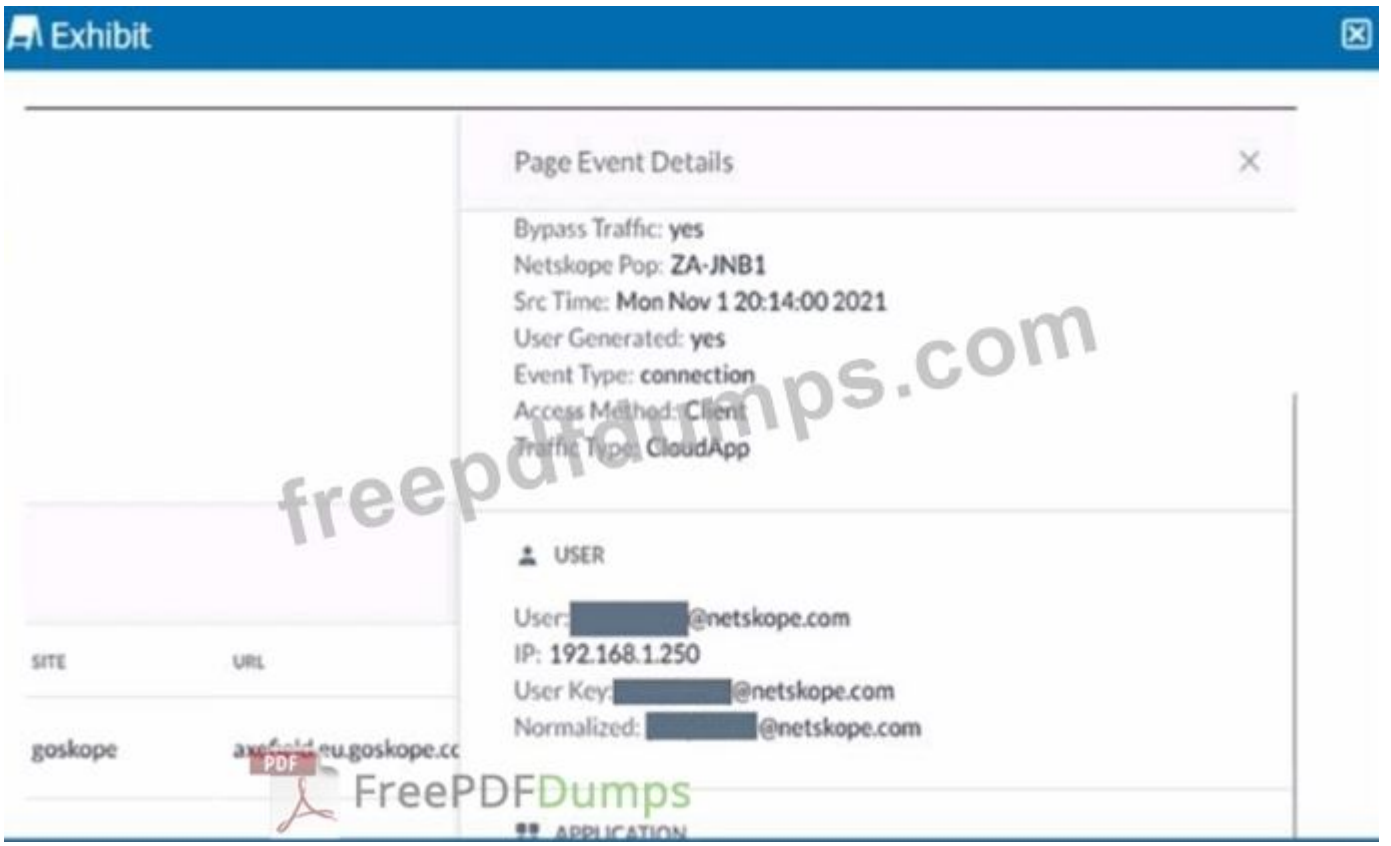
# Netskope.NSK200.v2026-08-11.q42

| | |
|---|---|
| **Exam Code:** | NSK200 |
| **Exam Name:** | Netskope Certified Cloud Security Integrator (NCCSI) |
| **Certification Provider:** | Netskope |
| **Free Question Number:** | 42 |
| **Version:** | v2026-08-11 |
| **# of views:** | 126 |
| **# of Questions views:** | 420 |
| https://www.freepdfdumps.com/Netskope.NSK200.v2026-08-11.q42.html | |

**NEW QUESTION: 1**
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 (LEAVE A REPLY)**

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. References: Page Events - Netskope Knowledge Portal, Add a Policy for SSL Decryption - Netskope Knowledge Portal, YouTube Content Control - Netskope Knowledge Portal

**NEW QUESTION: 2**
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: (SHOW ANSWER)**
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.

