Netskope.NSK300.v2026-04-21.q55

Exam Code:	NSK300
Exam Name:	Netskope Certified Cloud Security Architect
Certification Provider:	Netskope
Free Question Number:	55
Version:	v2026-04-21
# of views:	689
# of Questions views:	614
https://www.dumpsfiles.com/files/Netskope/NSK300/Netskope.NSK300.v2026-04-21.q55	

NEW QUESTION: 1
You are implementing a solution to deploy Netskope for machine traffic in an AWS account across multiple VPCs. You want to deploy the least amount of tunnels while providing connectivity for all VPCs.
How would you accomplish this task?
A. Use IPsec tunnels from the AWS Virtual Private Gateway.
B. Use GRE tunnels from the AWS Transit Gateway.
C. Use GRE tunnels from the AWS Virtual Private Gateway
D. Use IPsec tunnels from the AWS Transit Gateway.
Answer: (SHOW ANSWER)
The best approach to deploy Netskope for machine traffic across multiple VPCs in an AWS account with the least amount of tunnels while providing connectivity for all VPCs is to use IPsec tunnels from the AWS Transit Gateway. This method allows you to use the same Site-to-Site VPN connection to Netskope for multiple VPCs, thus minimizing the number of tunnels required12. The AWS Transit Gateway acts as a network transit hub, enabling you to connect your VPCs and on-premises networks through a central point of management and control. Using IPsec tunnels with the AWS Transit Gateway ensures that all VPCs connected to it utilize the same IPsec tunnel between the transit gateway and Netskope POP1.

NEW QUESTION: 2
You deployed Netskope Cloud Security Posture Management (CSPM) using pre-defined benchmark rules to monitor your cloud posture in AWS, Azure, and GCP. You are asked to assess if you can extend the Netskope CSPM solution by creating custom rules for each environment.
Which statement is correct?
A. With Netskope CSPM, you can create custom rules using Domain Specific Language for AWS. Azure, and GCP

B. Custom rules using Domain Specific Language are only available when using SSPM.
C. With Netskope CSPM, you can create custom rules using Domain Specific Language for AWS. Azure, but not for GCP.
D. You will need to evaluate SaaS Security Posture Management (SSPM) in addition to CSPM so that rules applied to GCP will align with Google Workspace
Answer: A (LEAVE A REPLY)
Netskope Cloud Security Posture Management (CSPM) allows for the creation of custom rules using Domain Specific Language (DSL) for all three major cloud platforms: AWS, Azure, and GCP. This capability is integral to CSPM and enables organizations to tailor their security posture assessments to their specific needs across different cloud environments.
The ability to create custom rules using DSL within Netskope CSPM for AWS, Azure, and GCP is documented in the Netskope Knowledge Portal. It provides detailed instructions on how to build custom rules under Policies > Security Posture > Profiles & Rules for security assessment of resources across these cloud platforms

NEW QUESTION: 3
You are asked to create a Real-time Protection policy to inspect outbound e-mail for DLP violations. You must prevent sensitive e-mail from leaving the corporate mail relay.
In this scenario, which Real-time Protection policy action must be specified?
A. Add SMTP Header
B. Alert
C. Forward to Proxy
D. Block
Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
A company's architecture includes a server subnet that is logically isolated from the rest of the network with no Internet access, no default gateway, and no access to DNS. New resources can only be provisioned on virtual resources in that segment and there is a firewall that is tunnel-capable securing the perimeter of the segment. The only requirement is to have content filtering for any server that might access the Internet using a browser.
Which two Netskope deployment methods would achieve this requirement? (Choose two.)
A. Deploy a mobile profile on the servers.
B. Deploy Data Plane on Premises (DPoP) with a proxy configuration on the servers.
C. Deploy IPsec or GRE tunnels in the segment to steer traffic from the servers to Netskope.
D. Install the Netskope Client on the servers
Answer: B,C (LEAVE A REPLY)
For a server subnet that is isolated and requires content filtering for any server that might access the Internet using a browser, the two Netskope deployment methods that would meet this requirement are:

B . Deploy Data Plane on Premises (DPoP) with a proxy configuration on the servers: Deploying DPoP would allow the isolated servers to connect to the Netskope cloud for content filtering through a proxy configuration. This setup would enable the servers to have controlled access to the Internet for content filtering purposes without requiring direct Internet access1.
C . Deploy IPsec or GRE tunnels in the segment to steer traffic from the servers to Netskope: By deploying IPsec or GRE tunnels, the traffic from the servers can be securely directed to Netskope for content filtering. This method is suitable for environments where servers do not have direct Internet access, as the tunnel provides a secure path for traffic to reach Netskope's cloud services1.
These deployment methods are designed to work in environments with strict network isolation and provide the necessary content filtering capabilities for servers accessing the Internet.

NEW QUESTION: 5
A recent report states that users are using non-sanctioned Cloud Storage platforms to share data Your CISO asks you for a list of aggregated users, applications, and instance IDs to increase security posture Which Netskope tool would be used to obtain this data?
A. Advanced Analytics
B. Behavior Analytics
C. Applications in Skope IT
D. Cloud Confidence Index (CCI)
Answer: A (LEAVE A REPLY)
To obtain a list of aggregated users, applications, and instance IDs, especially when dealing with non-sanctioned Cloud Storage platforms, the Advanced Analytics (A) tool within Netskope would be used. Advanced Analytics provides in-depth visibility into cloud app usage and activities. It allows security teams to create detailed reports and dashboards that can help identify risks and ensure compliance with company policies by analyzing user behavior, application access, and data movement across the organization1.

NEW QUESTION: 6
You are implementing Netskope Cloud Exchange in your company lo include functionality provided by third-party partners. What would be a reason for using Netskope Cloud Risk Exchange in this scenario?
A. to ingest events and alerts from a Netskope tenant
B. to feed SOC with detection and response services
C. to map multiple scores to a normalized range
D. to automate service tickets from alerts of interest
Answer: D (LEAVE A REPLY)
The reason for using Netskope Cloud Risk Exchange in this scenario is to automate service tickets from alerts of interest. Netskope Cloud Risk Exchange (CRE) is designed to ingest user, device, and application risk scores, creating a dashboard view of contributors to your company's overall risk score and trend. One of the key functionalities of CRE is to trigger risk-reducing

actions through business rules that are tuned to a weighted score. Automating service tickets from alerts of interest is a part of this functionality, as it allows for the automatic creation of tickets in response to specific alerts, streamlining the process of addressing potential security issues12.

NEW QUESTION: 7
You are building an architecture plan to roll out Netskope for on-premises devices. You determine that tunnels are the best way to achieve this task due to a lack of support for explicit proxy in some instances and IPsec is the right type of tunnel to achieve the desired security and steering. What are three valid elements that you must consider when using IPsec tunnels in this scenario? (Choose three.)
A. cipher support on tunnel-initiating devices
B. bandwidth considerations
C. the categories to be blocked
D. the impact of threat scanning performance
E. Netskope Client behavior when on-premises
Answer: (SHOW ANSWER)
When using IPsec tunnels, especially in the context of deploying Netskope for on-premises devices, several factors must be considered to ensure a secure and efficient architecture:
Cipher support on tunnel-initiating devices (A): It is crucial to ensure that the devices initiating the IPsec tunnels support the ciphers used by Netskope. This compatibility is necessary for establishing secure connections.
Bandwidth considerations (B): The bandwidth available for the IPsec tunnels will affect the data throughput and performance of the connection. Adequate bandwidth must be allocated to handle the expected traffic without causing bottlenecks.
The impact of threat scanning performance (D): The performance of threat scanning can be affected by the encryption and decryption processes in IPsec tunnels. It is important to consider how the threat scanning capabilities will perform under the additional load of encrypted traffic.
These elements are essential for the successful implementation of IPsec tunnels in a Netskope architecture plan for on-premises devices12.

NEW QUESTION: 8
Given the following:

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

Which result does this Skope IT query provide?
A. The query returns all events of user@company.com downloading or uploading to or from the site 'Amazon S3" using the Netskope Client.
B. The query returns all events of an IP address downloading or uploading to or from Amazon S3 using the Netskope Client.
C. The query returns all events of everyone except user@company.com downloading or uploading to or from the site "Amazon S3" using the Netskope Client.

D. The query returns all events of user@company.com downloading or uploading to or from the application "Amazon S3" using the Netskope Client.

Answer: A (LEAVE A REPLY)

The given Skope IT query specifies the following conditions:
User equals 'user@company.com'
Access method equals 'Client'
Activity equals 'Download' or 'Upload'
Site equals 'Amazon S3'
The query combines these conditions using logical operators (AND and OR).
The result of this query will include all events where the specified user ('user@company.com') is either downloading or uploading data to or from the site 'Amazon S3' using the Netskope Client.
It does not include events related to other users or IP addresses. Reference:
Netskope Security Cloud Introductory Online Technical Training
Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training

NEW QUESTION: 9

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

A. Go to Skope IT > Alerts, switch to Query Mode and perform the detection_engine eq 'Netskope Cloud Sandbox' query.

B. Go to Skope IT > Page Events, switch to Query Mode and perform the detection_engine eq 'Netskope Cloud Sandbox' query.

