrences.

C. The credit card numbers in your test data are Invalid 16-dlglt numbers.

D. There is no API protection configured for Dropbox.

Answer: BC

Explanation:

There are two possible scenarios that would cause the behavior of files containing test data for credit cards not triggering DLP events when uploaded to Dropbox. One scenario is that the DLP rule has the severity threshold set to a value higher than the number of occurrences. This means that the rule will only trigger an event if the number of matches for the sensitive data exceeds the specified threshold. For example, if the rule has a severity threshold of 10 and the file contains only 5 credit card numbers, then no event will be generated. To fix this, you can lower the severity threshold or remove it altogether. The other scenario is that the credit card numbers in your test data are invalid 16-digit numbers. This means that the numbers do not pass the Luhn algorithm check, which is a validation method used by Netskope DLP to detect valid credit card numbers. For example, if the number is 1234-5678-9012-3456, then it is not a valid credit card number and will not be detected by Netskope DLP. To fix this, you can use valid test credit card numbers that pass the Luhn algorithm check. The other options are not valid scenarios for this behavior. The Netskope client is not steering Dropbox traffic is not a valid scenario because there are corresponding page events, which means that the traffic is being steered to Netskope. There is no API protection configured for Dropbox is not a valid scenario because API protection is not required for DLP detection on file uploads, which are handled by real-time protection. Reference: DLP Rule Settings1, Credit Card Number Detection2

Question: 56

Review the exhibit.

You want to create a custom URL category to apply a secure Web gateway policy combining your own list of URLs and Netskope predefined categories.

In this scenario, which task must be completed?

A. Add the URL list to the Client configuration.

B. Add the URL list to a Custom category.

C. Add the URL list to a Steering configuration.

D. Add the URL list to a Real-time Protection policy.

Answer: B

Explanation:

In order to create a custom URL category to apply a secure Web gateway policy combining your own list of URLs and Netskope predefined categories, you must add the URL list to a Custom category. This is because Netskope allows you to create custom categories that can be used in policies to block or allow access to specific URLs. You can also include or exclude predefined categories and other URL lists in your custom category. To create a custom category, you need to go to Policies > Web > Custom Categories and click New Custom Category. Then you can select the predefined categories and URL

lists that you want to include or exclude in your custom category. You also need to give your custom category a name and save it. After creating a custom category, you can apply it to a Real-time Protection policy by selecting it from the Categories dropdown. The other options are not valid tasks for creating a custom URL category. You do not need to add the URL list to the Client configuration, as this is only required for client-side steering methods. You do not need to add the URL list to a Steering configuration, as this is only required for network-side steering methods. You do not need to add the URL list to a Real-time Protection policy directly, as this will not allow you to combine it with predefined categories. Reference: Custom Category3, Create Custom Categories

Question: 57

You want to reduce false positives by only triggering policies when contents of your customer database are uploaded to Dropbox. Your maximum database size is 2 MB. In this scenario, what are two ways to accomplish this task? (Choose two.)

A. Upload the .csv export lo the Netskope tenant DLP rules section to create an exact match hash.

B. Use the Netskope client to upload the .csv export to the Netskope management plane DLP container.

C. Send the .csv export to Netskope using a support ticket with the subject, "create exact match hash".

D. Use a Netskope virtual appliance to create an exact match hash.

Answer: AD

Explanation:

To reduce false positives by only triggering policies when contents of your customer database are uploaded to Dropbox, you can use two methods: Upload the .csv export to the Netskope tenant DLP rules section to create an exact match hash. This is a method that allows you to upload a file containing structured data, such as a customer database, to the Netskope tenant and generate a hash of the data. The hash is then used to match the data in the cloud traffic and trigger DLP policies. This method is suitable for files that are less than 10 MB in size. To upload the file, you need to go to Policies > Data Protection > DLP Rules and click on Exact Match Hashes. Then you can select the file from your local system and upload it. Use a Netskope virtual appliance to create an exact match hash. This is a method that allows you to create a file containing structured data, such as a customer
database, and upload it to the Netskope cloud using a virtual appliance. The virtual appliance encrypts the file before uploading it and generates a hash of the data. The hash is then used to match the data in the cloud traffic and trigger DLP policies. This method is suitable for files that are larger than 10 MB in size. To create the file, you need to follow a specific format and save it as a .csv file. To upload the file, you need to use the request dlp-pdd upload command on the virtual appliance CLI. The other options are not valid methods for this task. You cannot use the Netskope client to upload the .csv export to the Netskope management plane DLP container, as this is not a supported feature of the client. You cannot send the .csv export to Netskope using a support ticket with the subject, “create exact match hash”, as this is not a secure or efficient way of creating an exact match hash. Reference: Create an Exact Match Hash from the UI1, Create an Exact Match Hash from a Virtual Appliance2

Question: 58

Your company has a Symantec BlueCoat proxy on-premises and you want to deploy Netskope using proxy chaining. Which two prerequisites need to be enabled first in this scenario? (Choose two.)

A. Disable SSL decryption.

B. Disable the X-Authenticated-User header.

C. Enable SSL decryption.

D. Enable the X-Forwarded-For HTTP header

Answer: CD

Explanation:

To deploy Netskope using proxy chaining with Symantec BlueCoat proxy on-premises, you need to enable two prerequisites first: Enable SSL decryption on your Symantec BlueCoat proxy. This is required for proxy chaining because Netskope needs to inspect the SSL traffic that is sent from your proxy to the Netskope cloud. To enable SSL decryption, you need to configure your Symantec BlueCoat proxy to trust the Netskope certificate for SSL interception. You can download the certificate from Settings > Manage > Certificates > Signing CA in the Netskope UI. Enable the X- Forwarded-For HTTP header on your Symantec BlueCoat proxy. This is required for proxy chaining because Netskope needs to identify the original source IP address of the user behind your proxy. The X-Forwarded-For header is used to pass this information from your proxy to Netskope. To enable this header, you need to configure your Symantec BlueCoat proxy to send X-Forwarded-For HTTP header for all HTTP requests. The other options are not valid prerequisites for this scenario. You do not need to disable SSL decryption on your Symantec BlueCoat proxy, as this would prevent Netskope from inspecting the SSL traffic. You do not need to disable the X-Authenticated-User header on your Symantec BlueCoat proxy, as this is an optional header that can be used to pass additional user information from your proxy to Netskope.
Reference: Proxy Chaining3, Configure Forcepoint for Proxy Chaining

Question: 59

Review the exhibit.