**NEW QUESTION: 3**
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 (LEAVE A REPLY)**
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.

**NEW QUESTION: 4**

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: (SHOW ANSWER)**
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. References: Creating a Cloud App Definition - Netskope Knowledge Portal

**NEW QUESTION: 5**
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 (LEAVE A REPLY)**
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. References: Remote Browser Isolation - Netskope Knowledge Portal, Netskope Remote Browser Isolation - Netskope

**NEW QUESTION: 6**
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.** Create a new tenant steering exception type of Destination Locations that contains the Dropbox application.
**C.** Remove all Dropbox entries from the tenant steering SSL configuration entirely.
**D.** Modify the existing tenant steering exception configuration to block the Dropbox native application to force users to use the Dropbox website.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 7**
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 (LEAVE A REPLY)**
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. References: Add a Policy for SSL Decryption - Netskope Knowledge Portal, Default Microsoft appsuite SSL do not decrypt rule - Netskope Community

**NEW QUESTION: 8**
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: (SHOW ANSWER)**
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. References: 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

**NEW QUESTION: 9**
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: (SHOW ANSWER)**
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.

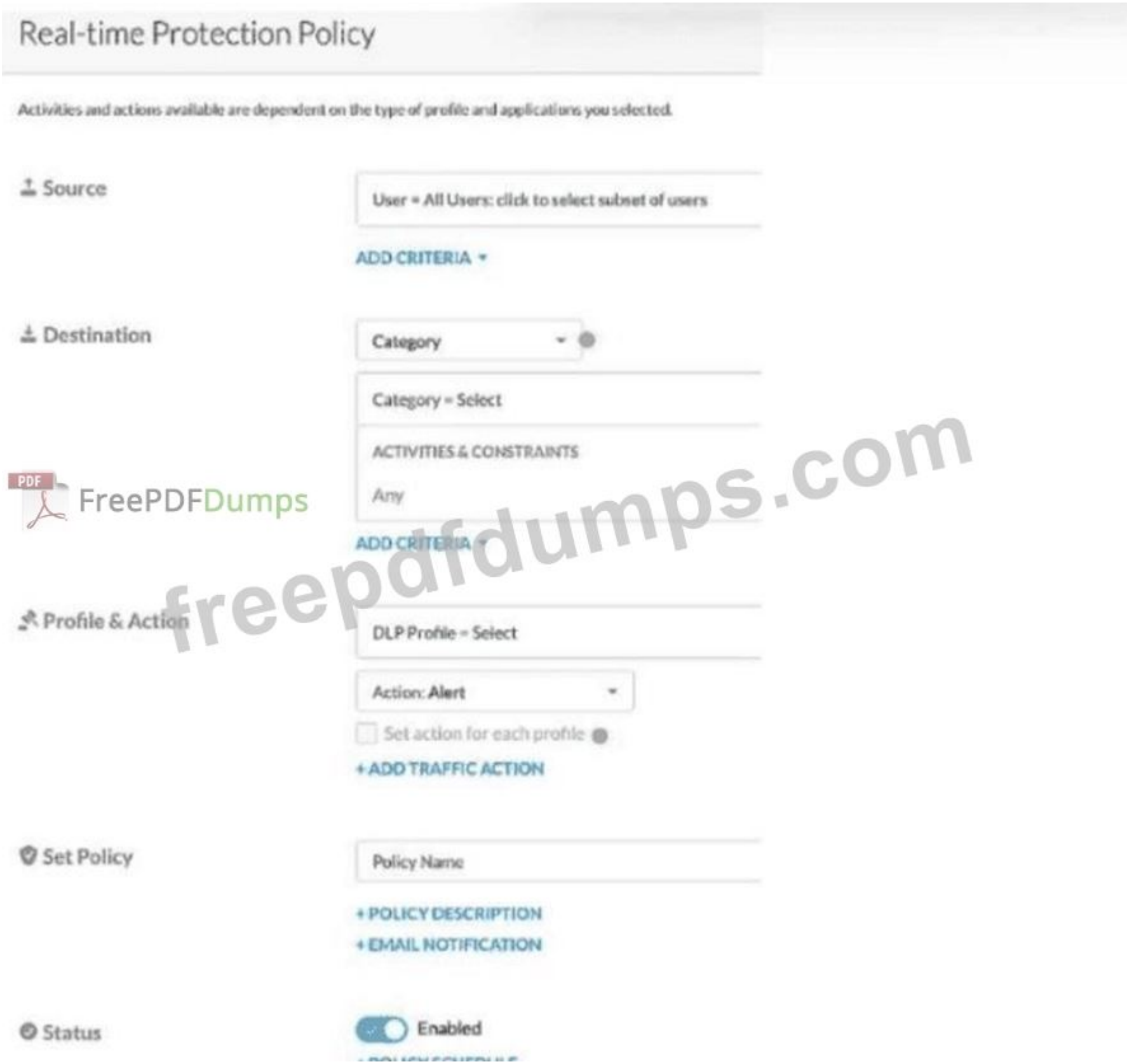
**NEW QUESTION: 10**
You are an administrator writing Netskope Real-time Protection policies and must determine proper policy ordering.
Which two statements are true in this scenario? (Choose two.)
**A.** You must place Netskope private access malware policies in the middle.
**B.** You do not need to 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: B,D (LEAVE A REPLY)**
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. References: 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