C. Go to Incidents > Malicious Sites, and perform the detection_engine eq 'Advanced Detection' query.

D. Go to Incidents > Malware and perform the detection_engine eq 'Netskope Cloud Sandbox' query.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 10

What is a Fast Scan component of Netskope Threat Detection?

A. Heuristic Analysis

B. Machine Learning

C. Dynamic Analysis

D. Statical Analysis

Answer: B (LEAVE A REPLY)

The Fast Scan component of Netskope Threat Detection utilizes Machine Learning to quickly detect and block malware in real-time. This is part of Netskope's multi-layered security approach, which includes various engines to defend against a wide range of threats. The Fast Scan capability specifically leverages machine learning-based detection for rapid analysis and response to potential threats1.

The information regarding the Fast Scan component and its use of Machine Learning can be found in the Netskope documentation, which outlines the threat protection framework and the role of machine learning in detecting and blocking malware

NEW QUESTION: 11
Review the exhibit.
You work for a medical insurance provider. You have Netskope Next Gen Secure Web Gateway deployed to all managed user devices with limited block policies. Your manager asks that you begin blocking Cloud Storage applications that are not HIPAA compliant Prior to implementing this policy, you want to verity that no business or departmental applications would be blocked by this policy.
Referring to the exhibit, which query would you use in the Edit Widget window to narrow down the results?
A. app-ccl-compliance-cert neq 'HIPAA' and category eq 'Cloud Storage'
B. Cloud Confidence Compliance neq HIPAA and Cloud Confidence Category is Cloud Storage
C. SELECT application WHERE 'HIPAA' NOT IN app-cci-compliance AND WHERE 'Cloud Storage' IN category
D. app-compliance does not contain HIPAA and category must equal Cloud Storage
Answer: A (LEAVE A REPLY)
The correct query to use in the Edit Widget window to narrow down the results is option A: "app-ccl-compliance-cert neq 'HIPAA' and category eq 'Cloud Storage'". This query filters out applications that are not HIPAA compliant and belong to the Cloud Storage category, ensuring that only non-HIPAA compliant cloud storage applications are displayed in the results. This helps in identifying and blocking such applications as per the manager's request without affecting business or departmental applications. It aligns with Netskope's capabilities to enforce controls and restrictions on high-risk cloud services to help address HIPAA and HITECH compliance, as well as to audit suspected violations with a full cloud and web activity trail1.

NEW QUESTION: 12
You are deploying the Netskope Client in a multi-user VDI environment and need to determine the command to deploy the MSI.
Which three parameters are required in this scenario? (Choose three.)
A. token=
B. installmode=IDP
C. mode=peruserconfig
D. autoupdate=on
E. host=
Answer: (SHOW ANSWER)

NEW QUESTION: 13

A company needs to block access to their instance of Microsoft 365 from unmanaged devices. They have configured Reverse Proxy and have also created a policy that blocks login activity for the AD group
"marketing-users" for the Reverse Proxy access method. During UAT testing, they notice that access from unmanaged devices to Microsoft 365 is not blocked for marketing users.
What is causing this issue?
A. There is a missing group name in the SAML response.
B. The username in the name ID field is not in the format of the e-mail address.
C. There is an invalid certificate in the SAML response.
D. The username in the name ID field does not have the "marketing-users" group name.
Answer: A (LEAVE A REPLY)
The issue is likely caused bya missing group name in the SAML response (A). When access to Microsoft 365 from unmanaged devices is not blocked as expected, despite having a policy in place, it often indicates that the SAML assertion is not correctly identifying the user as a member of the restricted group. In this case, the
"marketing-users" group name should be present in the SAML response to enforce the policy that blocks login activity for this group. If the group name is missing, the policy will not apply, and users will not be blocked as intended.
This explanation is consistent with the configuration requirements for access control using SAML responses, as detailed in Netskope's documentation on Reverse Proxy and SAML integration1.

NEW QUESTION: 14
You are attempting to merge two Advanced Analytics reports with DLP incidents: Report A with 3000 rows and Report B with 6000 rows. Once merged, you notice that the merged report is missing a significant number of rows.
What is causing this behavior?
A. Netskope automatically deduplicates data in merged reports.
B. Missing data is due to viewing limits.
C. Filters are applied differently to dimensions and measures
D. Visualizations have a system limit of 5000 rows.
Answer: B (LEAVE A REPLY)
When merging two Advanced Analytics reports in Netskope, if the merged report is missing rows, it is likely due to viewing limits within the system. Netskope's Advanced Analytics platform has limitations on the number of rows that can be viewed at once, which can result in missing data when dealing with large reports.
This viewing limit ensures performance and manageability of the data within the system.
The behavior of data viewing limits in Netskope Advanced Analytics is discussed in the Netskope Knowledge Portal, which provides insights into how data is explored and managed within the platform1

NEW QUESTION: 15

You need to extract events and alerts from the Netskope Security Cloud platform and push it to a SIEM solution. What are two supported methods to accomplish this task? (Choose two.)
A. Use Cloud Ticket Orchestrator.
B. Use Cloud Log Shipper.
C. Stream directly to syslog.
D. Use the REST API.
Answer: B,D (LEAVE A REPLY)
To extract events and alerts from the Netskope Security Cloud platform and integrate them with a SIEM (Security Information and Event Management) solution, you can utilize the following supported methods:
* Cloud Log Shipper (CLS):
* The Cloud Log Shipper is designed to forward Netskope logs to external systems, including SIEMs.
* It allows you to export logs in real-time or batch mode to a destination of your choice.
* By configuring CLS, you can ensure that Netskope events and alerts are sent to your SIEM for further analysis and correlation.
Reference: Netskope Documentation on Cloud Log Shipper
REST API:
The Netskope Security Cloud provides a comprehensive REST API that allows you to programmatically retrieve data, including events and alerts.
You can use the REST API to query specific logs, incidents, or other relevant information from Netskope.
By integrating with the REST API, you can extract data and push it to your SIEM solution.
Reference: Netskope REST API Documentation
References:
Netskope Cloud Security
Netskope Resources
Netskope Documentation
These methods ensure seamless data flow between Netskope and your SIEM, enabling effective security monitoring and incident response.

NEW QUESTION: 16
Your company purchased Netskope's Next Gen Secure Web Gateway You are working with your network administrator to create GRE tunnels to send traffic to Netskope Your network administrator has set up the tunnel, keepalives. and a policy-based route on your corporate router to send all HTTP and HTTPS traffic to Netskope. You want to validate that the tunnel is configured correctly and that traffic is flowing.
In this scenario, which two statements are correct? (Choose two.)
A. You can use your local router or network device to verify that keepalives are being received and traffic is flowing to Netskope.
B. You must use your own monitoring tools to verify that the tunnel is up.

C. You can verify that the tunnel is up and receiving traffic in the Netskope UI under Settings > Security Cloud Platform > GRE.
D. You can verify that the tunnel is up in the Netskope Trust portal at https://trust netskope.com/.
Answer: (SHOW ANSWER)
To validate that the GRE tunnel is configured correctly and that traffic is flowing to Netskope, the correct statements are:
* A: You can use your local router or network device to verify that keepalives are being received and traffic is flowing to Netskope. This is a standard method for checking the health and activity of a GRE tunnel.
* C: You can verify that the tunnel is up and receiving traffic in the Netskope UI under Settings > Security Cloud Platform > GRE. This is a feature provided by Netskope to monitor the status of GRE tunnels directly from the Netskope interface12.
Statement B is incorrect because Netskope provides its own tools for monitoring the status of the tunnel. Statement D is incorrect because the Netskope Trust portal provides information on the overall service status and updates, not specific tunnel status3.
The references for these answers can be found in the Netskope Knowledge Portal, which provides detailed guidance on configuring and validating GRE tunnels12. Additionally, the Netskope Community Forum offers insights and solutions for deploying and monitoring GRE tunnels

NEW QUESTION: 17
You deployed Netskope Cloud Security Posture Management (CSPM) using pre-defined benchmark rules to monitor your cloud posture in AWS, Azure, and GCP. You are asked to assess if you can extend the Netskope CSPM solution by creating custom rules for each environment.
Which statement is correct?
A. Custom rules using Domain Specific Language are only available when using SSPM.
B. You will need to evaluate SaaS Security Posture Management (SSPM) in addition to CSPM so that rules applied to GCP will align with Google Workspace
C. With Netskope CSPM, you can create custom rules using Domain Specific Language for AWS. Azure, but not for GCP.

D. With Netskope CSPM, you can create custom rules using Domain Specific Language for AWS. Azure, and GCP

Answer: D (LEAVE A REPLY)

Netskope Cloud Security Posture Management (CSPM) allows for the creation of custom rules using Domain Specific Language (DSL) for all three major cloud platforms: AWS, Azure, and GCP. This capability is integral to CSPM and enables organizations to tailor their security posture assessments to their specific needs across different cloud environments.

NEW QUESTION: 18

Review the exhibit.

You are attempting to block uploads of password-protected files. You have created the file profile shown in the exhibit.

