www.atmicnetworks.com

ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

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

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

www.atmicnetworks.com

Question: 1

You are asked to create a customized restricted administrator role in your Netskope tenant for a newly hired employee. Which two statements are correct in this scenario? (Choose two.)

A. An admin role prevents admins from downloading and viewing file content by default.
B. The scope of the data shown in the UI can be restricted to specific events.
C. All role privileges default to Read Only for all functional areas.
D. Obfuscation can be applied to all functional areas.

Answer: AC

Explanation:

Admin Role and File Content Viewing: By default, an admin role does not prevent admins from downloading and viewing file content. Admins have access to view and download file content unless specific restrictions are applied.
Role Privileges Default to Read Only: All role privileges in Netskope default to Read Only for all functional areas. This means that admins can view information but cannot make changes unless explicitly granted additional permissions.
Obfuscation: Obfuscation can be applied to specific functional areas, but it is not a default behavior for all areas.
Reference:
Netskope Security Cloud Introductory Online Technical Training
Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training

Question: 2

You are deploying the Netskope Client to Windows devices. The following command line would be used to install the client MSI file:

M1«J« *H* IKllmlJil tskw-Utes- hutKbwp :i»:d^r«HrcMi!lj I li»t*Uacd*«nf tuHtcMtijl^tiai-SMtiv!; tall-etei F.H i J (»y t o^dttwon n(!|

In this scenario, what is <token> referring to in the command line?

A. a Netskope user identifier
B. the Netskope organization ID
C. the URL of the IdP used to authenticate the users
D. a private token given to you by the SCCM administrator

Answer: B

Explanation:

In the context of deploying the Netskope Client to Windows devices, <token> in the command line refers to the Netskope organization ID. This is a unique identifier associated with your organization's account within the Netskope security cloud. It is used during the installation process to ensure that client devices are registered and managed under the correct organizational account, enabling appropriate security policies and configurations to be applied. Reference: The answer can be inferred from general knowledge about installing software clients and isn't directly available on Netskope's official resources.

Question: 3

Given the following:

uses q 'uEer^iM^ary.ciM' tai •cc«33_nrur_ 1 «q 'CliaU* end activity sq 'HKMUoad* x activity aq ♦tyliiar and Uta eq 'AMLSCHL fP **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

Explanation:

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

Question: 4

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

Explanation:

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. Reference:
Netskope Security Cloud Introductory Online Technical Training
Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training
Netskope Certification Description
Netskope Architectural Advantage Features

Question: 5

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

Explanation:

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

www.atmicnetworks.com

Question: 6

Review the exhibit.

You are the proxy administrator for a medical devices company. You recently changed a pilot group of users from cloud app steering to all Web traffic. Pilot group users have started to report that they receive the error shown in the exhibit when attempting to access the company intranet site that is publicly available. During troubleshooting, you realize that this site uses your company's internal certificate authority for SSL certificates.
Which three statements describe ways to solve this issue? (Choose three.)

A. Import the root certificate for your internal certificate authority into Netskope.
B. Bypass SSL inspection for the affected site(s).
C. Create a Real-time Protection policy to allow access.
D. Change the SSL Error Settings from Block to Bypass in the Netskope tenant.
E. Instruct the user to proceed past the error message

Answer: ABD

Explanation:

A . Import the root certificate for your internal certificate authority into Netskope:
This step ensures that Netskope recognizes and trusts SSL certificates issued by your company's internal certificate authority. By importing the root certificate, you enable proper SSL inspection and validation for internal sites.
B . Bypass SSL inspection for the affected site(s):
Since the intranet site uses your company's internal certificate authority, bypassing SSL inspection for this specific site allows users to access it without encountering SSL errors.
D . Change the SSL Error Settings from Block to Bypass in the Netskope tenant:
Adjusting the SSL Error Settings to "Bypass" allows users to proceed past SSL errors, including selfsigned certificate errors. This ensures uninterrupted access to the intranet site. Reference: Netskope Security Cloud Introductory Online Technical Training
Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training
Netskope Cloud Security Certification Program

Question: 7

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

Explanation:

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."

Question: 8

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

Explanation:

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. Reference:

The answer is based on general knowledge of networking concepts and how IP addresses are used in enterprise environments.

Question: 9

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

A. Create a new dashboard from scratch that mimics the Netskope dashboard you want to use.
B. Copy the dashboard into your Group or Personal folders and schedule from these folders.
C. Ask Netskope Support to provide the dashboard and import into your Personal folder.
D. Download the dashboard you want and Import from File into your Group or Personal folder.

Answer: D

Explanation:

To retain the original dashboard without automatic updates due to improvements made by Netskope, you can

www.atmicnetworks.com

download the desired dashboard and then import it from a file into your Group or Personal folder.

This approach ensures that you have a static version of the dashboard that won't be affected by future changes or enhancements. Reference:

The answer is based on general knowledge of dashboard management and customization within Netskope.

Question: 10

You have multiple networking clients running on an endpoint and client connectivity is a concern.

You are configuring co-existence with a VPN solution in this scenario, what is recommended to prevent potential routing issues?

A. Configure the VPN to split tunnel traffic by adding the Netskope IP and Google DNS ranges and set to Exclude in the VPN configuration.

B. Modify the VPN to operate in full tunnel mode at Layer 3. so that the Netskope agent will always see the traffic first.

C. Configure the VPN to full tunnel traffic and add an SSL Do Not Decrypt policy to the VPN configuration for all Netskope traffic.

D. Configure a Network Location with the VPN IP ranges and add it as a Steering Configuration exception.

Answer: B

Explanation:

To prevent potential routing issues and ensure that the Netskope agent consistently sees the traffic first, it is recommended to modify the VPN to operate in full tunnel mode at Layer 3.

In full tunnel mode, all traffic from the endpoint is routed through the VPN, including traffic destined for Netskope. This ensures that the Netskope agent can inspect and apply policies to all traffic, regardless of the destination.

Layer 3 full tunnel mode provides better visibility and control over the traffic flow, reducing the risk of routing conflicts or bypassing the Netskope inspection. Reference:

The answer is based on general knowledge of VPN configurations and their impact on traffic routing.

www.atmicnetworks.com

Question: 12

Users at your company's branch office in San Francisco report that their clients are connecting, but websites and SaaS applications are slow When troubleshooting, you notice that the users are connected to a Netskope data plane in New York where your company's headquarters is located. What is a valid reason for this behavior?