B Exhibit

Dashboard Enterprise applications > Netskope Cam Appt
V Over*#*

(D Decrement Plan

Manage

Q| Properties

A Ormers

Ai Roes aid adrnrnrstiatori (Prene*)

* Users and groups

3 Single s^n on

£ Provisioning

B Appl<abon praey

Current cycle status

incremental cycle slopped

complete

Vie* prov-wonng logs

Manage provisioning

Update credentials Ida

attribute mapprgt Add

U'Opanq film

Statistics to date

v View provisioning deUSs OX

v Ve* techrucai Information

What is the purpose of the configuration page shown Ii the exhibit?

A. to provision a Netskope client using SCCM

B. to allow users to authenticate against the proxy

C. to onboard Active Directory users to a Netskope tenant

D. to enforce administrative role-based access

Answer: C

Explanation:

The configuration page shown in the exhibit is used to onboard Active Directory users to a Netskope tenant. This is done by configuring the Active Directory settings in the Netskope platform and then importing the users from Active Directory. The configuration page allows you to specify the following parameters:

Directory Service: The type of directory service that you are using, such as Active Directory or LDAP.

Domain Name: The name of your Active Directory domain, such as example.com.

Domain Controller: The IP address or hostname of your Active Directory domain controller, such as dc1.example.com.

Username: The username of an account that has read access to your Active Directory, such as administrator@example.com.

Password: The password of the account that has read access to your Active Directory.

Base DN: The base distinguished name of the container or organizational unit that contains the users and groups that you want to import, such as OU=Users,DC=example,DC=com.

User Filter: The LDAP filter that defines the criteria for selecting the users that you want to import, such as (objectClass=user).

Group Filter: The LDAP filter that defines the criteria for selecting the groups that you want to import, such as (objectClass=group).

After configuring these parameters, you can click on Test Connection to verify that the connection to your Active Directory is successful. Then you can click on Import Users to start importing the users and groups from your Active Directory to your Netskope tenant.

Reference: Onboarding Active Directory Users to a Netskope Tenant1

Question: 60

You want to allow both the user identities and groups to be imported in the Netskope platform. Which two methods would satisfy this requirement? (Choose two.)

A. Use System for Cross-domain Identity Management (SCIM).

B. Use Manual Entries.

C. Use Directory Importer.

D. Use Bulk Upload with a CSV file.

Answer: AD

Explanation:

To allow both the user identities and groups to be imported in the Netskope platform, you can use either the System for Cross-domain Identity Management (SCIM) method or the Bulk Upload with a CSV file method. Both of these methods allow for the import of user identities and groups from different identity providers (IdPs) that support SCIM or CSV formats. The SCIM method is recommended for large-scale deployments, as it automates the exchange of user identity information across apps for user provisioning. The CSV method is recommended for small-scale deployments, as it allows for manual upload of user details in a comma-separated values file. The other methods are not suitable for this requirement. The Manual Entries method does not allow for the import of groups, only user emails. The Directory Importer method does not import users and groups directly into the Netskope platform, but rather connects to an Active Directory or LDAP server and periodically fetches user and group information.

Reference: Provisioning Users for Netskope Client2, SCIM Integration3, Bulk Upload via CSV file

Question: 61

Your customer has deployed the Netskope client to secure their Web traffic. Recently, they have enabled Cloud Firewall (CFW) to secure all outbound traffic for their endpoints. Through a recent

acquisition, they must secure all outbound traffic at several remote offices where they have access to the local security stack (routers and firewalls). They cannot install the Netskope client.

A. They can configure Reverse Proxy integrated with their IdP.
B. They can deploy Netskope's DPOP to steer the targeted traffic to the Netskope Security Cloud.
C. They can use IPsec and GRE tunnels with Cloud Firewall.
D. They can secure the targeted outbound traffic using Netskope's Cloud Threat Exchange (CTE).

Answer: C

Explanation:

The correct solution is to use IPsec and GRE tunnels with Cloud Firewall. Netskope Cloud Firewall supports secure tunneling methods such as IPsec and GRE, enabling companies to steer traffic to the Netskope Security Cloud without requiring the Netskope client. This is particularly useful when endpoint installation of the client is not feasible, such as in remote offices where network infrastructure like routers and firewalls are available.

Question: 62

You are using Skope IT to analyze and correlate a security incident. You are seeing too many events generated by API policies. You want to filter for logs generated by the Netskope client only.

A. Use the access_method filter and select Client from the dropdown menu.
B. Use the access_method filter and select Tunnel from the dropdown menu.
C. Use the access_method filter and select Logs from the dropdown menu.
D. Use query mode and use access_method neq Client.

Answer: A

Explanation:

To filter for logs specifically generated by the Netskope client, select "Client" from the access_method filter dropdown menu in Skope IT. This filter allows administrators to narrow down logs by access method, making it easier to troubleshoot issues related only to the Netskope client.

Question: 63

You are troubleshooting private application access from a user's computer. The user is complaining that they cannot access the corporate file share; however, the private tunnel seems to be established. You open the npadebuglog.log file in a text editor and cannot find any reference to the private application.

A. The absence of npadebuglog.log entries is not significant.
B. File shares cannot be published using private access.
C. The user is not added to the required real-time policy.
D. The user needs to re-authenticate for private applications.