Where should you add this profile to use in a Real-time Protection policy?

A. Add the profile to a DLP profile that is used in a Real-time Protection policy.

B. Add the profile to a Malware Detection profile that is used in a Real-time Protection policy.

C. Add the profile directly to a Real-time Protection policy as a Constraint.

D. Add the profile to a Constraint profile that is used in a Real-time Protection policy.

Answer: (SHOW ANSWER)

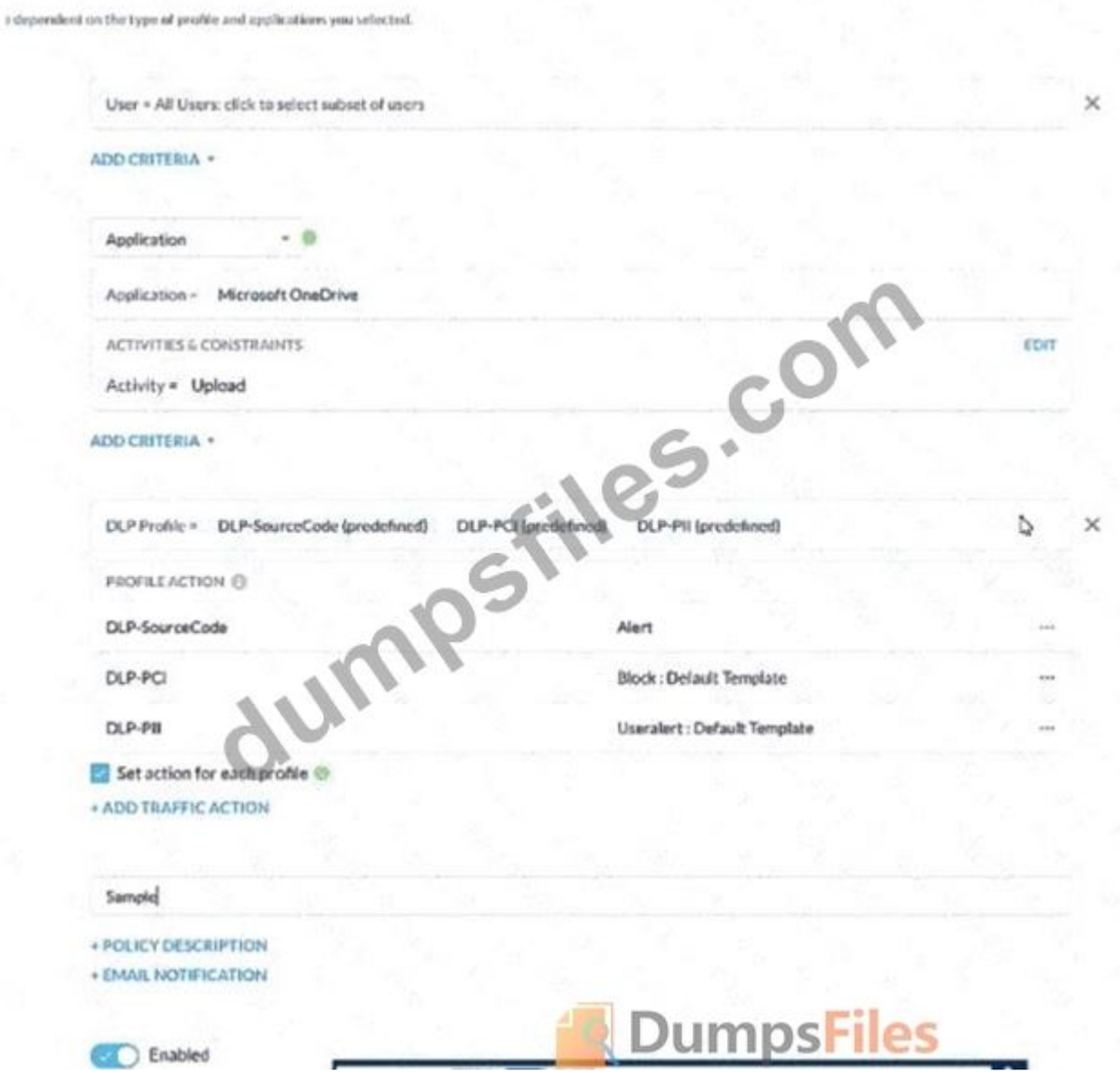
In Netskope Cloud Security, to block uploads of password-protected files, you should add the file profile to a DLP (Data Loss Prevention) profile that is used in a Real-time Protection policy. The DLP profiles in Netskope are designed to detect and protect sensitive data in real-time and at rest across the cloud environment. This approach ensures that any file matching the criteria set in the

file profile, such as being password-protected, will trigger the DLP rules and prevent the upload action in real-time.
The information aligns with the best practices for setting up DLP profiles in Netskope as described in their documentation and resources

NEW QUESTION: 19
Review the exhibit.

You created an SSL decryption policy to bypass the inspection of financial and accounting Web categories. However, you still see banking websites being inspected.
Referring to the exhibit, what are two possible causes of this behavior? (Choose two.)
A. The policy is in a "disabled" state.
B. An incorrect category has been selected
C. The policy is in a "pending changes" state.
D. An incorrect action has been specified.
Answer: B,D (LEAVE A REPLY)
The issue described in the exhibit is that banking websites are still being inspected despite creating an SSL decryption policy to bypass the inspection of financial and accounting web categories.
Possible Causes:
An incorrect category has been selected (Option B):
If the SSL decryption policy is configured to bypass the wrong category (e.g., not the actual financial and accounting category), it won't effectively exclude banking websites from inspection.
An incorrect action has been specified (Option D):
If the action specified in the policy is not set to "Bypass," it won't achieve the desired behavior. The policy should explicitly bypass SSL inspection for the selected category.
Solution:
Verify that the correct category (financial and accounting) is selected in the policy, and ensure that the action is set to "Bypass."

NEW QUESTION: 20
Review the exhibit.



A user has attempted to upload a file to Microsoft OneDrive that contains source code with PII and PCI data.

Referring to the exhibit, which statement Is correct?

A. The user will be blocked and a single Incident will be generated referencing the DLP-PCI profile.

B. The user will be blocked and a separate incident will be generated for each of the matching DLP profiles.

C. The user will be alerted and a single incident will be generated referencing the DLP-PII profile.

D. The user will be blocked and a single Incident will be generated referencing all of the matching DLP profiles

Answer: (SHOW ANSWER)

NEW QUESTION: 21

You configured a pair of IPsec funnels from the enterprise edge firewall to a Netskope data plane. These tunnels have been implemented to steer traffic for a set of defined HTTPS SaaS

applications accessed from end-user devices that do not support the Netskope Client installation. You discover that all applications steered through this tunnel are non-functional.
According to Netskope. how would you solve this problem?
A. Restart the tunnel to stop the tunnel from flapping.
B. Downgrade from IKE v2 to IKE v1.
C. Install the Netskope root and intermediate certificates on the end-user devices.
D. Disable Perfect Forward Secrecy on the tunnel configuration.
Answer: C (LEAVE A REPLY)
When applications steered through an IPsec tunnel are non-functional, it is often due to the lack of proper trust establishment between the end-user devices and the Netskope data plane. The solution is to install the Netskope root and intermediate certificates on the end-user devices . This ensures that the devices recognize and trust the encrypted connection established by the IPsec tunnel, allowing the HTTPS SaaS applications to function correctly. Without these certificates, the devices may not be able to verify the security of the connection, leading to application failures.

NEW QUESTION: 22
You deployed IPsec tunnels to steer on-premises traffic to Netskope. You are now experiencing problems with an application that had previously been working. In an attempt to solve the issue, you create a Steering Exception in the Netskope tenant tor that application: however, the problems are still occurring Which statement is correct in this scenario?
A. You must create a private application to steer Web application traffic to Netskope over an IPsec tunnel.
B. Exceptions only work with IP address destinations
C. Steering bypasses for IPsec tunnels must be applied at your edge network device.
D. You must deploy a PAC file to ensure the traffic is bypassed pre-tunnel
Answer: C (LEAVE A REPLY)
In the scenario where you have deployed IPsec tunnels to steer on-premises traffic to Netskope and are experiencing issues with an application, the correct statement is C: Steering bypasses for IPsec tunnels must be applied at your edge network device. This means that to effectively bypass the steering for a specific application, the configuration must be done on the network device that is establishing the IPsec tunnel, such as a firewall or router. This device controls the traffic before it enters the tunnel, so applying the bypass there ensures that the application's traffic does not get directed through the tunnel and can reach its destination directly.
The solution is based on standard practices for IPsec tunnel configuration and steering exceptions as described in Netskope's documentation on traffic steering and IPsec configuration12.