A. The Netskope Client's on-premises detection check failed.
B. The Netskope Client's default DNS over HTTPS call is failing.
C. The closest Netskope data plane to San Francisco is unavailable.
D. The Netskope Client's DNS call to Secure Forwarder is failing

Answer: C

Explanation:

The reported issue of slow website and SaaS application access for users in the San Francisco branch office, despite being connected to a Netskope data plane in New York, can be attributed to the geographical distance between the user location and the data plane. The Netskope Security Cloud operates through a distributed network of data planes strategically placed in various regions. When users connect to a data plane that is geographically distant, it can result in latency due to longer network traversal times. In this case, the closest Netskope data plane to San Francisco might be unavailable or experiencing high load, leading to performance issues. To address this, consider optimizing data plane selection based on proximity to the user location or investigating any data plane availability or performance issues.

Reference:
Netskope Cloud Security
Netskope Resources
Netskope Documentation

Question: 13

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

Explanation:

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

www.atmicnetworks.com

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

Reference:

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.

Question: 14

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: C, D

Explanation:

To enable the Netskope Client to automatically determine whether it is on-premises or off-premises, you can use the following options in the Netskope UI:

Enable Dynamic Steering:

This option is available in 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: Netskope Documentation on Dynamic Steering

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.

Reference: Netskope Documentation on Client Configuration

Question: 15

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

Which configuration satisfies these requirements?

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

Answer: C

Explanation:

To allow access from company-managed devices running the Netskope Client to only Amazon S3 buckets owned by the organization, the following configuration satisfies the requirements: Steering Configuration:
Policy Type: Real-time Protection
Constraint: Storage
Bucket Condition: Bucket Does Match -ALLAccounts
Action: Allow

By configuring the policy to allow traffic from company-managed devices (Netskope Clients) to Amazon S3 buckets, the organization ensures that only buckets owned by the organization are accessible.
The -ALLAccounts condition ensures that both existing and future buckets are allowed.
This configuration aligns with the requirement to allow access to organization-owned buckets while blocking access to other buckets.
Reference:
Netskope Cloud Security
Netskope Solution Brief
Netskope Community

Question: 16

Your organization's software deployment team did the initial install of the Netskope Client with SCCM. As the Netskope administrator, you will be responsible for all up-to-date upgrades of the client.
Which two actions would be required to accomplish this task9 (Choose two.)

A. In the Client Configuration, set Upgrade Client Automatically to Latest Release.
B. Set the installmode-IDP flag during the original Install.
C. Set the autoupdate-on flag during the original Install.
D. In the Client Configuration, set Upgrade Client Automatically to Specific Golden Release.

Answer: AC

Explanation:

To ensure that the Netskope Client is always up-to-date with the latest upgrades, two actions are required. First, in the Client Configuration, the administrator should set the option to Upgrade Client Automatically to Latest Release. This setting ensures that the client will automatically update to the most recent version available. Second, during the original installation of the Netskope Client, the autoupdate-on flag should be set. This flag enables the auto-update feature, allowing the client to receive and apply updates as they are released.

Reference: The information is based on the Netskope Client deployment options and upgrade process as detailed in the Netskope Knowledge Portal

Question: 17

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

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

Answer: AB

Explanation:

In the scenario where users are unable to access an application through Netskope Private Access, and after verifying that the Real-time Protection policy allows access, the application is steered for

the users, and it is reachable from internal machines, the next step is to verify the application's reachability through the Netskope Publisher. The two tools in the Netskope UI that would be used to accomplish this task are:

A . Reachability Via Publisher in the App Definitions page - This tool allows you to check if the application is reachable through the configured Publishers. It is essential to ensure that the application's connectivity is intact and that there are no issues with the Publishers themselves.

B . Troubleshooter tool in the App Definitions page - The Troubleshooter tool can help diagnose and resolve issues related to application reachability. It provides insights into potential problems and offers guidance on how to fix them.

These tools are designed to assist in troubleshooting and ensuring that applications are accessible through Netskope Private Access.

Reference: The explanation is based on the standard procedures for managing private applications and troubleshooting within the Netskope Private Access environment as outlined in the Netskope Knowledge Portal

Question: 18

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: D

Explanation:

When integrating a third-party Data Loss Prevention (DLP) engine that requires ICAP, the Netskope platform component that must be configured is the Netskope Adapter. The Netskope Adapter is designed to facilitate the integration of Netskope with various third-party tools and services, including DLP engines that use ICAP for communication. By configuring the Netskope Adapter, you can ensure that the third-party DLP engine can communicate effectively with the Netskope platform to provide comprehensive data protection.
Reference: This information is based on the integration capabilities of the Netskope platform, which includes the use of Netskope Adapters for third-party integrations as detailed in the Netskope Knowledge Portal1 and the Netskope Data Loss Prevention (DLP) documentation2

Question: 19

Your Netskope Client tunnel has connected to Netskope; however, the user is not receiving any steering or client configuration updates What would cause this issue?

A. The client is unable to establish communication to add-on-[tenantl.goskope.com.
B. The client is unable to establish communication to gateway-(tenant|.goskope.com.
C. The Netskope Client service is not running.
D. An invalid steering exception was created in the tenant

Answer: C

Explanation:

When the Netskope Client service is not running, it cannot execute the necessary processes to receive steering or client configuration updates. The service must be active to establish communication with the Netskope cloud and apply the configurations and policies defined by the administrator.
Reference: This information aligns with the Netskope Cloud Security Architect learning objectives and documents, which emphasize the importance of running client services for proper communication and functionality

Question: 20

You built a number of DLP profiles for different sensitive data types. If a file contains any of this sensitive data, you want to take the most restrictive policy action but also create incident details for all matching profiles.
Which statement is correct in this scenario?

A. Create a Real-time Protection policy for each DLP profile; each matched profile will generate a unique DLP incident.
B. Create a Real-time Protection policy for each DLP profile; all matched profiles will show up in a single DLP incident
C. Create a single Real-time Protection policy and include all of the DLP profiles; each matched profile will generate a unique DLP incident
D. Create a single Real-time Protection policy and include all of the DLP profiles; all matched profiles will show up in a single DLP incident.