Answer: C

Explanation:

If there are no references to the private application in the npadebuglog.log, it is likely that the user is not added to the required real-time policy. Without proper policy assignment, the user's traffic will not be routed correctly through the private access setup, causing access issues.

Question: 64

You discover the ongoing use of the native Dropbox client in your organization. Although Dropbox is not a corporate-approved application, you do not want to prevent the use of Dropbox. You do, however, want to ensure visibility into its usage.

A. Change Windows and Mac steering exception actions to use Tunnel mode and set Netskope as the source IP address for SSO services.
B. Modify the existing tenant steering exception configuration to block the Dropbox native application to force users to use the Dropbox website.

C. Remove all Dropbox entries from the tenant steering SSL configuration entirely.

D. Create a new tenant steering exception type of Destination Locations that contains the Dropbox application.

Answer: D

Explanation:

To allow the usage of Dropbox while maintaining visibility, create a new tenant steering exception of type "Destination Locations" for Dropbox. This will enable traffic visibility for Dropbox while avoiding a block, as requested.

Question: 65

Your company wants to deploy Netskope using a tunnel because you have a mixture of device operating systems. You also do not want to enable encryption because you want to maximize bandwidth.

A. explicit proxy

B. IPsec

C. proxy chaining

D. GRE

Answer: D

Explanation:

GRE tunnels are the optimal choice in this scenario. GRE is a commonly used, non-encrypted tunneling protocol that supports a variety of device operating systems, and it offers efficient bandwidth usage without encryption overhead, which aligns with the company's requirements.

Question: 66

Your company wants to know if there has been any unusual user activity. In the UI, you go to Skope IT

-> Alerts.

Which two types of alerts would you filter to find this information? (Choose two.)

A. Alert type = uba
B. Alert type = anomaly
C. Alert type = malware
D. Alert type = policy

Answer: AB

Explanation:

To identify unusual user activity, filter alerts by "uba" (User Behavior Analytics) and "anomaly." UBA and anomaly alerts highlight deviations from typical user behavior, which are indicators of unusual or potentially risky activities.

Question: 67

You want the ability to perform automated remediation of misconfigurations on GitHub, Microsoft 365, Salesforce, ServiceNow, and Zoom.

A. Netskope Infrastructure as a Service
B. Netskope Remote Browser Isolation
C. Netskope Cloud Firewall
D. Netskope SaaS Security Posture Management

Answer: D

Explanation:

Netskope SaaS Security Posture Management (SSPM) is designed to automate the detection and remediation of security misconfigurations across SaaS applications, including GitHub, Microsoft 365, Salesforce, ServiceNow, and Zoom. SSPM provides visibility into and correction of misconfigurations to protect corporate data in cloud applications.

Question: 68

Review the exhibit.

add log-upload syslogng parserconfig set log-upload syslogng parserconfig 0

logsource <log-source>

You are asked to deploy a virtual appliance OPLP to accept syslog messages directly from the enterprise Palo Alto Networks firewall. You believe that you have configured the OPLP to accept the firewall logs, yet they are not appearing in Risk Insights. Referring to the exhibit, which parser name would be required to complete the new configuration?

A. panw-syslog
B. sfwder
C. custom-csv
D. squid

Answer: A

Explanation:
The correct parser name to process syslog messages from Palo Alto Networks firewalls is "panw- syslog." Using the appropriate parser ensures that the logs are correctly interpreted and ingested by Netskope, making them available in Risk Insights.

Question: 69

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.

Answer: D

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: 70

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.

Answer: A

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: 71

You created the Netskope application in your IdP for user provisioning and validated that the API Integration settings are correct and functional. However, you are not able to push the user groups from the IdP into your Netskope tenant.

A. The IdP group contains active users, as well as one or more deactivated users.

B. The IdP does not have Create User permissions.
C. You do not have enough users assigned to the IdP group.
D. You failed to push the IdP users before attempting to push the IdP groups.

Answer: A

Explanation:
If user groups cannot be pushed from the IdP into Netskope, one possible cause is that the group contains both active and deactivated users. Deactivated users in a group can create conflicts during provisioning, as Netskope expects all users in the group to be active.

Question: 72

Your IT organization is migrating its user directory services from Microsoft Active Directory to a cloudbased Identity Provider (IdP) solution, Azure AD. You are asked to adapt the Netskope user provisioning process to work with this new cloud-based IdP.

A. Directory Importer
B. Microsoft GPO
C. SCIMApp
D. Manual Import

Answer: C

Explanation:
The SCIMApp integration is the best choice for Azure AD as it allows for seamless user provisioning between cloud-based IdPs and Netskope. SCIM (System for Cross-domain Identity Management) is a standard for automating user provisioning and works effectively with cloud IdPs like Azure AD.

Question: 73

Your team is asked to investigate ten Netskope DLP incidents. You want to assign these incidents among different team members.