**NEW QUESTION: 11**
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 (LEAVE A REPLY)**
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. References: Real-time Protection Policies1, API Data Protection Policies2

**NEW QUESTION: 12**
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: (SHOW ANSWER)**
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. References: Troubleshooting Netskope Client - Netskope Knowledge Portal, Client Health Check - Netskope Knowledge Portal

**NEW QUESTION: 13**
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: B,D (LEAVE A REPLY)**

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.

**NEW 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 (LEAVE A REPLY)**

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

**NEW QUESTION: 15**

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: (SHOW ANSWER)**

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. References: Proxy Chaining3, Configure Forcepoint for Proxy Chaining

**NEW QUESTION: 16**
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: A,D (LEAVE A REPLY)**
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. References: Explicit Proxy3, [Explicit Proxy over IPSec and GRE Tunnels]



**NEW QUESTION: 17**
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 vl 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 (LEAVE A REPLY)**

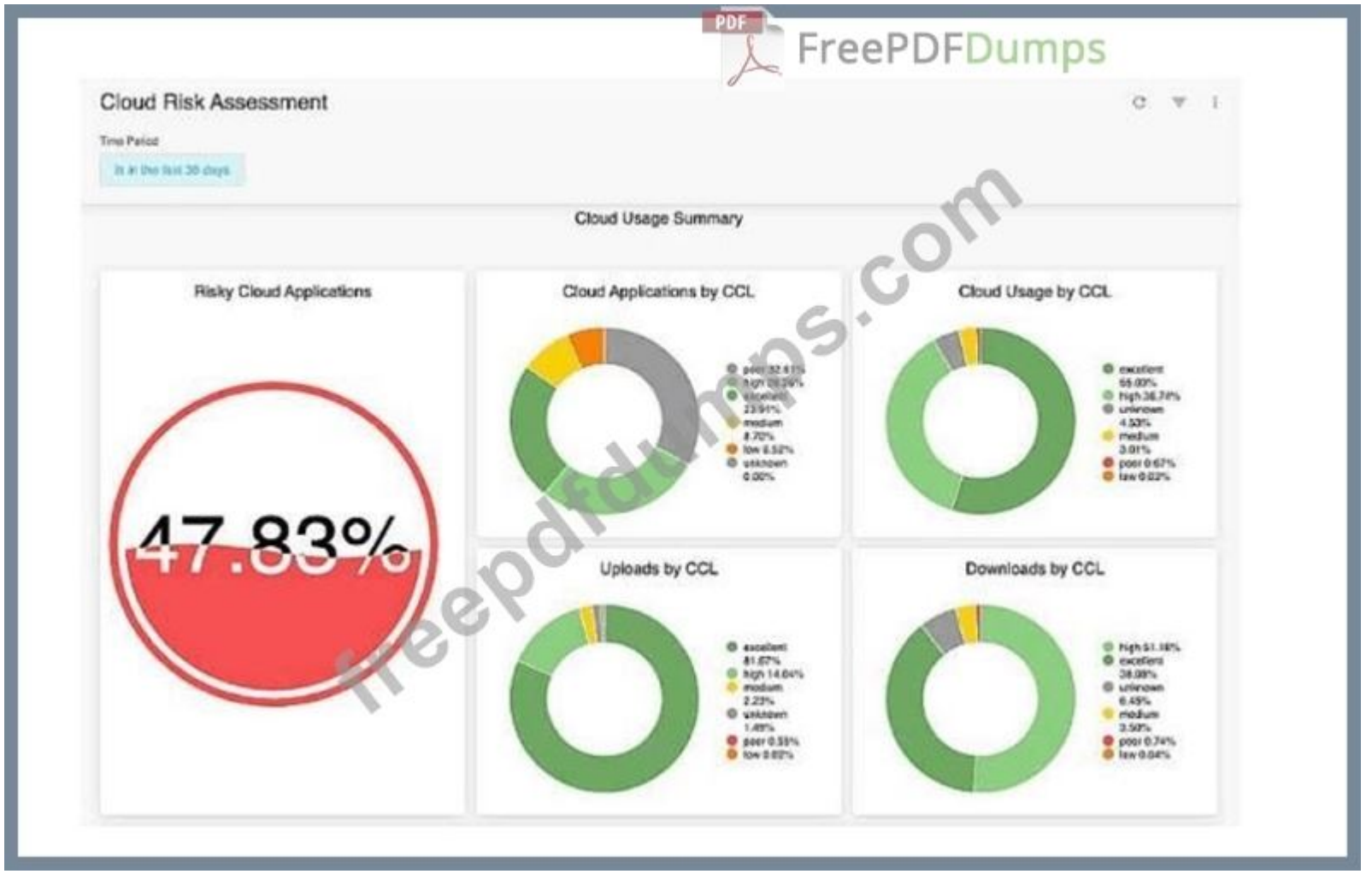
The statement that describes how Netskope's REST API, v1 and v2, handles authentication is A. Both REST API v1 and v2 require the use of tokens to make calls to the API. A token is a unique string that identifies the user or application that is making the API request. The token must be included in the 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. References: 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