NEW QUESTION: 23
Your company purchased Netskope's Next Gen Secure Web Gateway You are working with your network administrator to create GRE tunnels to send traffic to Netskope Your network administrator has set up the tunnel, keepalives. and a policy-based route on your corporate router

to send all HTTP and HTTPS traffic to Netskope. You want to validate that the tunnel is configured correctly and that traffic is flowing.
In this scenario, which two statements are correct? (Choose two.)
A. You can use your local router or network device to verify that keepalives are being received and traffic is flowing to Netskope.
B. You must use your own monitoring tools to verify that the tunnel is up.
C. You can verify that the tunnel is up and receiving traffic in the Netskope UI under Settings > Security Cloud Platform > GRE.
D. You can verify that the tunnel is up in the Netskope Trust portal at https://trust netskope.com/.
Answer: A,C (LEAVE A REPLY)
To validate that the GRE tunnel is configured correctly and that traffic is flowing to Netskope, the correct statements are:
A: You can use your local router or network device to verify that keepalives are being received and traffic is flowing to Netskope. This is a standard method for checking the health and activity of a GRE tunnel.
C: You can verify that the tunnel is up and receiving traffic in the Netskope UI under Settings > Security Cloud Platform > GRE. This is a feature provided by Netskope to monitor the status of GRE tunnels directly from the Netskope interface12.
Statement B is incorrect because Netskope provides its own tools for monitoring the status of the tunnel. Statement D is incorrect because the Netskope Trust portal provides information on the overall service status and updates, not specific tunnel status3.

NEW QUESTION: 24
You have deployed Netskope to all users of the organization and you are now ready to begin ingesting all events, alerts, and Web transactions into your SIEM as a part of your requirements.
What are three ways in which you would accomplish this task? (Choose three.)
A. Use the Netskope Publisher to a stream syslog to your SIEM.
B. Use syslog directly to Splunk.
C. Use custom API calls to ingest to a data lake and then into your SIEM.
D. Use Cloud Log Shipper to an IaaS storage repository and then into your SIEM.
Answer: (SHOW ANSWER)

NEW QUESTION: 25
You deployed Netskope Cloud Security Posture Management (CSPM) using pre-defined benchmark rules to monitor your cloud posture in AWS, Azure, and GCP. You are asked to assess if you can extend the Netskope CSPM solution by creating custom rules for each environment.
Which statement is correct?
A. Custom rules using Domain Specific Language are only available when using SSPM.
B. You will need to evaluate SaaS Security Posture Management (SSPM) in addition to CSPM so that rules applied to GCP will align with Google Workspace

C. With Netskope CSPM, you can create custom rules using Domain Specific Language for AWS. Azure, but not for GCP.
D. With Netskope CSPM, you can create custom rules using Domain Specific Language for AWS. Azure, and GCP
Answer: D (LEAVE A REPLY)
Netskope Cloud Security Posture Management (CSPM) allows for the creation of custom rules using Domain Specific Language (DSL) for all three major cloud platforms: AWS, Azure, and GCP. This capability is integral to CSPM and enables organizations to tailor their security posture assessments to their specific needs across different cloud environments.
The ability to create custom rules using DSL within Netskope CSPM for AWS, Azure, and GCP is documented in the Netskope Knowledge Portal. It provides detailed instructions on how to build custom rules under Policies > Security Posture > Profiles & Rules for security assessment of resources across these cloud platforms

NEW QUESTION: 26
You have an NG-SWG customer that currently steers all Web traffic to Netskope using the Netskope Client. They have identified one new native application on Windows devices that is a certificate-pinned application. Users are not able to access the application due to certificate pinning. The customer wants to configure the Netskope Client so that the traffic from the application is steered to Netskope and the application works as expected.
Which two methods would satisfy the requirements? (Choose two.)
A. Bypass traffic using the bypass action in the Real-time Protection policy.
B. Configure the SSL Do Not Decrypt policy to not decrypt traffic for domains used by the native application.
C. Configure domain exceptions in the steering configuration for the domains used by the native application.
D. Tunnel traffic to Netskope and bypass traffic inspection at the Netskope proxy.
Answer: (SHOW ANSWER)
To address the issue of a certificate-pinned application not being accessible due to certificate pinning, while still steering the traffic to Netskope, the two methods that would satisfy the requirements are:
B: Configure the SSL Do Not Decrypt policy to not decrypt traffic for domains used by the native application. This ensures that the SSL traffic for the specified domains is not decrypted, thus avoiding issues with certificate pinning.
C: Configure domain exceptions in the steering configuration for the domains used by the native application. By setting domain exceptions, traffic to these domains will bypass SSL decryption, allowing the certificate-pinned application to function as expected1.
These methods are in line with Netskope's capabilities for handling certificate-pinned applications, which often require bypassing decryption to prevent breaking the application's functionality due to its security features1.

NEW QUESTION: 27
What are three valid Instance Types for supported SaaS applications when using Netskope's API-enabled Protection? (Choose three.)
A. Forensic
B. API Data Protection
C. Behavior Analytics
D. DLP Scan
E. Quarantine
Answer: B,D,E (LEAVE A REPLY)
When using Netskope's API-enabled Protection for supported SaaS applications, the valid instance types are:
API Data Protection (B): This type is used to connect to cloud apps using APIs to find sensitive content, enforce policy controls, and quarantine malware1.
DLP Scan (D): This instance type involves scanning for data loss prevention, which is a key component of Netskope's API Data Protection1.
Quarantine (E): This instance type allows for the isolation of potentially harmful or sensitive data until it can be reviewed or remediated1.
Behavior Analytics and Forensic (A) are not listed as instance types for API-enabled Protection in the provided resources.

NEW QUESTION: 28


Review the exhibit.
You work for a medical insurance provider. You have Netskope Next Gen Secure Web Gateway deployed to all managed user devices with limited block policies. Your manager asks that you begin blocking Cloud Storage applications that are not HIPAA compliant Prior to implementing this policy, you want to verity that no business or departmental applications would be blocked by this policy.
Referring to the exhibit, which query would you use in the Edit Widget window to narrow down the results?
A. app-ccl-compliance-cert neq 'HIPAA' and category eq 'Cloud Storage'
B. Cloud Confidence Compliance neq HIPAA and Cloud Confidence Category is Cloud Storage
C. SELECT application WHERE 'HIPAA' NOT IN app-cci-compliance AND WHERE 'Cloud Storage' IN category
D. app-compliance does not contain HIPAA and category must equal Cloud Storage
Answer: A (LEAVE A REPLY)
The correct query to use in the Edit Widget window to narrow down the results is option A: "app-ccl- compliance-cert neq 'HIPAA' and category eq 'Cloud Storage'". This query filters out applications that are not HIPAA compliant and belong to the Cloud Storage category, ensuring that only non-HIPAA compliant cloud storage applications are displayed in the results. This helps in identifying and blocking such applications as per the manager's request without affecting business or departmental applications. It aligns with Netskope's capabilities to enforce controls and restrictions on high-risk cloud services to help address HIPAA and HITECH compliance, as well as to audit suspected violations with a full cloud and web activity trail1.
The reference for constructing such queries can be found in Netskope's official documentation, which provides detailed information on filtering application data to manage compliance findings and view security posture compliance2. Additionally, Netskope's resources on HIPAA Cloud Compliance and Risk Insights can be used to understand the compliance and data center certifications related to HIPAA

NEW QUESTION: 29
You are asked to ensure that a Web application your company uses is both reachable and decrypted by Netskope. This application is served using HTTPS on port 6443. Netskope is configured with a default Cloud Firewall configuration and the steering configuration is set for All Traffic.
Which statement is correct in this scenario?
A. Create a Firewall App in Netskope along with the corresponding Real-time Protection policy to allow the traffic.
B. Nothing is required since Netskope is steering all traffic.
C. Enable "Steer non-standard ports" in the steering configuration and add the domain and port as a new non-standard port
D. Enable "Steer non-standard ports" in the steering configuration and create a corresponding Real-time Protection policy to allow the traffic

Answer: C (LEAVE A REPLY)
To ensure that the web application using HTTPS on port 6443 is both reachable and decrypted by Netskope, the correct action is toenable "Steer non-standard ports" in the steering configuration and add the domain and port as a new non-standard port. This is because Netskope's default configuration steers standard HTTP
/HTTPS traffic, typically on ports 80 and 443.Since port 6443 is a non-standard port for HTTPS traffic, it requires explicit configuration to be steered through Netskope1.
The process for configuring non-standard ports in Netskope is detailed in the Netskope Knowledge Portal, which provides step-by-step instructions on how to steer HTTP(S) traffic over non-standard ports1. This includes adding the specific non-standard port number in the steering configuration to ensure that traffic to and from that port is properly handled by Netskope.