Answer: D

Explanation:

When configuring a Real-time Protection policy with multiple DLP profiles, if the content matches multiple profiles, the policy performs the most restrictive action associated with the DLP profiles that match for that policy. The resulting incident lists all the profiles that matched along with their corresponding forensic information. This means that even though the most restrictive action is taken, details for all matching profiles are created and included in a single DLP incident12.
Reference: The explanation is based on the best practices and detailed descriptions provided in the Netskope Knowledge Portal and Community discussions, which outline the process of handling multiple DLP profile matches within a single Real-time Protection policy

Question: 21

You are consuming Audit Reports as part of a Salesforce API integration. Someone has made a change to a Salesforce account record field that should not have been made and you are asked to verify the previous value of the structured data field. You have the approximate date and time of the change, user information, and the new field value.
How would you accomplish this task?

A. Create a classic report and apply a query that filters on the changed field value.
B. Use the Application Events Data Collection within Advanced Analytics and filter on the changed field value.
C. Query Skope IT Page Events and look for the specific Page URL that was called under the Application section.
D. Query Skope IT for an Access Method of API Connector and search Application Event Details for the Old Value field using the User details and Edit Activity.

Answer: D

Explanation:

To verify the previous value of a structured data field in Salesforce after an unauthorized change, you would use Skope IT with an Access Method of API Connector. This method allows you to search the Application Event Details for the 'Old Value' field. By filtering with the user details and the edit activity, you can pinpoint the exact change and retrieve the original value of the field.
Reference: The approach is consistent with the Netskope Cloud Security Architect's guidelines for using API Data Protection with Salesforce. The documentation provides a detailed procedure for configuring Salesforce for API Data Protection, which includes the use of Netskope Audit Reports and the ability to track changes through the 'Old Value' field

Question: 22

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

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

Answer: A

Explanation:

Network Steering in Digital Experience Management is the appropriate Netskope monitoring tool for this scenario. It allows the Network Operations Center (NOC) to quickly view the status of the tunnels and provides an easy way to visualize the locations of the tunnels. This tool is designed to give a clear overview of network health and performance, which is essential for managing global connectivity and ensuring the reliability of the service.

Reference: The use of Network Steering in Digital Experience Management for monitoring tunnel status and location visualization is supported by Netskope's documentation on secure web gateway use cases and best practices for deployment and validation of IPSec/GRE tunnels

Question: 23

What is a Fast Scan component of Netskope Threat Detection?

A. Heuristic Analysis B. Machine Learning C. Dynamic Analysis D. Statical Analysis

Answer: B

Explanation:

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.

Reference: 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

Question: 24

You are architecting a Netskope steering configuration for devices that are not owned by the organization The users could be either on-premises or off-premises and the architecture requires that traffic destined to the company's instance of Microsoft 365 be steered to Netskope for inspection.
How would you achieve this scenario from a steering perspective?

A. Use IPsec and GRE tunnels.
B. Use reverse proxy.
C. Use explicit proxy and the Netskope Client
D. Use DPoP and Secure Forwarder

Answer: C

Explanation:

For devices not owned by the organization, using an explicit proxy along with the Netskope Client is the best approach to steer traffic for inspection. This method allows for granular control over the traffic, ensuring that only the traffic destined for the company's instance of Microsoft 365 is inspected by Netskope. The explicit proxy configuration can be applied regardless of whether the users are on-premises or off-premises, providing a

consistent steering mechanism for all users. Reference: The steering configuration for non-owned devices and the use of explicit proxy in conjunction with the Netskope Client are detailed in the Netskope Knowledge Portal. The portal provides guidelines on how to set up steering configurations to direct traffic from end users to the Netskope Cloud for real-time analysis, which is applicable for both managed and unmanaged devices1

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

Explanation:

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

Question: 26

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

Explanation:

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.

Reference: 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

Question: 27

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: ABD

Explanation:

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.

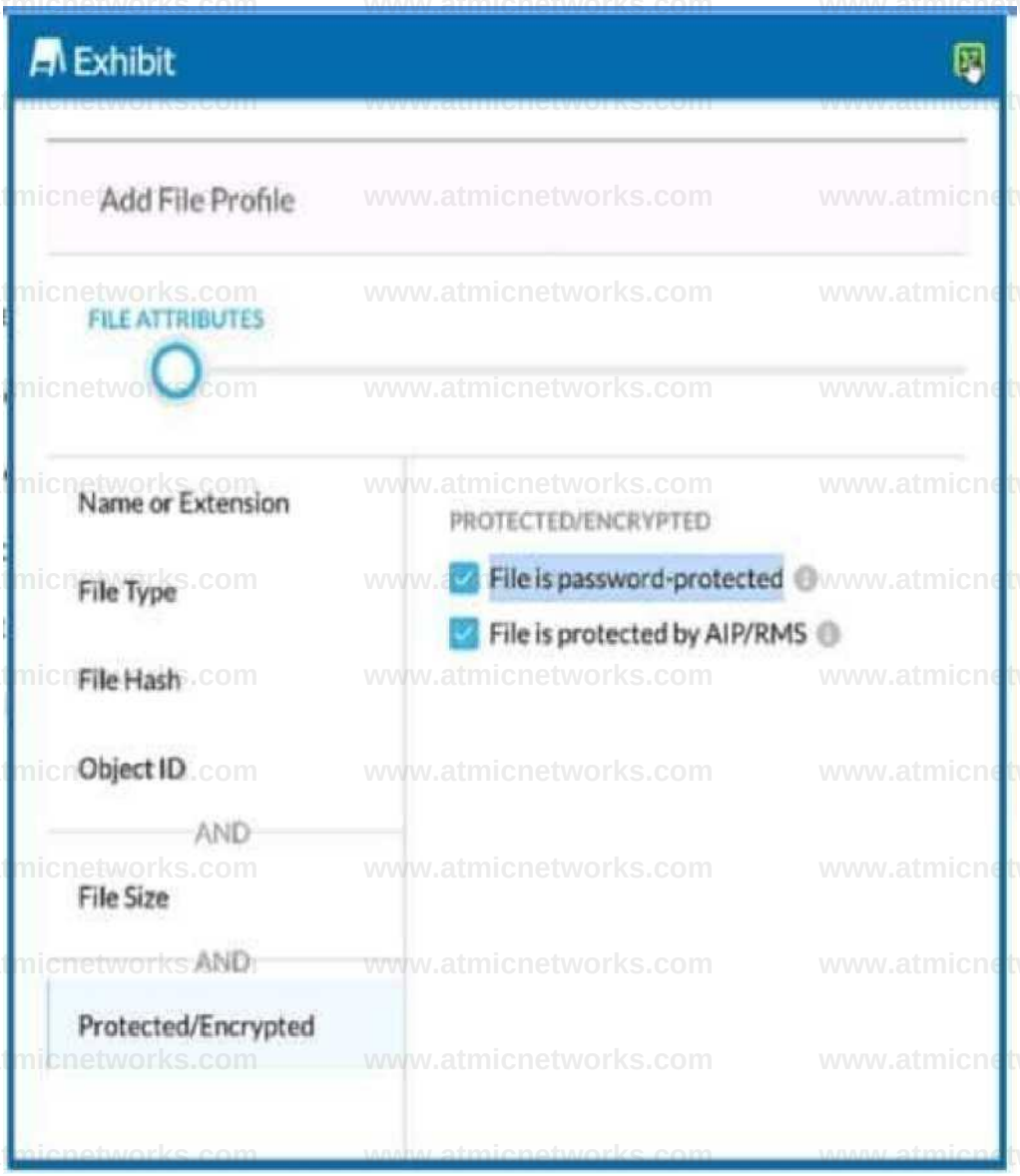
The impact of threat scanning performance (D): The performance of threat scanning can be affected by the encryption and decryption processes in IPsec tunnels. It is important to consider how the threat scanning capabilities will perform under the additional load of encrypted traffic.