**NEW QUESTION: 18**
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 (LEAVE A REPLY)**
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.

**NEW QUESTION: 19**
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 (LEAVE A REPLY)**
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.

**NEW QUESTION: 20**

Examine the image provided.




You are asked to provide the results of a cloud risk assessment to your executive team. The results must be presented visually, as well as have the ability to drill down and pivot on the data. Referring to the image, what will satisfy the requirements in this scenario?

**A.** Netskope Advanced Analytics

**B.** Netskope Reports

**C.** Skope IT Application Events

**D.** Discovered Apps in the Cloud Confidence Index (CCI)

**Answer: A (LEAVE A REPLY)**

Netskope Advanced Analytics is the correct choice because the requirement is not just to show application risk data, but to present it visually and allow drill-down and pivot-style analysis. Advanced Analytics supports custom reports, dashboards, widgets, and visualizations built from event and alert data. Netskope also describes drill-down behavior within visualizations, where users can click data points and explore the underlying details. This makes it appropriate for an executive cloud risk assessment because it supports high- level presentation and deeper analysis from the same reporting layer. Netskope Reports are less flexible for interactive pivoting and drill-down. Skope IT Application Events are operational logs, not executive reporting dashboards. CCI discovered apps can support risk review, but it does not satisfy the full visualization, pivot, and drill-down requirement.

**NEW QUESTION: 21**

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.

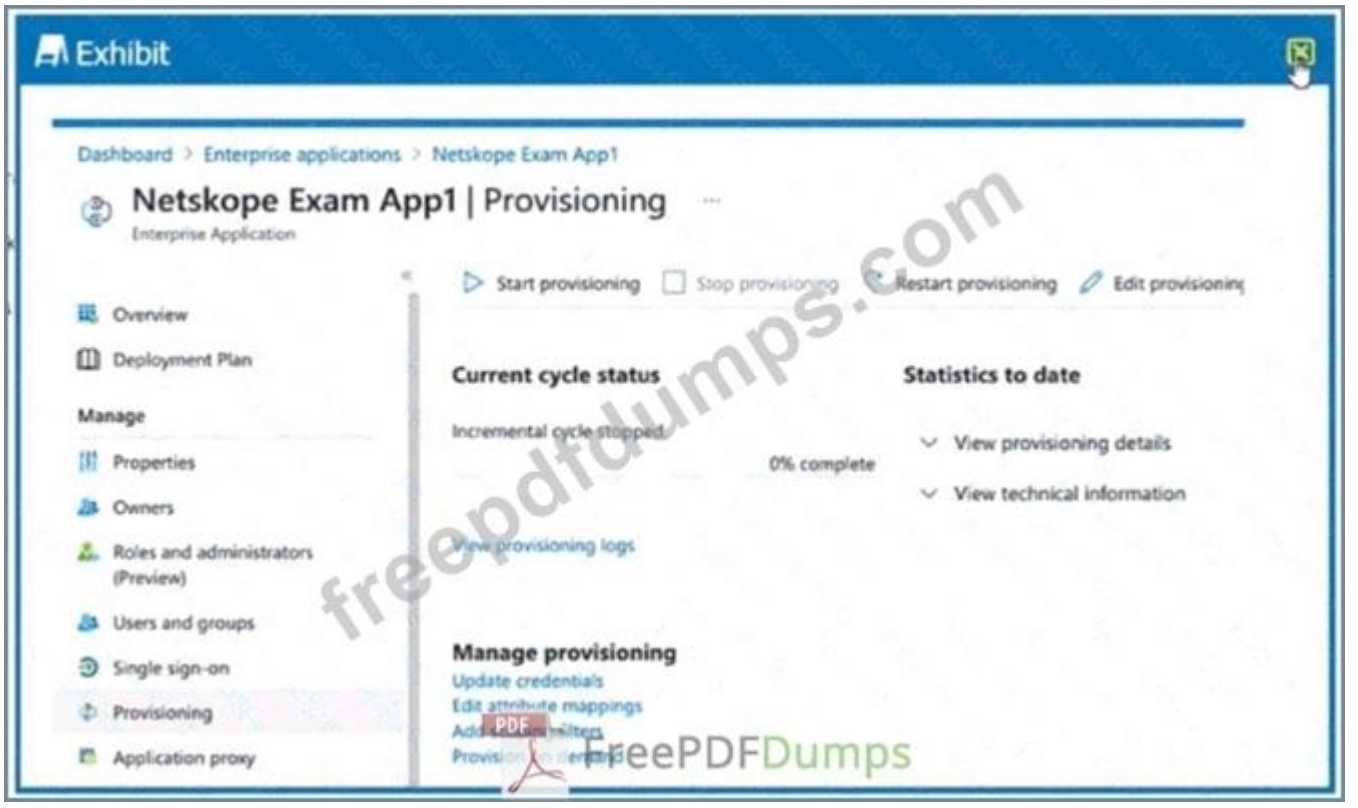
**D.** You must use an Advanced Threat Protection license to support multiple tokens to share events.