A. Use your ticketing tool.

B. Use the Forensic Incident workflow.

C. Use the DLP Incident workflow.

D. Use the Quarantine Incident workflow.

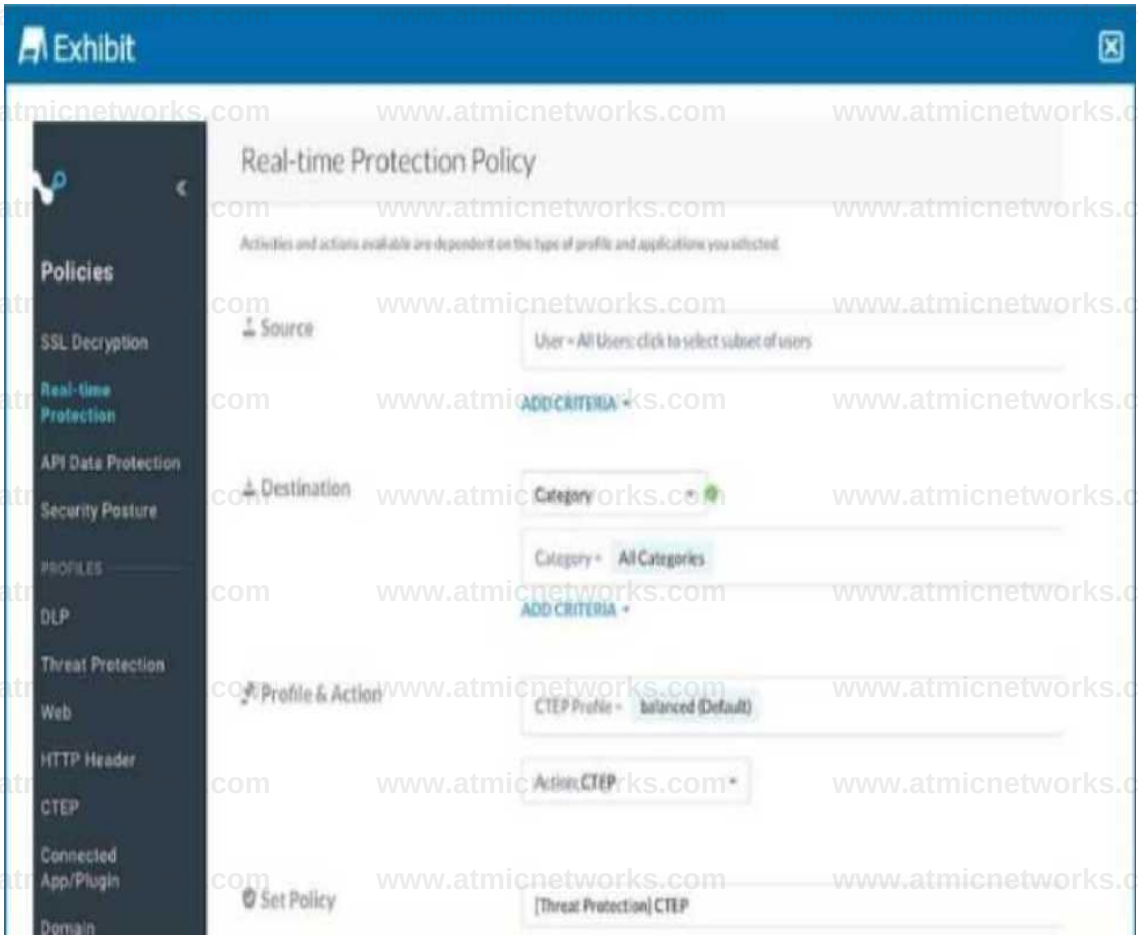
Answer: C

Explanation:

The DLP Incident workflow in Netskope is specifically designed for managing and investigating DLP incidents. This workflow allows incidents to be assigned to team members, facilitating efficient investigation and resolution of data loss concerns.

Question: 74

Review the exhibit.



Your Real-time Protection policy contains some rules with only a browse activity. The exhibit shows a new policy rule.

Where is the correct location to place this rule?

A. at the bottom
B. before browse activity
C. after browse activity
D. at the top

Answer: D

Explanation:

The correct practice is to place high-priority rules, such as those with specific scanning actions, at the top of the Real-time Protection policy rule list. Placing the rule at the top ensures it is applied before other less restrictive rules, like those configured only for browsing activities.

Question: 75

You are testing policies using the DLP predefined identifier "Card Numbers (Major Networks; all)." No DLP policy hits are observed.

A. You must use Netskope API protection.
B. Your data must have valid credit card numbers.
C. You must normalize credit card numbers to 16-digit consecutive numbers.
D. You must use the Netskope client to perform advanced DLP and optical character recognition.