These elements are essential for the successful implementation of IPsec tunnels in a Netskope architecture plan for on-premises devices12.

Reference: The considerations for using IPsec tunnels are outlined in the Netskope Knowledge Portal and Community discussions, which provide guidance on deployment and validation of IPsec tunnels, including cipher support, bandwidth management, and maintaining threat scanning performance

Question: 28

Review the exhibit.



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

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

A. Add the profile to a DLP profile that is used in a Real-time Protection policy.
B. Add the profile to a Malware Detection profile that is used in a Real-time Protection policy.
C. Add the profile directly to a Real-time Protection policy as a Constraint.
D. Add the profile to a Constraint profile that is used in a Real-time Protection policy.

Answer: A

Explanation:

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.

Reference: The information aligns with the best practices for setting up DLP profiles in Netskope as described in

their documentation and resources

Question: 29

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

Explanation:

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.
Reference: The answers are based on the information available in the Netskope Knowledge Portal and the documentation for Classic API Data Protection

Question: 30

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

Explanation:

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 Realtime 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.
Reference: 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

Question: 31

You are using Netskope CSPM for security and compliance audits across your multi-cloud environments. To decrease the load on the security operations team, you are researching how to auto-re mediate some of the security violations found in low-risk environments.
Which statement is correct in this scenario?

A. Netskope does not support automatic remediation of security violation results due to the high risk associated with it.
B. You can use Netskope API-enabled Protection for auto-remediation of security violation results.
C. You can use Netskope Auto-remediation frameworks from the public Netskope GitHub Open Source repository for auto-re mediation of security violation results.
D. You can use Netskope Cloud Exchange for auto-remediation of security violation results.

Answer: C

Explanation:

Netskope supports automatic remediation of security violations through its Auto-Remediation frameworks, which are available in the public Netskope GitHub Open Source repository. These frameworks allow for the automatic mitigation of risks associated with security misconfigurations in your cloud environment. The Netskope Auto-Remediation framework for AWS, for example, deploys a set of AWS Lambda functions that query the Netskope API at scheduled intervals and automatically mitigates supported violations1. Similarly, there are frameworks for GCP and other cloud environments that follow the same principle2. This capability is particularly useful for low-risk environments where the security operations team's workload can be reduced by automating the remediation process.
Reference: The answer is based on the information provided by Netskope's community resources and documentation, which detail the use of their Auto-Remediation frameworks for various cloud platforms

Question: 32

Review the exhibit.

www.atmicnetworks.com

•» 0 OCHwATOto MOO ACTIO*

A*r : MtoototOtorMSSwArAtinrCorp Noor • Mtew

Mr Mw.mMt Oto. Ml OwOrto to (tone* Mtotmft OneOire Ml MT Otter MSOnrOMl* toton* Rw O Stark CMJMM Trmnito

v Crate. PoM. Store Uptard

Ao* MrrmonOto.MSOnrOtotopMmntAnorCorp New* 0 • Alto,

tor MH>to»ri Oto. M55WW tour

OBtok CM run 1M*M>

two 0 OCttMhUM

X: Moo^tOtorMSSutotetoCorp tore O Aitor

tew XX MrratotOtorMSSuw tom OBtok Drtrull Tmftelr

Aw X! MurowftOtterMSOnrOnrrtoBmrm, MoowttOreDrrrr MSGCC Otoe 315 OnrOrer to Buuren tore OAtto.