**Answer: C (LEAVE A REPLY)**

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.

**NEW QUESTION: 22**

Review the exhibit.




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 (LEAVE A REPLY)**

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.

Onboarding Active Directory Users to a Netskope Tenant1

**NEW QUESTION: 23**

The risk team at your company has determined that traffic from the sales team to a custom Web application should not be inspected by Netskope. All other traffic to the Web application should continue to be inspected.

In this scenario, how would you accomplish this task?

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

**Answer: (SHOW ANSWER)**

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.

**NEW QUESTION: 24**

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 (LEAVE A REPLY)**

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. References: Quarantine - Netskope Knowledge Portal, Threat Protection - Netskope Knowledge Portal

**NEW QUESTION: 25**
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 (LEAVE A REPLY)**
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.

**NEW QUESTION: 26**
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 (LEAVE A REPLY)**
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. References: REST API v2 Overview - Netskope Knowledge Portal, Update a URL List - Netskope Knowledge Portal

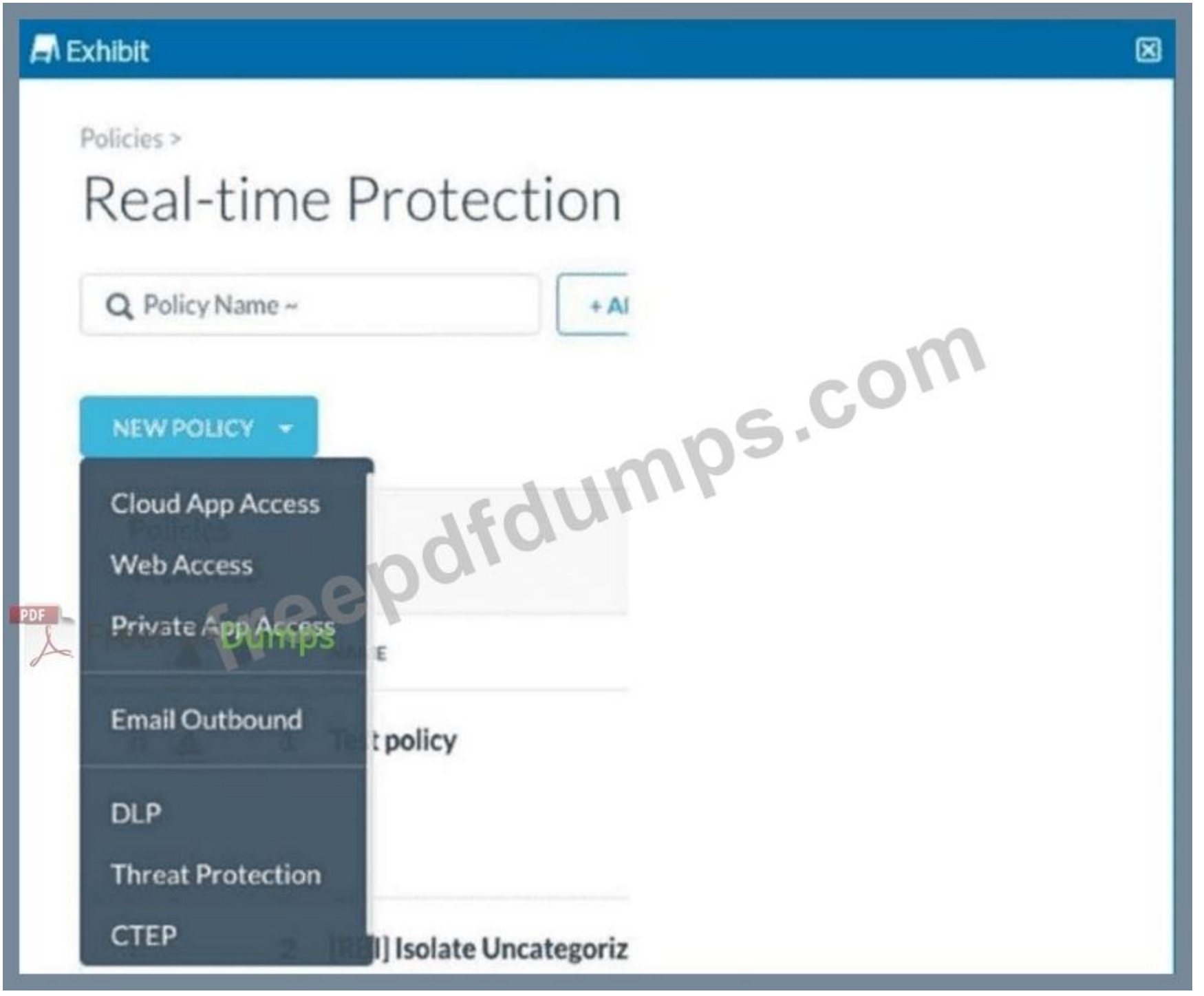
**NEW QUESTION: 27**
You want to secure Microsoft Exchange and Gmail SMTP traffic for DLP using Netskope. Which statement is true about this scenario when using the Netskope client?
**A.** Netskope can inspect outbound SMTP traffic for Microsoft Exchange and Gmail.
**B.** Enable Cloud Firewall to Inspect 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 (LEAVE A REPLY)**
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. References: Configure Netskope SMTP Proxy with Microsoft O365 Exchange, Configure Netskope SMTP Proxy with Gmail, SMTP DLP, Best Practices for Email Security with SMTP proxy

**NEW QUESTION: 28**
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: (SHOW ANSWER)**
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.

**NEW QUESTION: 29**
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: C,D (LEAVE A REPLY)**
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.

**NEW QUESTION: 30**
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 (LEAVE A REPLY)**

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.