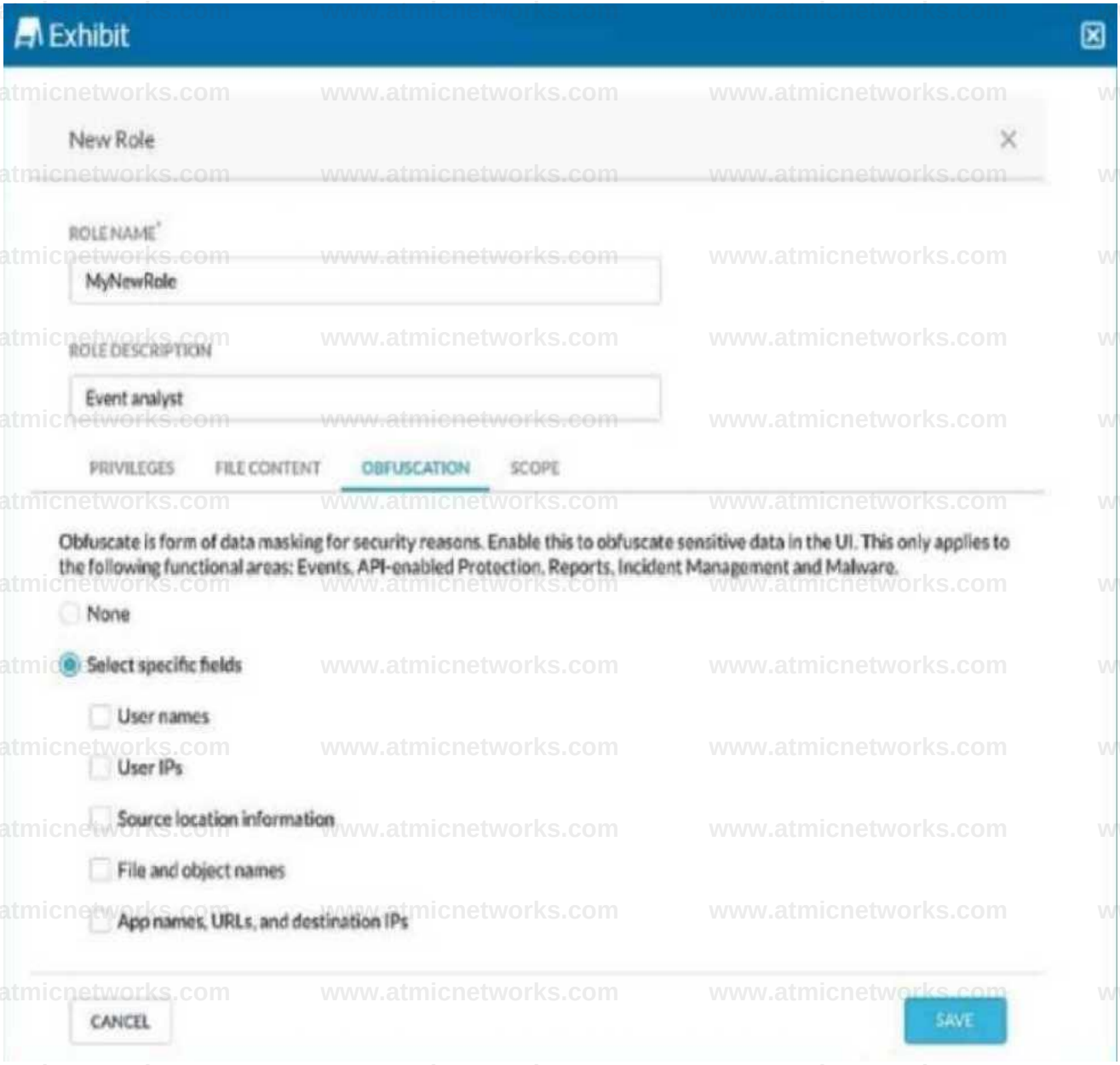
Answer: B

Explanation:

For DLP policies to detect sensitive data like credit card numbers, the data must contain valid credit card numbers as defined by the DLP pattern. Invalid or incorrectly formatted numbers will not trigger DLP policy hits.

Question: 76

Review the exhibit.



You are asked to create a new role that allows analysts to view Events and Reports while providing user privacy. You need to avoid directly exposing identities and user location information.
Which three fields must you obfuscate in this scenario? (Choose three.)

A. User IPs
B. User names
C. App names, URLs, and destination IPs
D. File and object names
E. Source location information

Answer: ABE

Explanation:

To ensure user privacy in the Events and Reports view, obfuscate sensitive information like User IPs, User names, and Source location information. This helps protect identities and prevent location tracking of users while allowing visibility into activity details.

Question: 77

Your company is using on-premises QRadar as a SIEM solution. They are replacing it with Rapid7 in the cloud. The legacy on-premises QRadar will eventually be decommissioned. Your IT department does not want to use the same token that QRadar uses.

A. Netskope does not support multiple REST API tokens.
B. You must use Netskope REST API v1 to support multiple tokens to share events.
C. You must use Netskope REST API v2 to support multiple tokens to share events.
D. You must use an Advanced Threat Protection license to support multiple tokens to share events.

Answer: C

Explanation:

Netskope REST API v2 supports multiple tokens, allowing different applications or integrations (like QRadar and Rapid7) to have distinct tokens. This avoids token conflicts and enhances security by isolating access permissions for different SIEM systems.

Question: 78

You are deploying a Netskope client in your corporate office network. You are aware of firewall or proxy rules that need to be modified to allow traffic.

Which two statements are true in this scenario? (Choose two.)

A. You need to allow TLS 1.1 traffic to pass through the firewalls from the users' IP to all destinations.
B. You must enable SSL decryption in the proxy to inspect the Netskope tunnel.
C. It is recommended to allow UDP port 443 to the Netskope IP ranges to allow DTLS.