NEW QUESTION: 30
You created a Real-time Protection policy that blocks all activities to non-corporate S3 buckets, but determine that the policy is too restrictive. Specifically, users are complaining that normal websites have stopped rendering properly.
How would you solve this problem?
A. Create a Real-time Protection policy to allow the Browse activity to the Amazon S3 application.
B. Create a Real-time Protection policy to allow the Browse activity to the Cloud Storage category
C. Create a Real-time Protection policy to allow the Download activity to the Cloud Storage category
D. Create a Real-time Protection policy to allow the Download activity to the Amazon S3 application
Answer: B (LEAVE A REPLY)
To solve the problem of normal websites not rendering properly due to a Real-time Protection policy that blocks all activities to non-corporate S3 buckets, the best solution is to create a Real-time Protection policy to allow the Browse activity to the Cloud Storage category. This approach will enable users to view content from various cloud storage services, including Amazon S3, without allowing full access to non-corporate S3 buckets. It's a more granular and less restrictive policy that allows necessary browsing activities while still maintaining control over the upload and download activities to non-corporate buckets1.
The Netskope Knowledge Portal provides information on how to configure Real-time Protection policies, including how to set up policies that allow certain activities while blocking others1. Additionally, the Netskope Community Forum offers insights into best practices for policy configuration to avoid overly restrictive rules that can impact normal web browsing

NEW QUESTION: 31
A company has deployed Explicit Proxy over Tunnel (EPoT) for their VDI users They have configured Forward Proxy authentication using Okta Universal Directory They have also configured a number of Real- time Protection policies that block access to different Web categories for different AD groups so. for example, marketing users are blocked from accessing

gambling sites. During User Acceptance Testing, they see inconsistent results where sometimes marketing users are able to access gambling sites and sometimes they are blocked as expected They are seeing this inconsistency based on who logs into the VDI server first.
What is causing this behavior?
A. Forward Proxy is not configured to use the Cookie Surrogate
B. Forward Proxy is not configured to use the IP Surrogate
C. Forward Proxy authentication is configured but not enabled.
D. Forward Proxy is configured to use the Cookie Surrogate
Answer: A (LEAVE A REPLY)
* The inconsistent results observed during User Acceptance Testing (where marketing users sometimes access gambling sites and sometimes are blocked) are likely due to the configuration of the Forward Proxy.
* Cookie Surrogate: The Cookie Surrogate is a mechanism used in Forward Proxy deployments to maintain user context across multiple requests. It ensures that user-specific policies are consistently applied even when multiple users share the same IP address (common in VDI environments).
* Issue: If the Forward Proxy is not configured to use the Cookie Surrogate, it may lead to inconsistent behavior. When different users log into the VDI server, their requests may not be associated with their specific user context, resulting in varying policy enforcement.
* Solution: Ensure that the Forward Proxy is properly configured to use the Cookie Surrogate, allowing consistent policy enforcement based on individual user identities. References:
* Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training
* Netskope Security Cloud Introductory Online Technical Training
* Netskope Architectural Advantage Features

NEW QUESTION: 32
You recently began deploying Netskope at your company. You are steering all traffic, but you discover that the Real-time Protection policies you created to protect Microsoft OneDrive are not being enforced.
Which default setting in the UI would you change to solve this problem?
A. Disable the default Microsoft appsuite SSL rule.
B. Disable the default certificate-pinned application

C. Remove the default steering exception for domains.
D. Remove the default steering exception for Cloud Storage.
Answer: C (LEAVE A REPLY)
When deploying Netskope and steering all traffic, if you find that the Real-time Protection policies for Microsoft OneDrive are not being enforced, the likely issue is with the default steering exceptions. To resolve this, you should remove the default steering exception for domains . This is because the default exceptions may include domains related to Microsoft services, which could prevent the Real-time Protection policies from being applied to traffic directed towards OneDrive. By removing these exceptions, you ensure that all traffic, including that to OneDrive, is subject to the policies you have set up.
This recommendation is based on best practices for configuring Real-time Protection policies in Netskope, as outlined in their documentation, which suggests that exceptions should be carefully managed to ensure that security policies are enforced as intended

NEW QUESTION: 33
You are assisting your network administrator to troubleshoot an issue with client-based NPA.
In the Netskope UI, what information do you need from the administrator to run the NPA troubleshooter for this user? (Choose two.)
A. User & Device
B. Private App Name
C. Private App ID
D. Publisher Name
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 34
Given the following:

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

Which result does this Skope IT query provide?
A. The query returns all events of user@company.com downloading or uploading to or from the site
'Amazon S3" using the Netskope Client.
B. The query returns all events of an IP address downloading or uploading to or from Amazon S3 using the Netskope Client.
C. The query returns all events of everyone except user@company.com downloading or uploading to or from the site "Amazon S3" using the Netskope Client.
D. The query returns all events of user@company.com downloading or uploading to or from the application "Amazon S3" using the Netskope Client.
Answer: A (LEAVE A REPLY)
* The given Skope IT query specifies the following conditions:
* User equals 'user@company.com'
* Access method equals 'Client'

* Activity equals 'Download' or 'Upload'
* Site equals 'Amazon S3'
* The query combines these conditions using logical operators (AND and OR).
* The result of this query will include all events where the specified user ('user@company.com') is either downloading or uploading data to or from the site 'Amazon S3' using the Netskope Client.
* It does not include events related to other users or IP addresses. References:
* Netskope Security Cloud Introductory Online Technical Training
* Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training

NEW QUESTION: 35
You want customers to configure Real-time Protection policies. In which order should the policies be placed in this scenario?
A. Threat, CASB, RBI, Web
B. RBI, CASB, Web, Threat
C. Threat, RBI, CASB, Web
D. CASB, RBI, Threat, Web
Answer: B (LEAVE A REPLY)
* When configuring Real-time Protection policies in Netskope, the recommended order is as follows:
* RBI (Risk-Based Index) Policies: These policies focus on risk assessment and prioritize actions based on risk scores. They help identify high-risk activities and users.
* CASB (Cloud Access Security Broker) Policies: These policies address cloud-specific security requirements, such as controlling access to cloud applications, enforcing data loss prevention (DLP) rules, and managing shadow IT.
* Web Policies: These policies deal with web traffic, including URL filtering, web categories, and threat prevention.
* Threat Policies: These policies focus on detecting and preventing threats, such as malware, phishing, and malicious URLs.
* Placing the policies in this order ensures that risk assessment and cloud-specific controls are applied before addressing web and threat-related issues. References:
* Netskope Security Cloud Introductory Online Technical Training
* Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training
* Netskope Certification Description
* Netskope Architectural Advantage Features

NEW QUESTION: 36
You are troubleshooting an issue with users who are unable to reach a financial SaaS application when their traffic passes through Netskope. You determine that this is because of IP restrictions in place with the SaaS vendor. You are unable to add Netskope's IP ranges at this time, but need to allow the traffic.
How would you allow this traffic?

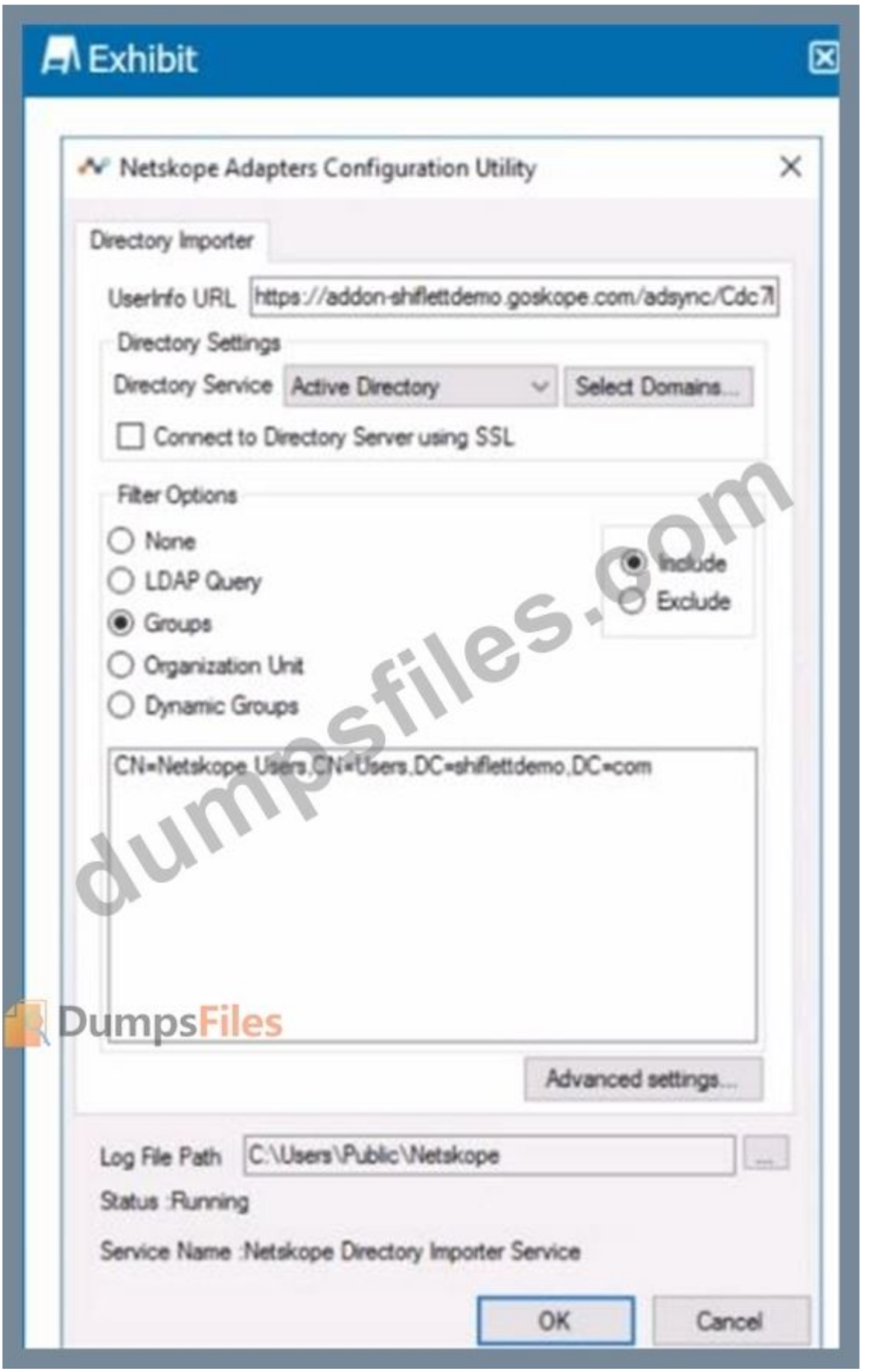
A. Use NPAto implement Source IP anchonng so the traffic will egress from the corporate data center.
B. Use Explicit Proxy Over Tunnel (EPoT) so the traffic will egress from the corporate data center.
C. Use Cloud Explicit Proxy so the traffic will egress from the corporate data center
D. Use an IPsec tunnel to forward traffic so it will egress from the corporate data center
Answer: C (LEAVE A REPLY)
To allow traffic to a financial SaaS application that is being blocked due to IP restrictions, the best option is to use Cloud Explicit Proxy. This method allows traffic to egress from the corporate data center without requiring Netskope's IP ranges to be added to the SaaS vendor's allowlist. By configuring an allowlist in the Cloud Explicit Proxy settings, you can add any source egress IP addresses for your on-premises users, and Netskope will allow the traffic from the added user and IP address without authenticating1.