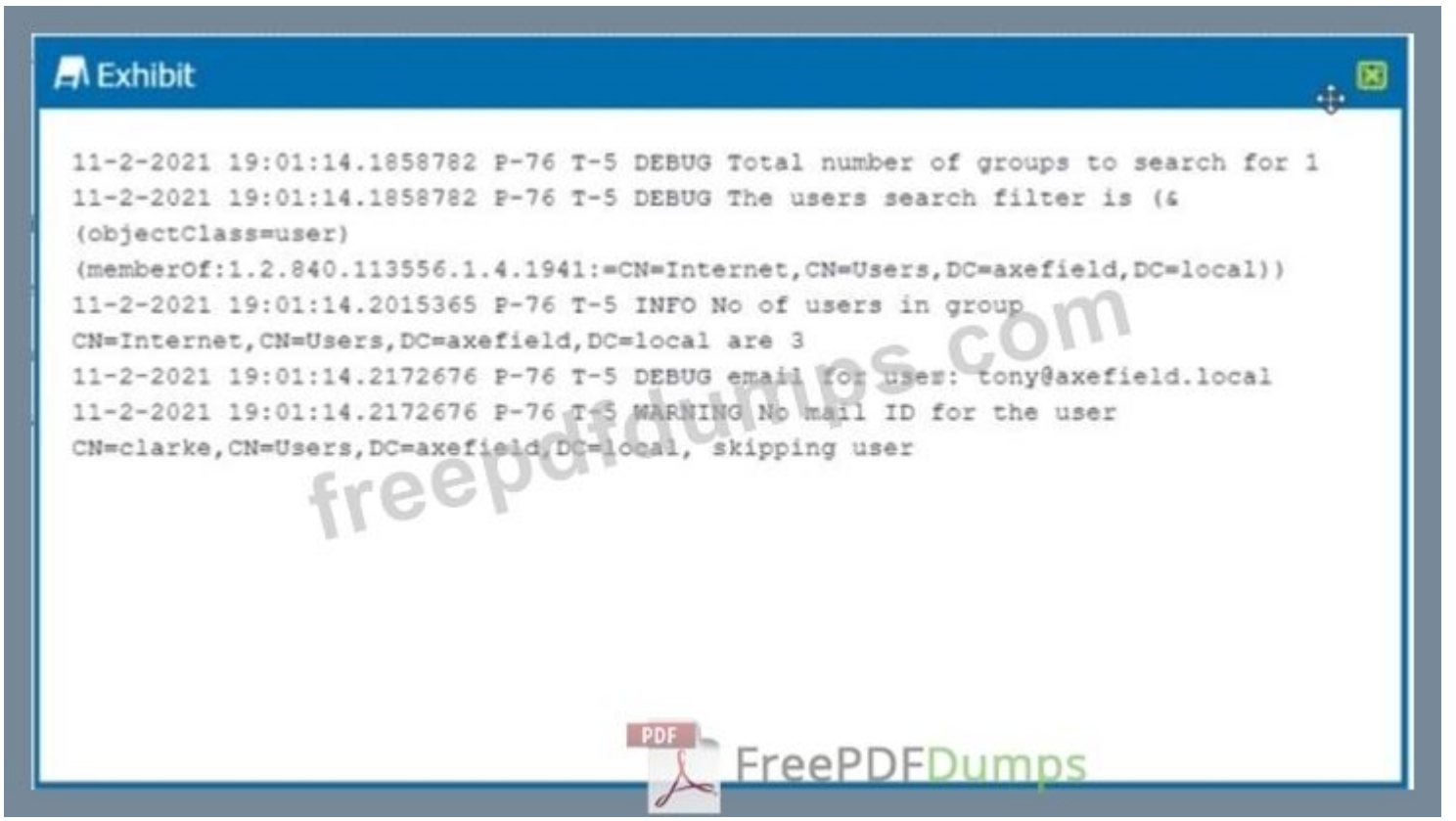
**NEW QUESTION: 31**
You are asked to prevent Netskope from inspecting Google traffic while maintaining visibility. According to Netskope, what is the recommended way to accomplish this task?
**A.** Create a real-time policy to block Google traffic.
**B.** Create a steering exception.
**C.** Add a trusted CA to allow Netskope to trust the traffic source.
**D.** Create a Do Not Decrypt SSL policy for the Google traffic.
**Answer: D (LEAVE A REPLY)**
The correct method is to create a Do Not Decrypt SSL policy for the Google traffic. This satisfies both parts of the requirement: Netskope does not perform SSL inspection on the selected Google traffic, but the traffic is still sent to the Netskope Cloud, preserving visibility and policy awareness. A steering exception would bypass Netskope entirely at the device level, which means the traffic would not reach the Netskope Cloud and visibility would be reduced or lost. A real-time block policy would deny the traffic, not merely prevent inspection. Adding a trusted CA only addresses certificate trust and does not define an inspection bypass.
Netskope specifically distinguishes SSL decryption bypasses from steering bypasses and recommends SSL bypasses when visibility should be preserved.



**NEW QUESTION: 32**
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: A,C (LEAVE A REPLY)**
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. References: Application Events - Netskope Knowledge Portal, Alerts - Netskope Knowledge Portal

**NEW QUESTION: 33**
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 (LEAVE A REPLY)**
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.

**NEW 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 (LEAVE A REPLY)**
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. References: REST API v2 Overview - Netskope Knowledge Portal, Manage URL Lists
- Netskope Knowledge Portal

**NEW QUESTION: 35**
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 (LEAVE A REPLY)**
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. References: Provisioning Users for Netskope Client1, SCIM Integration2

**NEW QUESTION: 36**
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 (LEAVE A REPLY)**

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.

**NEW QUESTION: 37**
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: (SHOW ANSWER)**
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. References: Optical Character Recognition (OCR) - Netskope Knowledge Portal, Add a Policy for Data Protection - Netskope Knowledge Portal

**NEW QUESTION: 38**
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: A,B (LEAVE A REPLY)**
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