MMt 0 MMMMto toot

tor ' Mtrotefl Otter MSSutetenwCMp tew & Alo*

to XI Mteatol Otter MS tote tore

0 Steck DHerttmotetr

kOM 0 MirnULlK* «C#»1 'lf

AM torotot Oto* MS OntOrwt to tatoa. MKratm CMtOrw MS GCC Oto < MS OncOtvc to Butorrr Cie.ll. ISnt Store Upta*l NAM oatos D< trull lcrrttelc

to ! MerototOtter MSOntOrwrtoArUnnrAcrneCorp MM « Aitor

www.atmicnetworks.com

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

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

Answer: BC

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

Question: 33

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

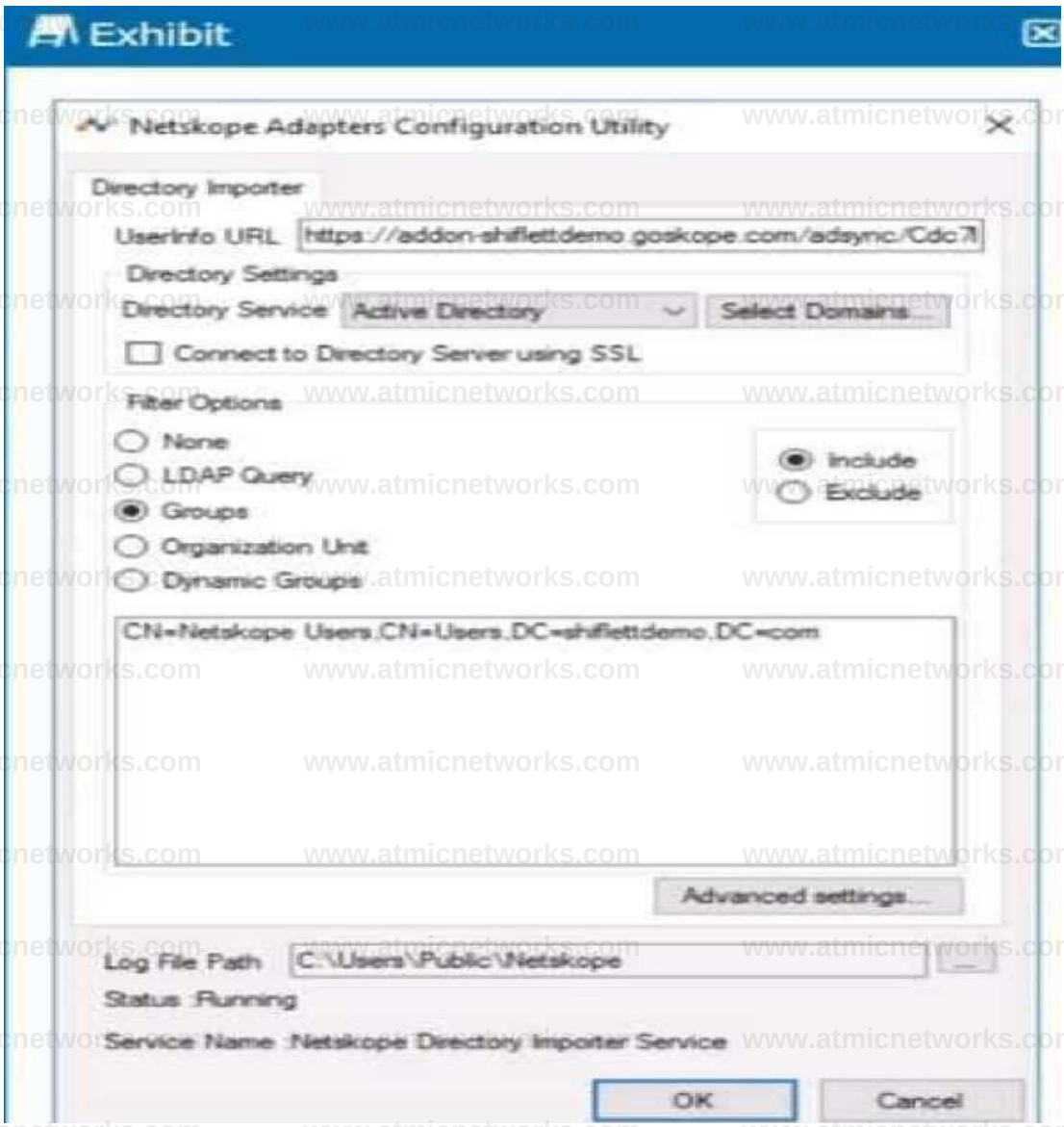
Explanation:

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.

Reference: This solution is based on standard practices for securing IPsec tunnels and ensuring device compatibility with encrypted traffic steering, as outlined in Netskope's documentation on traffic steering and IPsec configuration

Question: 34

Review the exhibit.



www.atmicnetworks.com

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: BCE

Explanation:

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.

Reference: These potential reasons are based on the standard operation and configuration of the Netskope Directory Importer as described in the Netskope Knowledge Portal and documentation

Question: 35

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?

* HTTP Tramarttom

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

Explanation:

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.
Reference: 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

Question: 36

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

Explanation:

To obtain a list of aggregated users, applications, and instance IDs, especially when dealing with nonsanctioned 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.
Reference: The capabilities of the Advanced Analytics tool are outlined in Netskope's documentation and resources, which describe its use for gaining insights into cloud application usage and security posture

Question: 37

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://trustnetskope.com/.

Answer: AC

Explanation:

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.
Reference: 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

Question: 38

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

Explanation:

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.
Reference: The information about policy actions for AWS S3 bucket scans is available in the Netskope

documentation, which provides guidance on creating API Data Protection policies for scanning S3 buckets and the actions that can be taken when a policy is triggered1.

Question: 39

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: D

Explanation:

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.
Reference: Detailed guidance on configuring IPsec VPN tunnels between your AWS Transit Gateway and Netskope POPs can be found in the Netskope Knowledge Portal1. Additionally, the Netskope Community Forum provides insights on setting up IPsec Tunnels for AWS egress traffic, which includes information relevant to deploying Netskope across multiple VPCs2.

Question: 40

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

Explanation:

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.
Reference: 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.

Question: 41

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

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

Answer: D

Explanation:

The reason for using Netskope Cloud Risk Exchange in this scenario is to automate service tickets from alerts of interest. Netskope Cloud Risk Exchange (CRE) is designed to ingest user, device, and application risk scores, creating a dashboard view of contributors to your company's overall risk score and trend. One of the key functionalities of CRE is to trigger risk-reducing actions through business rules that are tuned to a weighted score. Automating service tickets from alerts of interest is a part of this functionality, as it allows for the automatic creation of tickets in response to specific alerts, streamlining the process of addressing potential security issues12.
Reference: The use cases for Netskope Cloud Risk Exchange, including the automation of service tickets, can be found in the official Netskope resources1. Further information on how to integrate and utilize Netskope Cloud Risk Exchange for automating service tickets can be found in the Netskope Knowledge Portal3.

Question: 42

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: BC

Explanation:

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.