D. You need to allow TCP port 443 to the Netskope IP ranges or domains.

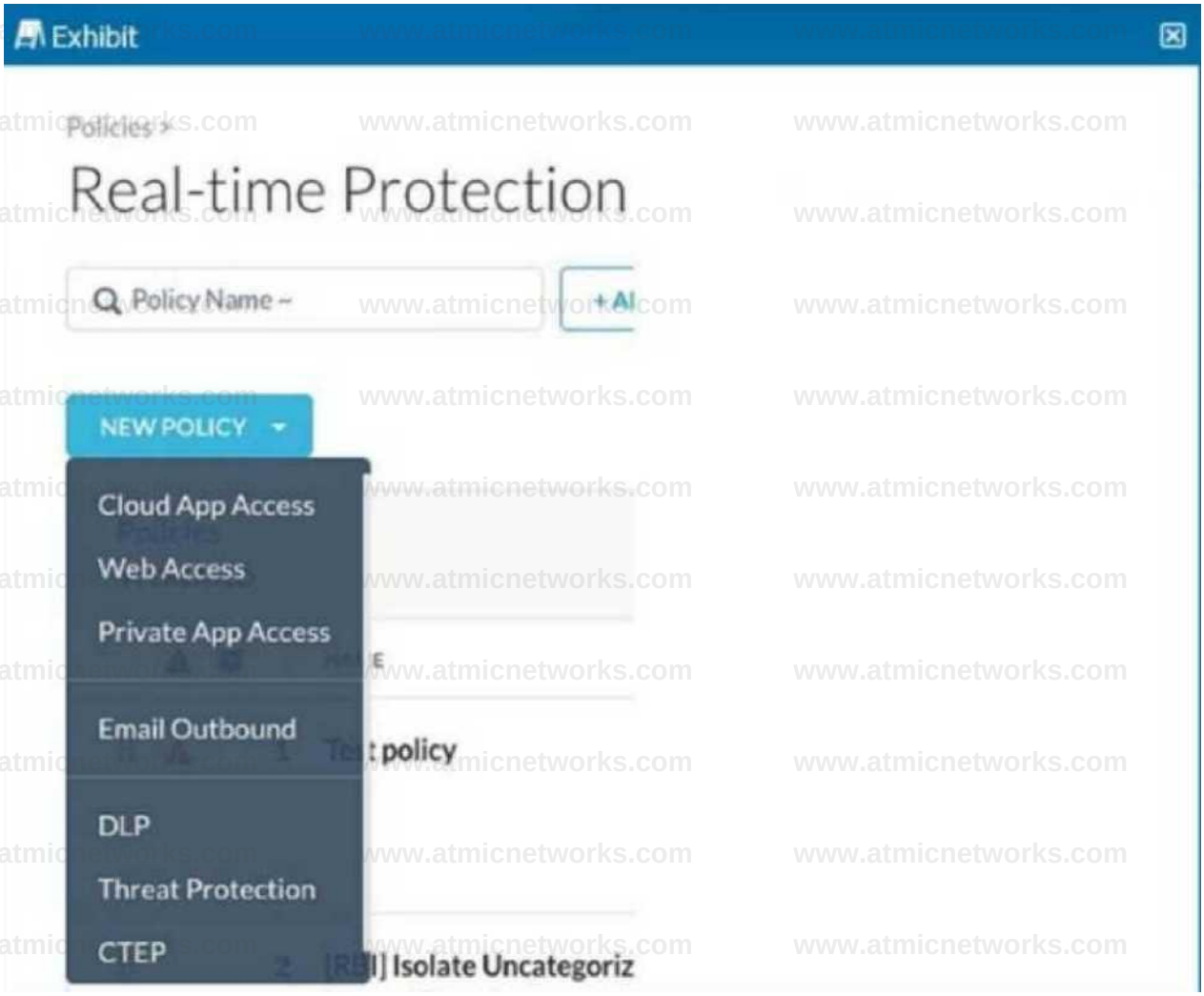
Answer: CD

Explanation:

Allowing UDP port 443 is recommended to support DTLS, which enhances performance over the Netskope tunnel. TCP port 443 must also be allowed as it is essential for secure HTTPS connections used by Netskope services.

Question: 79

Review the exhibit.



You are asked to create a new Real-time Protection policy to scan SMTP emails using data loss prevention (DLP) for personal health information (PHI). The scope is limited to only emails being sent from Microsoft Exchange Online to outside recipients.

A. Web Access policy
B. Email Outbound policy
C. CTEP policy
D. DLP policy

Answer: B

Explanation:

An "Email Outbound" policy is specifically designed to apply data loss prevention controls on outbound emails, such as SMTP traffic from Exchange Online. This policy type enables granular control over outbound email content, ensuring compliance with DLP policies for PHI data.

Question: 80

Your company asks you to use Netskope to integrate with Endpoint Detection and Response (EDR) vendors such as Crowdstrike.

Which two requirements are needed for a successful integration and sharing of threat data? (Choose two.)

A. Remediation profile
B. Device classification
C. API Client ID
D. Custom log parser

Answer: AC

Explanation:

Integrating with EDR vendors like Crowdstrike requires an API Client ID for authentication and data sharing. A remediation profile is also necessary to define automated actions that can be taken when threats are detected, ensuring effective response to endpoint threats.

Question: 81

Your customer is using a virtual desktop infrastructure (VDI) for their support engineers. Multiple users will be logging into the same device, and they want to detect activities for each user.

A. Install Netskope client in default mode and enable DTLS.
B. Install Netskope client and create a separate steering configuration for each user.
C. Install Netskope client in peruserconfig mode.
D. Install Netskope client and create a separate device configuration for each user.

Answer: C

Explanation:

Installing the Netskope client in "peruserconfig" mode allows for user-specific configurations on shared devices like those in a VDI environment. This mode enables Netskope to detect and report activities separately for each user, even if multiple users are logged into the same device.

Question: 82

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

Answer: A

Explanation:
Deploying the Netskope client on remote and traveling users' devices provides the highest level of visibility into their activities regardless of their location. The Netskope client can steer traffic securely to the Netskope Security Cloud, offering consistent monitoring and protection.

Question: 83

You want to prevent a document stored in Google Drive from being shared externally with a public link.

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

Answer: C

Explanation:
An API Data Protection policy is appropriate for controlling document sharing permissions in Google Drive. This policy type can enforce restrictions on file sharing, such as preventing public links, which ensures data protection within cloud storage applications.

Question: 84

A company allows their users to access OneDrive on their managed laptops. It is against corporate policy to upload any documents to their personal OneDrive. The company needs to enforce this policy to protect their customer's sensitive data.
What are two ways to enforce this policy? (Choose two.)