NEW QUESTION: 37
You deployed IPsec tunnels to steer on-premises traffic to Netskope. You are now experiencing problems with an application that had previously been working. In an attempt to solve the issue, you create a Steering Exception in the Netskope tenant tor that application: however, the problems are still occurring Which statement is correct in this scenario?
A. You must create a private application to steer Web application traffic to Netskope over an IPsec tunnel.
B. Exceptions only work with IP address destinations
C. Steering bypasses for IPsec tunnels must be applied at your edge network device.
D. You must deploy a PAC file to ensure the traffic is bypassed pre-tunnel
Answer: C (LEAVE A REPLY)
In the scenario where you have deployed IPsec tunnels to steer on-premises traffic to Netskope and are experiencing issues with an application, the correct statement is C: Steering bypasses for IPsec tunnels must be applied at your edge network device. This means that to effectively bypass the steering for a specific application, the configuration must be done on the network device that is establishing the IPsec tunnel, such as a firewall or router. This device controls the traffic before it enters the tunnel, so applying the bypass there ensures that the application's traffic does not get directed through the tunnel and can reach its destination directly.

NEW QUESTION: 38
You successfully configured Advanced Analytics to identify policy violation trends Upon further investigation, you notice that the activity is NULL. Why is this happening in this scenario?
A. The SSPM policy was not configured during setup.
B. The REST API v1 token has expired.
C. A policy violation was identified using API Protection.
D. A user accessed a static Web page.
Answer: (SHOW ANSWER)

The reason for the activity being NULL in this scenario is likely because a user accessed a static Web page. In Netskope's Advanced Analytics, when the activity is reported as NULL, it often indicates that there was no dynamic interaction or transaction to record, which is typical when a static web page is accessed1. Static web pages do not generate the kind of events or activities that are tracked by policies, hence they appear as NULL in the activity field.

NEW QUESTION: 39
Review the exhibit.



You installed Directory Importer and configured it to import specific groups ot users into your Netskope tenant as shown in the exhibit. One hour after a new user has been added to the domain, the user still has not been provisioned to Netskope.

What are three potential reasons for this failure? (Choose three.)
A. Directory Importer does not support ongoing user syncs; you must manually provision the user.
B. The server that the Directory Importer is installed on is unable to reach Netskope's add-on endpomt.
C. The user is not a member of the group specified as a filter
D. Active Directory integration is not enabled on your tenant.
E. The default collection interval is 180 minutes, therefore a sync may not have run yet.
Answer: B,C,E (LEAVE A REPLY)
The three potential reasons for the failure of a new user not being provisioned to Netskope an hour after being added to the domain could be:
B . The server that the Directory Importer is installed on is unable to reach Netskope's add-on endpoint: If the server cannot connect to Netskope's endpoint, it cannot sync the user data. This could be due to network issues, incorrect configuration, or firewall restrictions1.
C . The user is not a member of the group specified as a filter: The Directory Importer may be configured to import users from specific groups only. If the new user is not a member of these groups, they will not be imported into Netskope1.
E . The default collection interval is 180 minutes, therefore a sync may not have run yet: The Directory Importer may be scheduled to sync every 180 minutes. If only an hour has passed, the sync process might not have occurred yet, and the user would not be provisioned until the next sync interval1.

NEW QUESTION: 40
A company has deployed Explicit Proxy over Tunnel (EPoT) for their VDI users They have configured Forward Proxy authentication using Okta Universal Directory They have also configured a number of Real-time Protection policies that block access to different Web categories for different AD groups so. for example, marketing users are blocked from accessing gambling sites. During User Acceptance Testing, they see inconsistent results where sometimes marketing users are able to access gambling sites and sometimes they are blocked as expected They are seeing this inconsistency based on who logs into the VDI server first.
What is causing this behavior?
A. Forward Proxy is not configured to use the Cookie Surrogate
B. Forward Proxy is not configured to use the IP Surrogate
C. Forward Proxy authentication is configured but not enabled.
D. Forward Proxy is configured to use the Cookie Surrogate
Answer: A (LEAVE A REPLY)
The inconsistent results observed during User Acceptance Testing (where marketing users sometimes access gambling sites and sometimes are blocked) are likely due to the configuration of the Forward Proxy.
Cookie Surrogate: The Cookie Surrogate is a mechanism used in Forward Proxy deployments to maintain user context across multiple requests. It ensures that user-specific policies are

consistently applied even when multiple users share the same IP address (common in VDI environments).
Issue: If the Forward Proxy is not configured to use the Cookie Surrogate, it may lead to inconsistent behavior. When different users log into the VDI server, their requests may not be associated with their specific user context, resulting in varying policy enforcement.
Solution: Ensure that the Forward Proxy is properly configured to use the Cookie Surrogate, allowing consistent policy enforcement based on individual user identities. Reference:
Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training Netskope Security Cloud Introductory Online Technical Training Netskope Architectural Advantage Features

NEW QUESTION: 41
You created a Real-time Protection policy that blocks all activities to non-corporate S3 buckets, but determine that the policy is too restrictive. Specifically, users are complaining that normal websites have stopped rendering properly.
How would you solve this problem?
A. Create a Real-time Protection policy to allow the Browse activity to the Amazon S3 application.
B. Create a Real-time Protection policy to allow the Browse activity to the Cloud Storage category
C. Create a Real-time Protection policy to allow the Download activity to the Cloud Storage category
D. Create a Real-time Protection policy to allow the Download activity to the Amazon S3 application
Answer: B (LEAVE A REPLY)
To solve the problem of normal websites not rendering properly due to a Real-time Protection policy that blocks all activities to non-corporate S3 buckets, the best solution is to create a Real-time Protection policy to allow the Browse activity to the Cloud Storage category. This approach will enable users to view content from various cloud storage services, including Amazon S3, without allowing full access to non-corporate S3 buckets. It's a more granular and less restrictive policy that allows necessary browsing activities while still maintaining control over the upload and download activities to non-corporate buckets1.

NEW QUESTION: 42
You are currently designing a policy for AWS S3 bucket scans with a custom DLP profile Which policy action(s) are available for this policy?
A. Alert, Quarantine. Block, User Notification
B. Alert, User Notification
C. Alert only
D. Alert, Quarantine
Answer: D (LEAVE A REPLY)
When designing a policy for AWS S3 bucket scans with a custom DLP profile in Netskope, the available policy actions are Alert and Quarantine. These actions allow you to be notified when a

policy violation occurs and to quarantine sensitive data to prevent potential data loss or exposure. The Alert action will notify the designated personnel or system when a match to the DLP profile is found during the scan. The Quarantine action will move the offending file to a secure location where it can be reviewed and dealt with appropriately1.

NEW QUESTION: 43
A company needs to block access to their instance of Microsoft 365 from unmanaged devices. They have configured Reverse Proxy and have also created a policy that blocks login activity for the AD group "marketing-users" for the Reverse Proxy access method. During UAT testing, they notice that access from unmanaged devices to Microsoft 365 is not blocked for marketing users. What is causing this issue?
A. There is a missing group name in the SAML response.
B. The username in the name ID field is not in the format of the e-mail address.
C. There is an invalid certificate in the SAML response.
D. The username in the name ID field does not have the "marketing-users" group name.
Answer: A (LEAVE A REPLY)
The issue is likely caused by a missing group name in the SAML response (A). When access to Microsoft 365 from unmanaged devices is not blocked as expected, despite having a policy in place, it often indicates that the SAML assertion is not correctly identifying the user as a member of the restricted group. In this case, the "marketing-users" group name should be present in the SAML response to enforce the policy that blocks login activity for this group. If the group name is missing, the policy will not apply, and users will not be blocked as intended.