Reference: The deployment methods and their suitability for isolated server subnets are based on Netskope's documentation and resources, which detail various deployment options and their use cases21.

Question: 43

You successfully configured Advanced Analytics to identify policy violation trends Upon further investigation, you notice that the activity is NULL. Why is this happening in this scenario?

A. The SSPM policy was not configured during setup.
B. The REST API v1 token has expired.
C. A policy violation was identified using API Protection.
D. A user accessed a static Web page.

Answer: D

Explanation:

The reason for the activity being NULL in this scenario is likely because a user accessed a static Web page. In Netskope's Advanced Analytics, when the activity is reported as NULL, it often indicates that there was no dynamic interaction or transaction to record, which is typical when a static web page is 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.

Reference: This explanation is supported by the Netskope Knowledge Portal, which mentions that applications fields with null values indicate incidents generated from web traffic, such as accessing static web pages2. Further information on interpreting NULL values in Advanced Analytics reports can be found in the Netskope documentation1.

Question: 44

Your company has a large number of medical forms that are allowed to exit the company when they are blank. If the forms contain sensitive data, the forms must not leave any company data centers, managed devices, or approved cloud environments. You want to create DLP rules for these forms. Which first step should you take to protect these forms?

A. Use Netskope Secure Forwarder to create EDM hashes of all forms.
B. Use Netskope Secure Forwarder to create an MIP tag for all forms.
C. Use Netskope Secure Forwarder to create fingerprints of all forms.

D. Use Netskope Secure Forwarder to create an ML Model of all forms

Answer: C

Explanation:

The first step to protect the medical forms containing sensitive data is to create fingerprints of all forms © using Netskope Secure Forwarder. Fingerprints are unique identifiers that can be used to detect when a form contains sensitive data. By creating fingerprints, you can set up DLP (Data Loss Prevention) rules that will allow blank forms to exit the company but will prevent forms with sensitive data from leaving the protected environments. This method ensures that only forms without sensitive information are allowed to be shared externally.
Reference: The process of creating fingerprints for DLP rules is a common practice in data security to protect sensitive information. It is part of the DLP capabilities provided by Netskope, as outlined in their documentation on data protection and loss prevention1.

Question: 45

A hospital has a patient form that they share with their patients over Gmail. The blank form can be freely shared among anyone. However, if the form has any information filled out. the document is considered confidential. Which rule type should be used in the DLP profile to match such a document?

A. Use fingerprint classification.
B. Use a dictionary rule for all your patient names.
C. Use Exact Match with patient names
D. Use predefined DLP Rule(s) that match the patient name.

Answer: A

Explanation:

The appropriate rule type to use in the DLP profile for a document that is considered confidential when filled out is fingerprint classification. Fingerprinting is a method used to identify and protect sensitive data within documents. It works by creating a digital fingerprint of a file, which can then be used to detect any copies or derivatives of that file. In this case, fingerprinting would allow the hospital to differentiate between the blank patient form, which can be freely shared, and the same form with patient information filled out, which is confidential1.
Reference: Netskope's DLP rules can contain elements such as predefined data identifiers, custom data identifiers, keyword identifiers from a dictionary file, RegEx expressions, and exact match criteria1. For this specific use case, fingerprint classification is the most effective method as it can accurately detect the presence of filled-out information in the forms, which is crucial for maintaining patient confidentiality as per HIPAA regulations1.

Question: 46

You have enabled CASB traffic steering using the Netskope Client, but have not yet enabled a Realtime Protection policy. What is the default behavior of the traffic in this scenario?

A. Traffic will be blocked and logged.
B. Traffic will be allowed and logged.
C. Traffic will be blocked, but not logged.

D. Traffic will be allowed, but not logged.

Answer: B

Explanation:

In the scenario where CASB traffic steering is enabled using the Netskope Client without a Real-time Protection policy being activated, the default behavior of the traffic is to allow and log it (B). This means that the traffic will not be blocked; instead, it will be permitted to pass through and will be recorded for monitoring and analysis purposes. This default setting ensures visibility into the traffic and user activities without immediately enforcing a block, allowing for a period of observation and policy tuning before potentially more restrictive actions are taken1.

Reference: The default behavior of traffic steering in Netskope, including the logging of allowed traffic, is detailed in Netskope's best practices and community discussions on Real-time Protection policies1.

Question: 47

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

Explanation:

To ensure that the web application using HTTPS on port 6443 is both reachable and decrypted by Netskope, the correct action is to enable "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.

Reference: 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 nonstandard 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.

Question: 48

Your client is an NG-SWG customer. They are going to use the Explicit Proxy over Tunnel (EPoT) steering method. They have a specific list of domains that they do not want to steer to the Netskope Cloud.

What would accomplish this task''

A. Define exception domains in the PAC file.
B. Define exceptions in the Netskope steering configuration
C. Create a real-time policy with a bypass action.
D. Use an SSL decryption policy.