A. Create DLP policies to block the upload of all the identified documents.

B. Create DLP policies to allow document uploading only to the corporate OneDrive instance.

C. Create a new application instance for the corporate OneDrive.

D. Fingerprint all the documents to have a catalog of all the documents that the company needs to protect.

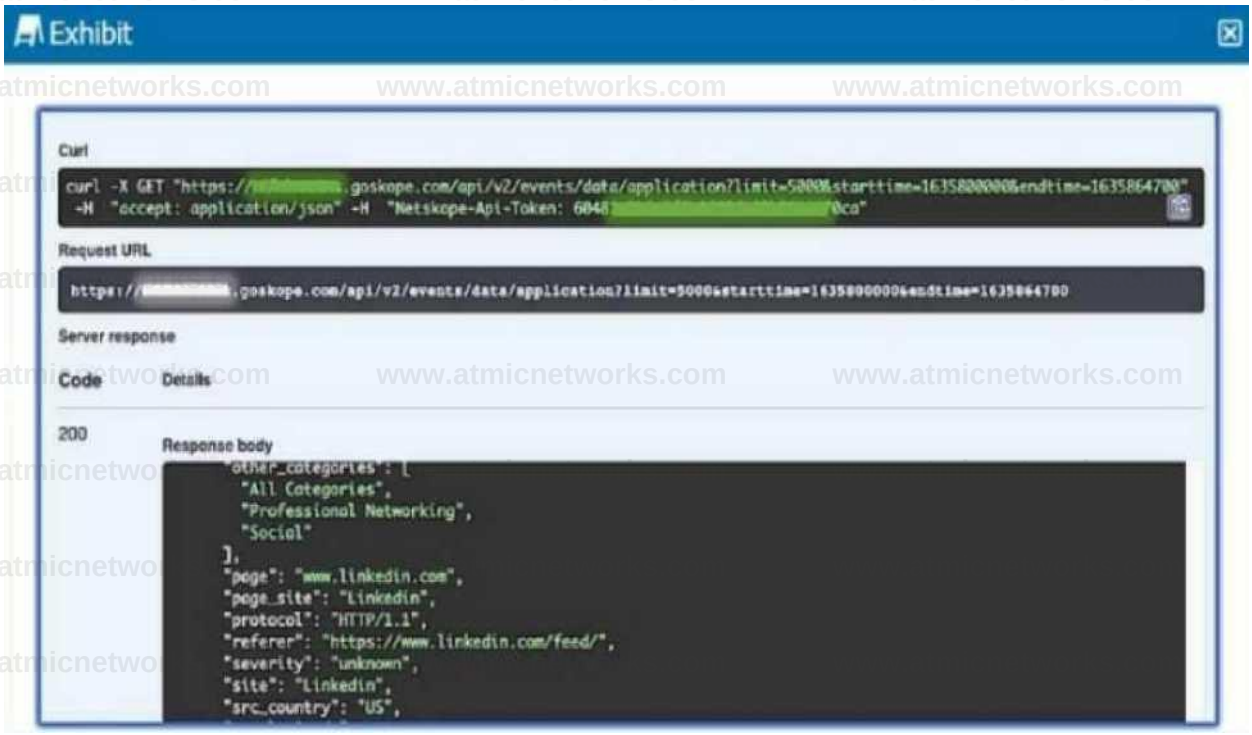
Answer: AB

Explanation:

By setting DLP policies that either block uploads of sensitive documents or restrict them to only the corporate OneDrive, the company can enforce its policy. These policies ensure that sensitive data remains within approved environments and does not get uploaded to personal instances.

Question: 85

Review the exhibit.



Referring to the exhibit, which three statements are correct? (Choose three.)

A. The request was processed successfully.
B. A request was submitted to extract application event details.
C. An invalid token was used.
D. The request was limited to the first 5000 records.
E. The request was confined to only the "Professional Networking and Social" category.

Answer: ABD

Explanation:

The "200" response code confirms that the request was processed successfully. The request URL indicates that it was set to retrieve application event data with a limit of 5000 records. Additionally, the response includes categories such as "Professional Networking and Social," verifying that these were part of the requested data.

Question: 86

You use Netskope to provide a default Malware Scan profile for use with your malware policies. Also, you want to create a custom malware detection profile.
In this scenario, what are two additional requirements to complete this task? (Choose two.)

A. Add a custom hash list as an allowlist.
B. Add a quarantine profile.
C. Add a remediation profile.
D. Add a custom hash list as a blocklist.

Answer: BD

Explanation:

To create a custom malware detection profile, adding a quarantine profile ensures that detected threats are appropriately isolated. Additionally, a custom hash list as a blocklist allows you to block specific known malware hashes, further enhancing the customization of the malware detection profile.

Question: 87

You want to provide malware protection for all cloud storage applications.
In this scenario, which action would accomplish this task?

A. Create a real-time threat protection policy with a category of Cloud Storage.
B. Apply a data protection profile.
C. Apply a CTEP profile.
D. Create an API threat protection policy with a category of Cloud Storage.

Answer: A

Explanation:
Creating a real-time threat protection policy specifically targeting the "Cloud Storage" category ensures that all supported cloud storage applications are covered by malware protection. This approach allows real-time scanning and response to malware threats within cloud storage environments.

Question: 88

With Netskope DLP, which feature would be used to detect keywords such as "Confidential" or "Access key"?

A. Regular Expression
B. Exact Match
C. Fingerprint Classification
D. Dictionary

Answer: D

Explanation:
The Dictionary feature in Netskope DLP is designed to detect specific keywords or phrases, such as "Confidential" or "Access key." By using a pre-defined list of sensitive terms, the Dictionary feature enables policy enforcement based on the presence of these keywords in data.

Question: 89

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

Answer: BD

Explanation:

Placing high-risk block policies at the top ensures that critical blocks are enforced first, protecting against the most severe threats. Additionally, an "allow all" Web Access policy at the bottom is not necessary, as policy defaults can handle remaining traffic not explicitly addressed by other rules.

Question: 90

You have created a specific Skope IT application events query and want to have the query automatically run and display the results every time you log into your tenant.

Which two statements are correct in this scenario? (Choose two.)

A. Add the Watchlist widget from the library to your home page.
B. Export a custom Skope IT watchlist to a report and then schedule it to run daily.
C. Save a custom Skope IT watchlist, then manage filters and share with others.
D. Add your Skope IT query to a custom watchlist.

Answer: CD

Explanation:

Adding a Skope IT query to a custom watchlist allows the query to be saved and easily accessed.

Saving the watchlist and managing filters also lets you customize it further and share it with others in your organization if needed.

Question: 91

You are configuring GRE tunnels from a Palo Alto Networks firewall to a Netskope tenant with the Netskope for Web license enabled. Your tunnel is up as seen from the Netskope dashboard. You are unable to ping hosts behind the Netskope gateway.

Which two statements are true about this scenario? (Choose two.)

A. You need to call support to enable the GRE POP selection feature.
B. Netskope only supports Web traffic through the tunnel.
C. You can only ping the probe IP provided by Netskope.
D. There is no client installed on the source hosts in your network.