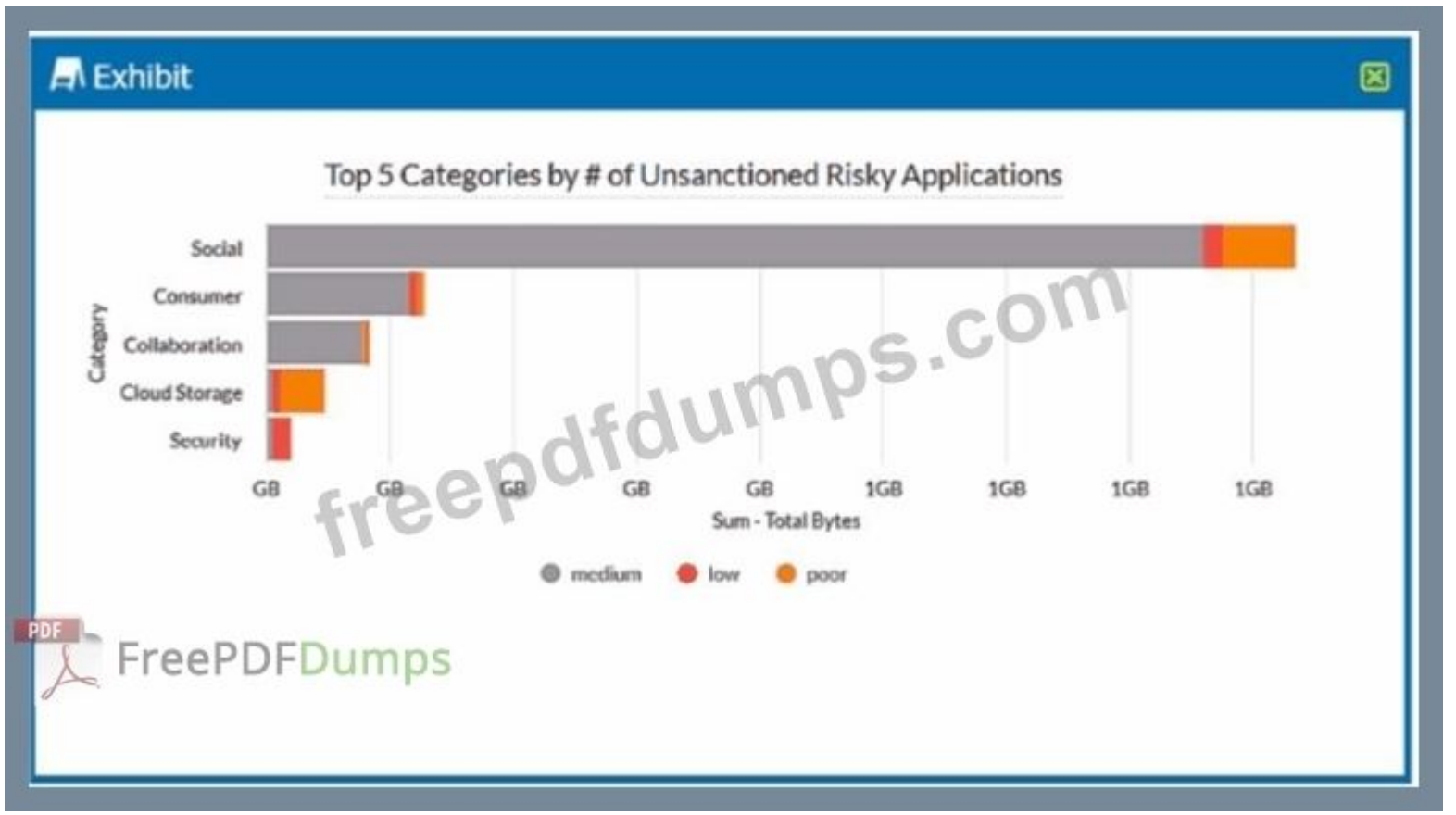
**NEW QUESTION: 39**
Your customer has deployed the Netskope client to secure their Web traffic. Recently, they have enabled Cloud Firewall (CFW) to secure all outbound traffic for their endpoints. Through a recent acquisition, they must secure all outbound traffic at several remote offices where they 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 (LEAVE A REPLY)**
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.

**NEW QUESTION: 40**
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: (SHOW ANSWER)**
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. References: Certificate Pinned Applications - Netskope Knowledge Portal, Certificate Pinned App (CPA) - The Netskope Community, Steering Configuration - Netskope Knowledge Portal, Steering Exceptions - Netskope Knowledge Portal

**NEW QUESTION: 41**
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: (SHOW ANSWER)**
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.

**NEW QUESTION: 42**
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: B,D (LEAVE A REPLY)**

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.

References: Advanced Analytics

**Valid NSK200 Dumps** shared by Actual4test.com for Helping Passing NSK200 Exam! Actual4test.com now offer the **newest NSK200 exam dumps**, the Actual4test.com NSK200 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com NSK200 dumps with Test Engine here: https://www.actual4test.com/NSK200_examcollection.html (**98** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)