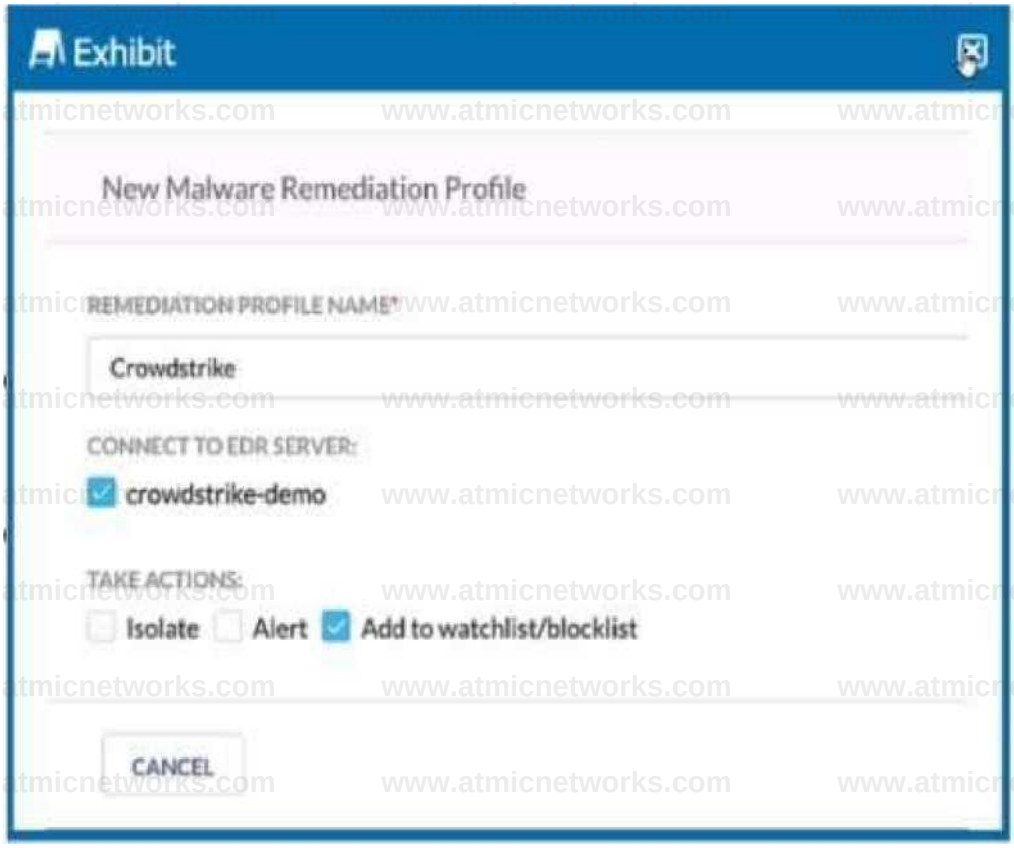
Answer: A

Explanation:

To accomplish the task of not steering specific domains to the Netskope Cloud while using the Explicit Proxy over Tunnel (EPoT) steering method, you would define exception domains in the PAC file (A). This is because the PAC file is used to specify which domains should bypass the proxy and connect directly, thus allowing for granular control over the traffic that is steered to Netskope1. Reference: The use of PAC files for steering exceptions is a standard practice in proxy configurations and is supported by Netskope's EPoT steering method as outlined in their documentation1.

Question: 49

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: A

Explanation:

The remediation profile shown in the exhibit will take the action of isolating the endpoint. This is indicated by the "Isolate" option being checked under "TAKE ACTIONS" in the configuration settings. When this option is selected, the remediation profile is configured to isolate the endpoint upon detection of a threat, which is a common response to contain a potential security breach and prevent further spread of malware within the network1.

Reference: The Netskope Knowledge Portal provides detailed information on integrating CrowdStrike for EDR and the actions that can be taken by remediation profiles, including endpoint isolation1. Further details on the integration process and remediation actions can be found in the documentation provided by Netskope23.

Question: 50

You jus! deployed and registered an NPA publisher for your first private application and need to provide access to this application for the Human Resources (HR) users group only. How would you

accomplish this task?

A. 1. Enable private app steering in the Steering Configuration assigned to the HR group.
2. Create a new Private App.
3. Create a new Real-time Protection policy as follows;
Source = HR user group Destination = Private App Action = Allow
B. 1. Create a new private app and assign it to the HR user group.
2. Create a new Real-time Protection policy as follows:
Source = HR user group Destination = Private App Action = Allow.
C. 1. Enable private app steering in Tenant Steering Configuration.
2. Create a new private app and assign it to the HR user group.
D. 1. Enable private app steering in the Steering Configuration assigned to the HR group.
2. Create a new private app and assign it to the HR user group
3. Create a new Real-time Protection policy as follows:
Source = HR user group Destination = Private App Action = Allow

Answer: D

Explanation:

To provide access to a private application for the Human Resources (HR) users group only after deploying and registering an NPA publisher, you would need to:
Enable private app steering in the Steering Configuration assigned to the HR group: This ensures that only traffic from the HR user group is steered towards the private application.
Create a new private app and assign it to the HR user group: This step involves defining the private application within Netskope and specifying that only the HR user group should have access to it.
Create a new Real-time Protection policy as follows:
Source = HR user group: This specifies that the policy applies to the HR user group.
Destination = Private App: This defines the private application as the destination for the policy.
Action = Allow: This action allows the HR user group to access the private application.
By following these steps, you can ensure that only the HR user group has access to the private application, aligning with the principles of least privilege and zero trust access control.
Reference: The process for providing access to a private application for a specific user group is detailed in

Netskope's documentation on Private Access and Private App Management12.

Question: 51

A company wants to capture and maintain sensitive PII data in a relational database to help their customers. There are many employees and contractors that need access to sensitive customer data to perform their duties The company wants to prevent the exfiltration of sensitive customer data by their employees and contractors.

In this scenario. what would satisfy this requirement?

A. fingerprinting
B. exact data match
C. regular expression
D. machine learning

Answer: A

Explanation:

Fingerprinting would satisfy the requirement to prevent the exfiltration of sensitive Personally Identifiable Information (PII) data by employees and contractors. Fingerprinting is a data protection technique that involves creating a unique digital representation of sensitive data. This allows for the detection of any exact or partial matches of the fingerprinted data leaving the company's environment, thereby preventing unauthorized data exfiltration. It is particularly effective in scenarios where multiple individuals require access to sensitive data, as it can protect against both inadvertent and malicious attempts to move data outside of authorized channels1. Reference: Netskope's Data Loss Prevention (DLP) capabilities include fingerprinting as a method to secure sensitive data consistently across the enterprise1. The Netskope Knowledge Portal provides further information on how to enable and configure fingerprinting and other DLP settings to protect sensitive PII data2.

Question: 52

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

Explanation:

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.

www.atmicnetworks.com

Reference: 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.

Question: 53

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

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

Answer: A

Explanation:

To allow traffic from a website with a self-signed certificate that is being blocked by Netskope with an SSL error, the correct action is to configure a Do Not Decrypt SSL Decryption rule. This rule will allow the traffic to pass without being decrypted, thus bypassing the SSL error caused by the selfsigned certificate. This is a common practice for handling traffic from trusted internal applications or specific external sites that use self-signed certificates1.
Reference: The Netskope Community Forum discusses the application of exceptions for sites with self-signed certificates and the use of SSL decryption policies to bypass the blocking1. Additionally, the Netskope Knowledge Portal provides information on managing error settings and configuring SSL decryption rules2.