Answer: BC

Explanation:

Netskope's GRE tunneling supports only web traffic, which means ICMP traffic (ping) is not supported for hosts behind the Netskope gateway. You may, however, ping the probe IP provided by Netskope to test connectivity, as this IP is designated for diagnostics.

Question: 92

You are currently migrating users away from a legacy proxy to the Netskope client in the company's corporate offices. You have deployed the client to a pilot group; however, when the client attempts to connect to Netskope, it fails to establish a tunnel.

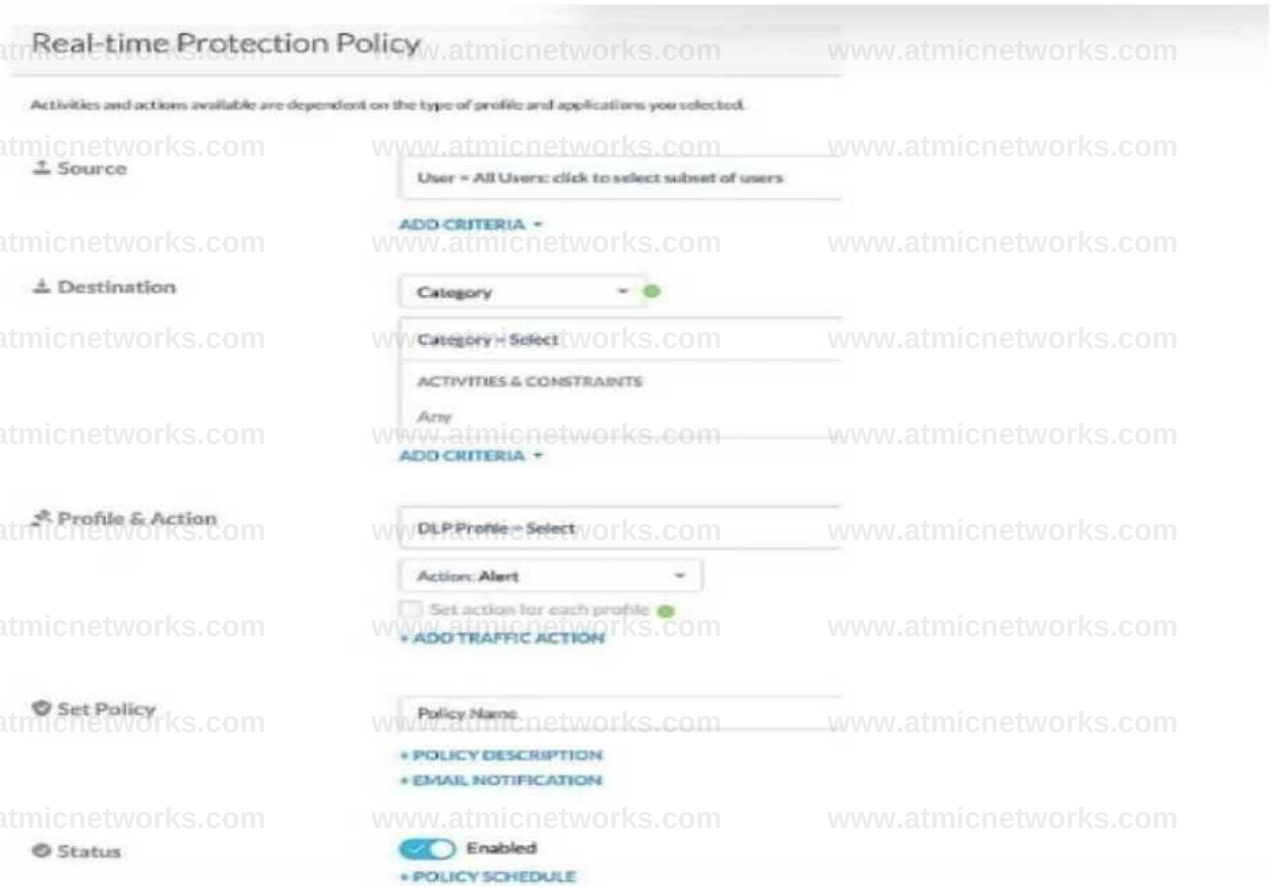
In this scenario, what would cause this problem?

A. The legacy proxy is intercepting SSL/TLS traffic to Netskope.
B. The corporate firewall is blocking UDP port 443 to Netskope.
C. The corporate firewall is blocking the Netskope EPoT address.
D. The client cannot reach dns.google for EDNS resolution.

Answer: B

Explanation:
The corporate firewall blocking UDP port 443 to Netskope could cause tunnel establishment failures. Netskope clients rely on this port for secure tunneling (via DTLS), so ensuring UDP port 443 is open is essential for connectivity. Additionally, legacy proxies intercepting traffic could also disrupt the SSL/TLS traffic necessary for the Netskope tunnel.

Question: 93
Review the exhibit.



Given the information shown below:

- for PCI data uploads, you want to provide no notification,
- for PHI data uploads, you want to allow users to proceed by clicking OK,
- for GDPR data uploads, you want to provide block notification,
- if none of the above matches, you want to provide no notification.

You want to reduce the number of policies by combining multiple DLP profiles Into one policy.

Referring to the exhibit, which two statements are true? (Choose two.)

A. You must open a support ticket to enable the Advanced Policies feature.
B. You must check the "set action for each profile" flag.
C. You can have only one action if you use multiple DLP profiles in the same policy.
D. You can apply a unique action to each profile In the same policy.

Answer:

BD

Explanation:

To apply different actions for each DLP profile in the same policy, you need to enable the "set action for each profile" flag. This allows you to configure unique actions (e.g., block, allow) for each DLP profile within a single combined policy, thus reducing the total number of policies needed

*** Netskope Exam App11 Provisioning**

r> Sort provisioning Q Stop provisioning Q Restart provisioning ^ Edit pronsionex