NEW QUESTION: 44
You deployed the Netskope Client for Web steering in a large enterprise with dynamic steering. The steering configuration includes a bypass rule for an application that is IP restricted. What is the source IP for traffic to this application when the user is on-premises at the enterprise?
A. Loopback IPv4
B. Netskope data plane gateway IPv4
C. Enterprise Egress IPv4
D. DHCP assigned RFC1918 IPv4
Answer: C (LEAVE A REPLY)
* When a user is on-premises at the enterprise and accesses an application that is IP restricted, the source IP for traffic to this application is the Enterprise Egress IPv4 address.
* The Enterprise Egress IP represents the external IP address of the enterprise network as seen by external services or applications.
* This IP address is used for communication between the user's device and external resources, including applications that are IP restricted. References:
* The answer is based on general knowledge of networking concepts and how IP addresses are used in enterprise environments.

NEW QUESTION: 45
Review the exhibit.

You are asked to integrate Netskope with Crowdstrike EDR. You added the Remediation profile shown in the exhibit.
Which action will this remediation profile take?
A. The endpoint will be isolated.
B. The malware hash will be added as an IOC in Crowdstrike.
C. The malware will be quarantined.
D. The malware hash will be added as an IOC in Netskope.
Answer: B (LEAVE A REPLY)
In the exhibit, the Malware Remediation Profile is configured with:
* Connected EDR Server: crowdstrike-demo
* Selected Action: Add to watchlist/blocklist
* Not Selected: Isolate, Alert
When using CrowdStrike as an EDR integration, the action "Add to watchlist/blocklist" corresponds to:
Adding the malware hash as an Indicator of Compromise (IOC) inside CrowdStrike Falcon. CrowdStrike will then block or flag that hash across all managed endpoints, depending on its local policies.

NEW QUESTION: 46
Users in your network are attempting to reach a website that has a self-signed certificate using a GRE tunnel to Netskope. They are currently being blocked by Netskope with an SSL error. How would you allow this traffic?

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

NEW QUESTION: 47
Review the exhibit.

You installed Directory Importer and configured it to import specific groups ot users into your Netskope tenant as shown in the exhibit. One hour after a new user has been added to the domain, the user still has not been provisioned to Netskope.
What are three potential reasons for this failure? (Choose three.)
A. The default collection interval is 180 minutes, therefore a sync may not have run yet.
B. Directory Importer does not support ongoing user syncs; you must manually provision the user.
C. Active Directory integration is not enabled on your tenant.
D. The server that the Directory Importer is installed on is unable to reach Netskope's add-on endpoint.
E. The user is not a member of the group specified as a filter
Answer: C,D,E (LEAVE A REPLY)

NEW QUESTION: 48
Your company just had a new Netskope tenant provisioned and you are asked to create a secure tenant configuration. In this scenario, which two default settings should you change? {Choose two.)
A. Change Safe Search to Disabled
B. Change Untrusted Root Certificate to Block.
C. Change the No SNI setting to Block.
D. Change "Disallow concurrent logins by an Admin" to Enabled.
Answer: B,D (LEAVE A REPLY)
For a new Netskope tenant provisioned, to create a secure tenant configuration, you should consider changing the following default settings:
* B. Change Untrusted Root Certificate to Block: This setting will ensure that any traffic coming from an untrusted root certificate is blocked, which is a critical security measure to prevent man-in-the-middle attacks and other types of cyber threats1.
* D. Change "Disallow concurrent logins by an Admin" to Enabled: This setting will prevent multiple concurrent logins by the same admin account, which is an important security control to mitigate the risk of unauthorized access.If an admin's credentials are compromised, this setting will help limit the potential damage by ensuring that only one session can be active at a time1.
These changes are part of the recommended security hardening guidelines for Netskope tenants to enhance the overall security posture of the tenant environment.
The recommendations for changing default settings for a secure tenant configuration are based on Netskope' s security hardening guidelines, which provide detailed instructions on how to enhance the security of Netskope products and components deployed in customer environments1.

NEW QUESTION: 49
You want customers to configure Real-time Protection policies. In which order should the policies be placed in this scenario?
A. Threat, CASB, RBI, Web

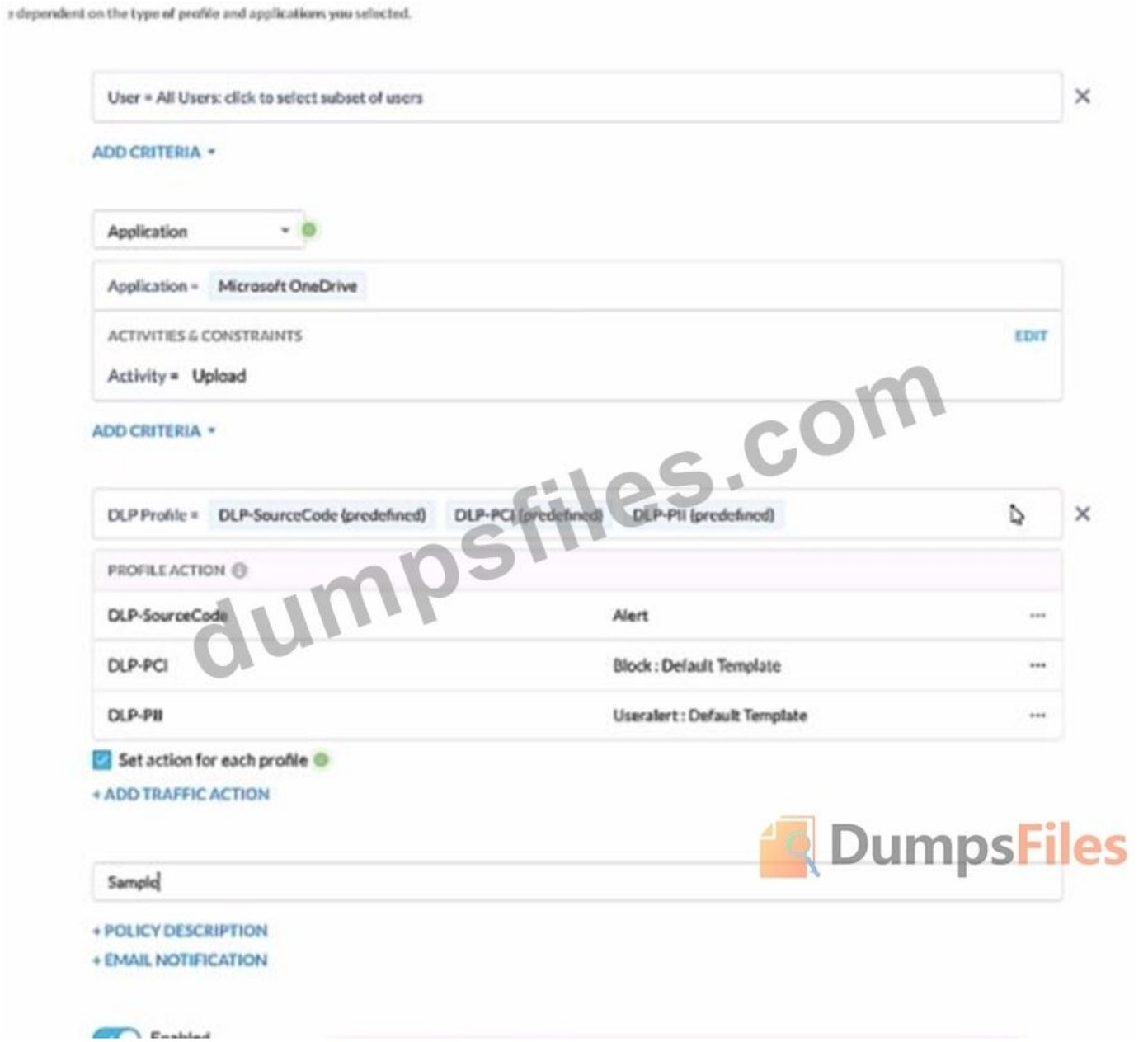
B. CASB, RBI, Threat, Web
C. Threat, RBI, CASB, Web
D. RBI, CASB, Web, Threat
Answer: C (LEAVE A REPLY)

NEW QUESTION: 50
You want to integrate with a third-party DLP engine that requires ICAP. In this scenario, which Netskope platform component must be configured?
A. On-Premises Log Parser (OPLP)
B. Secure Forwarder
C. Netskope Cloud Exchange
D. Netskope Adapter
Answer: B (LEAVE A REPLY)
To integrate Netskope with a third-party DLP engine using ICAP, you must configure the Netskope Secure Forwarder.
Secure Forwarder is the only Netskope component that supports:
* ICAP communication
* Forwarding inline web traffic to external DLP engines
* Bidirectional ICAP requests/responses (REQMOD/RESPMOD)
This allows Netskope to send inspected content to your on-prem or third-party DLP appliance for additional scanning.
Why the other options are incorrect
* A. On-Premises Log Parser (OPLP)Used for ingesting logs into Netskope - not for ICAP or traffic processing.
* C. Netskope Cloud ExchangeUsed for integrations with SIEM, SOAR, ticketing, threat intel - not for inline DLP.
* D. Netskope AdapterUsed mainly for SSPM/API integrations - not relevant for ICAP or external DLP engines.