Question: 54

You want to verify that Google Drive is being tunneled to Netskope by looking in the nsdebuglog file.
You are using Chrome and the Netskope Client to steer traffic. In this scenario, what would you expect to see in the log file?

A)
2&22/M/C OlsOHC 9.7 31010 stAgeatKE p752b t2Sda7 inf: tunnel-cpp:712 nsTunael TLS [aessld 502| Tunneling flow from addr: 1*0*0.1:44000. process; google drive to host; play.googleapxs.coa>, addr; 172.217.4.4G;443 to naProxy

B)
2022/01/0 31:00:04.001013 stAgestSE p752h t2Ma7 info- tunnel.cpp:712 nsTunnel US [wasld 502] Tunneling flow froa aid:: 1.0.0.1:03710, pcocein: google chrcae helper to host; dxl're.google.coa, edit; 172.217.4.40:443 to csFtoxy

C)
2022/01/0 01:00:00.001010 stAgestJiE p752b t2Sd*7 inf: bypassAppMgr .^pz'JS Byp*ssAppMgx Bypassing UW» flow to process google chrome helper ip: 172.217.4.4€, port: 443, host: drive.google.co®

D)
2022/01/0 01:00:00.001010 stAgencllE p752b t2Ma7 Info AppPrc-xyfrovlder.«n:3C3 aain Sew UD? flow: Process • google ch:one helper, IF:port - [9.8.8.8:53]

A. Option A B. Option B C. Option C D. Option D

Answer: A

Explanation:

When verifying that Google Drive traffic is being tunneled to Netskope using Chrome and the Netskope Client, you would expect to see log entries indicating that the traffic is being directed through Netskope's proxy. Specifically, Option A is correct as it shows the process "google drive" being tunneled to nsProxy. The log entry for Option A indicates that a TLS tunneling flow from a local address and process (Google Drive) is being directed to a host (play.googleapis.com) and then to Netskope's proxy (nsProxy). This is consistent with how Netskope tunnels specified traffic for security and policy enforcement1.

Reference: The expected log entries are based on the standard operation of Netskope Client and how it steers traffic to Netskope's cloud services, as detailed in Netskope's documentation1.

Question: 55

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-timeProtection policy to allow the Browse activity to the Amazon S3 application.
B. Create a Real-timeProtection policy to allow the Browse activity to the Cloud Storage category
C. Create a Real-timeProtection policy to allow the Download activity to the Cloud Storage category
D. Create a Real-timeProtection policy to allow the Download activity to the Amazon S3 application

Answer: B

Explanation:

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.

Reference: 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

Question: 56

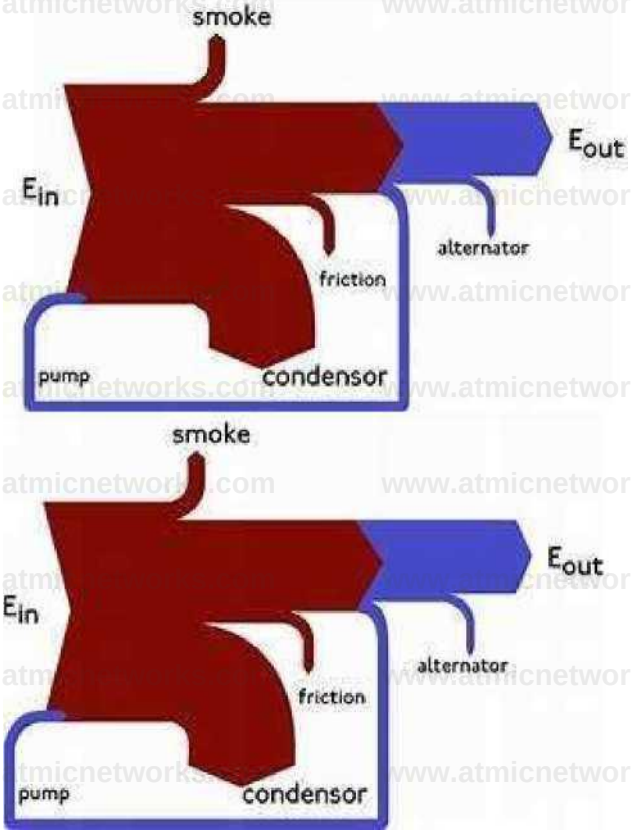
Your CISO asks that you to provide a report with a visual representation of the top 10 applications (by number of objects) and their risk score. As the administrator, you decide to use a Sankey visualization in Advanced Analytics to represent the data in an efficient manner.

In this scenario, which two field types are required to produce a Sankey Tile in your report? {Choose two.)

A. Dimension
B. Measure
C. Pivot Ranks
D. Period of Type

Answer: AB

Explanation:



To produce a Sankey Tile in a report that visually represents the top 10 applications by number of objects and their risk score, you would need:

Dimension (A): This field type would be used to represent the nodes in the Sankey visualization, which could be the applications in this case1.

Measure (B): This field type would provide the weight of the links between the nodes, representing the number of objects or the risk score associated with each application1.

These two field types are essential for creating a Sankey visualization as they define the structure and flow of data between different stages or categories within the visualization.

Reference: The requirements for creating a Sankey visualization are based on the general principles of data visualization and the specific features of Sankey diagrams, which typically involve dimensions and measures to represent the flow of data1.

Question: 57

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: BC

Explanation:

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.

Reference: The Netskope Knowledge Portal provides detailed information on managing certificate- pinned applications, including how to configure SSL Do Not Decrypt policies and domain exceptions in the steering configuration1. Additionally, the Netskope Community Forum offers insights and best practices for handling certificate-pinned applications2.

Question: 58

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

Explanation:

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.

Reference: 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.

Question: 59

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

Explanation:

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.
Reference: The process for configuring an allowlist in Cloud Explicit Proxy to manage unauthenticated traffic from specific IP addresses is detailed in the Netskope Knowledge Portal1. This solution is suitable for scenarios where adding Netskope's IP ranges to the SaaS vendor's IP restrictions is not feasible.

Question: 60

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

Explanation:

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.

Reference: 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.

www.atmicnetworks.com