NEW QUESTION: 51
Your customer is currently using Directory Importer with Active Directory (AD) to provision users to Nelskope. They have recently acquired three new companies (A. B. and C) and want to onboard users from the companies onto the NetsKope platform. Information about the companies is shown below.
- Company A uses Active Directory.
-- Company B uses Azure AD.
-- Company C uses Okta Universal Directory.
Which statement is correct in this scenario?
A. Users from Company B and Company C cannot be provisioned because the customer is already using AD Importer.

B. Either Company B or Company C users cannot be provisioned because integration with only one SCIM solution is allowed.
C. Users from Companies A. B, and C can be provisioned to Netskope by deploying additional AD Importers and integrating more than one SCIM solution.
D. Company A users cannot be provisioned to Netskope because the customer is already using AD Importer to import users from another Active Directory environment.
Answer: C (LEAVE A REPLY)
Users from Companies A, B, and C can indeed be provisioned to Netskope. Company A, which uses Active Directory, can continue to use the existing AD Importer. For Company B that uses Azure AD and Company C that uses Okta Universal Directory, integration with SCIM (System for Cross-domain Identity Management) solutions is possible.Netskope supports provisioning users from multiple directories, including Active Directory and cloud-based identity providers like Azure AD and Okta, by using additional AD Importers and integrating more than one SCIM solution12. The correct approach for provisioning users from different companies that use various directory services is supported by Netskope's capabilities to integrate with multiple identity providers and directory services, as outlined in their documentation and community resources12.

NEW QUESTION: 52
Review the exhibit.



A user has attempted to upload a file to Microsoft OneDrive that contains source code with PII and PCI data.

Referring to the exhibit, which statement Is correct?

A. The user will be blocked and a single Incident will be generated referencing the DLP-PCI profile.

B. The user will be blocked and a single Incident will be generated referencing all of the matching DLP profiles

C. The user will be blocked and a separate incident will be generated for each of the matching DLP profiles.

D. The user will be alerted and a single incident will be generated referencing the DLP-PII profile.

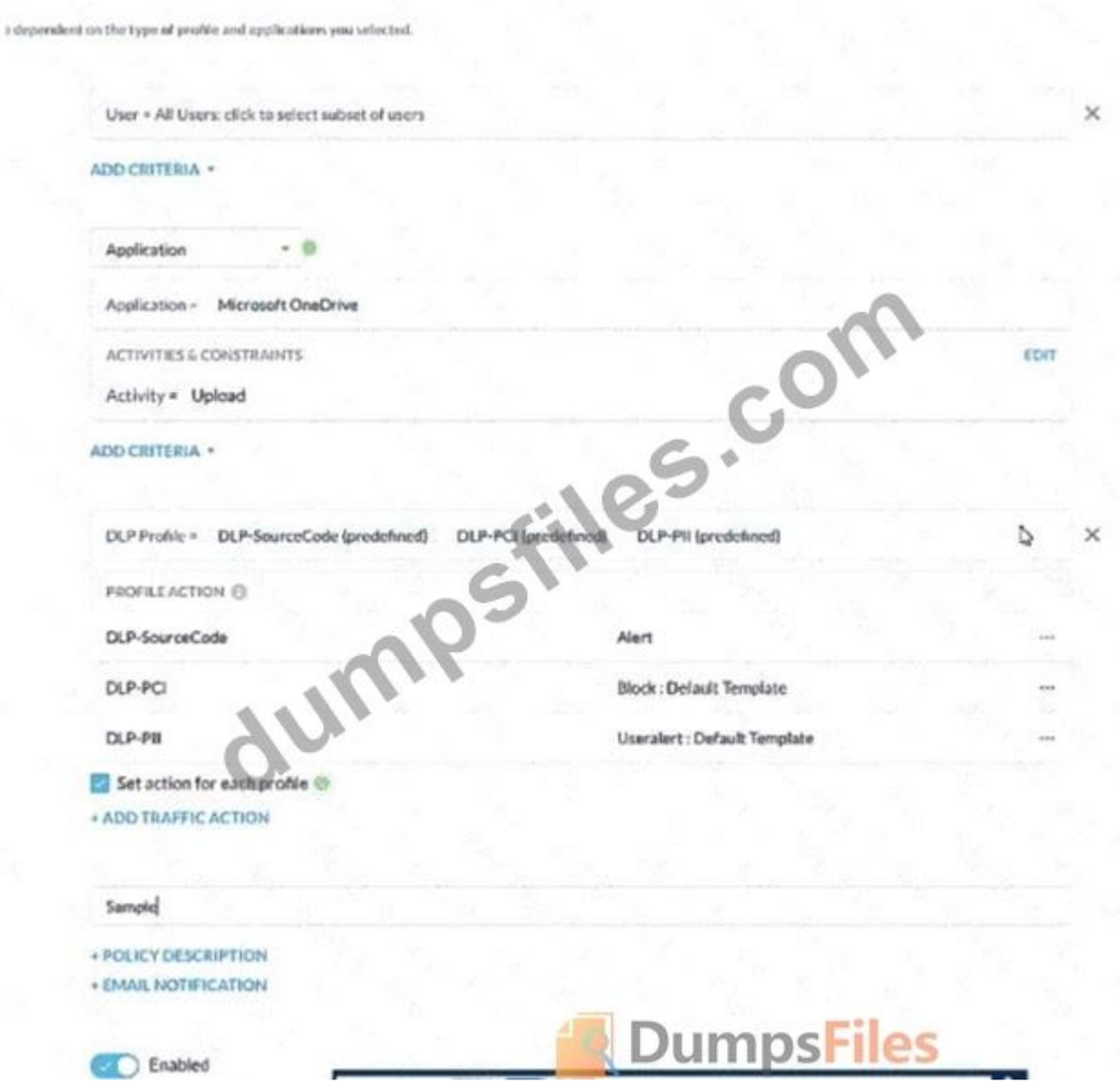
Answer: (SHOW ANSWER)

In the given scenario, a user is attempting to upload a file containing sensitive PII and PCI data to Microsoft OneDrive. The Netskope Security Cloud provides real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Based

on the exhibit provided, different DLP (Data Loss Prevention) profiles are triggered - DLP-SourceCode, DLP-PCI, and DLP-PII. Each of these profiles has specific actions associated with them; for instance, an alert is generated for Source Code while blocking actions are initiated for PCI and PII data. Since multiple DLP profiles are triggered due to the sensitive nature of the content in the file being uploaded, separate incidents will be generated for each matching profile ensuring comprehensive security coverage and incident reporting.
Reference:
Netskope Cloud Security
Netskope Resources
Netskope Documentation

NEW QUESTION: 53
You want to enable the Netskope Client to automatically determine whether it is on-premises or off-premises. Which two options in the Netskope UI would you use to accomplish this task? (Choose two.)
A. the All Traffic option in the Steering Configuration section of the UI
B. the New Exception option in the Traffic Steering options of the UI
C. the Enable Dynamic Steering option in the Steering Configuration section of the UI
D. the On Premises Detection option under the Client Configuration section of the UI
Answer: (SHOW ANSWER)
To enable the Netskope Client to automatically determine whether it is on-premises or off-premises, you can use the following options in the Netskope UI:
Enable Dynamic Steering:
This option is available in the Steering Configuration section of the UI.
By enabling dynamic steering, the Netskope Client can intelligently determine the appropriate data plane (on-premises or cloud) based on the user's location and network conditions.
It ensures that traffic is directed to the optimal data plane for improved performance and security.
Reference:
On Premises Detection:
This option is available under the Client Configuration section of the UI.
By configuring on-premises detection, the Netskope Client can identify whether it is connected to the local network (on-premises) or accessing resources from outside (off-premises).
It helps in applying relevant policies and steering traffic accordingly.

NEW QUESTION: 54
Review the exhibit.



A user has attempted to upload a file to Microsoft OneDrive that contains source code with PII and PCI data.

Referring to the exhibit, which statement Is correct?

A. The user will be blocked and a single Incident will be generated referencing all of the matching DLP profiles

B. The user will be blocked and a single Incident will be generated referencing the DLP-PCI profile.

C. The user will be alerted and a single incident will be generated referencing the DLP-PII profile.

D. The user will be blocked and a separate incident will be generated for each of the matching DLP profiles.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 55

What is a Fast Scan component of Netskope Threat Detection?

A. Heuristic Analysis

B. Machine Learning

C. Dynamic Analysis
D. Statical Analysis
Answer: (SHOW ANSWER)
The Fast Scan component of Netskope Threat Detection utilizes Machine Learning to quickly detect and block malware in real-time. This is part of Netskope's multi-layered security approach, which includes various engines to defend against a wide range of threats. The Fast Scan capability specifically leverages machine learning-based detection for rapid analysis and response to potential threats1.