Number: NSK300
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: NSK300

Exam Name: Netskope Certified Cloud Security Integrator

Exam A

QUESTION 1
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.

Correct Answer: B, D
Section:
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.
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.
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 2
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

Correct Answer: C, D
Section:
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 theSteering Configurationsection 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.
On Premises Detection:
This option is available under theClient Configurationsection 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.

QUESTION 3
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

Correct Answer: C
Section:
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-ALLAccountscondition 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.
Netskope Cloud Security
Netskope Solution Brief
Netskope Community

QUESTION 4
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.

Correct Answer: A, C
Section:
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 toUpgrade 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, theautoupdate-onflag should be set. This flag enables the auto-update feature, allowing the client to receive and apply updates as they are released.

QUESTION 5
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.

Correct Answer: A
Section:
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 6
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

Correct Answer: B
Section:
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 7
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

Correct Answer: A
Section:
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

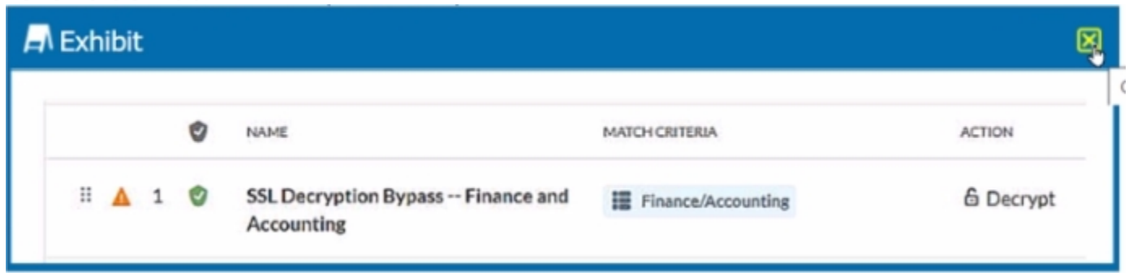
QUESTION 8
Review the exhibit.

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

Correct Answer: A, B, D
Section:
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 self-signed 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

QUESTION 9
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.

Correct Answer: B, D
Section:
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 10
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

Correct Answer: C
Section:
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 theEnterprise Egress IPv4address.
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 11
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.

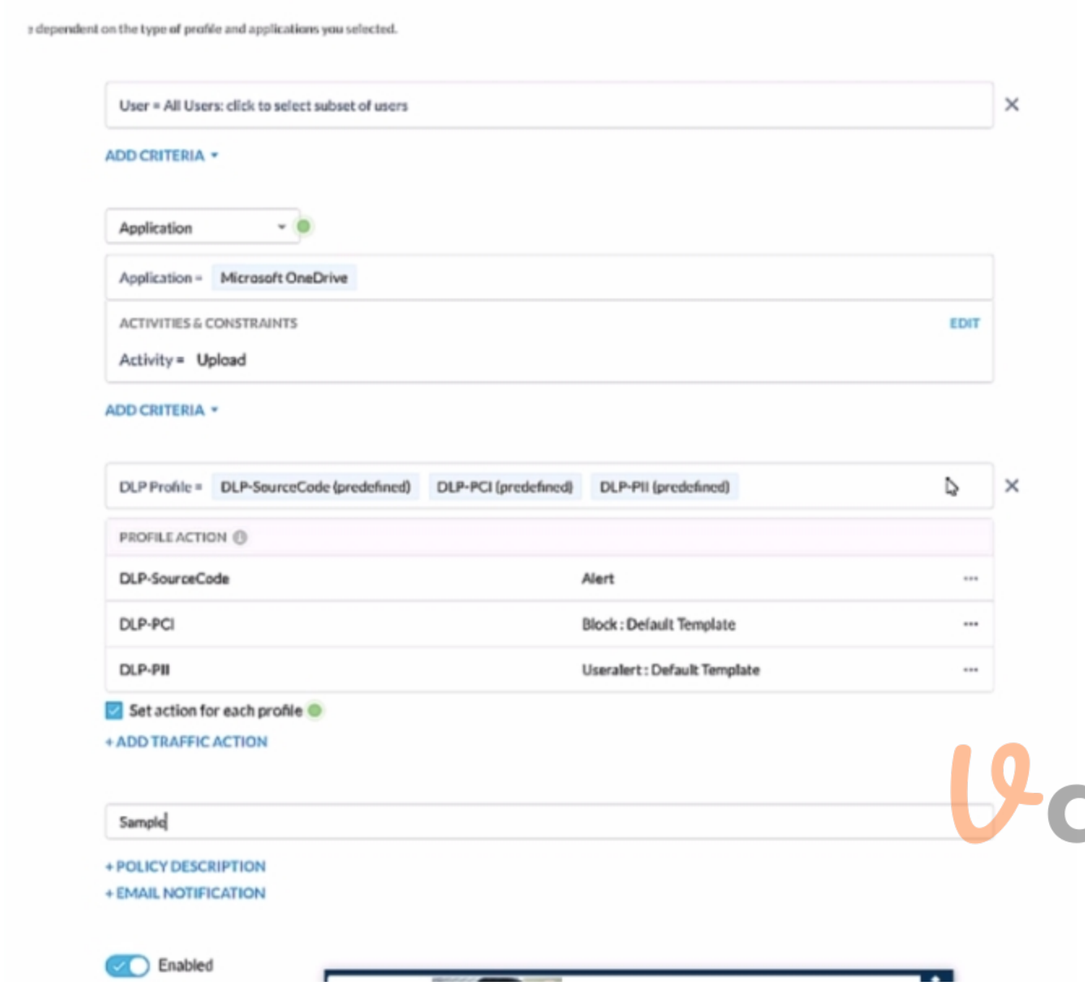
Correct Answer: D
Section:
Explanation:
To retain the original dashboard without automatic updates due to improvements made by Netskope, you can download the desired dashboard and then import it from a file into your Group or Personal folder.
This approach ensures that you have a static version of the 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 12
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.

Correct Answer: B
Section:
Explanation:
To prevent potential routing issues and ensure that the Netskope agent consistently sees the traffic first, it is recommended tomodify 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.

QUESTION 13
Review the exhibit.



A user has attempted to upload a file to Microsoft OneDrive that contains source code with Pll 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.

Correct Answer: C
Section:
Explanation:
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.
Netskope Cloud Security
Netskope Resources
Netskope Documentation

QUESTION 14
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

Correct Answer: C
Section:
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.
Netskope Cloud Security
Netskope Resources
Netskope Documentation

QUESTION 15
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 UI 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

Correct Answer: A, B
Section:
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 Publisherin 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 toolin 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.

QUESTION 16
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

Correct Answer: D
Section:
Explanation:
When integrating a third-party Data Loss Prevention (DLP) engine that requires ICAP, the Netskope platform component that must be configured is theNetskope 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.

QUESTION 17
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

Correct Answer: C
Section:
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.

QUESTION 18
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

Correct Answer: C
Section:
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.

QUESTION 19
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

Correct Answer: D
Section:
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.

QUESTION 20
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.

Correct Answer: B
Section:
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.

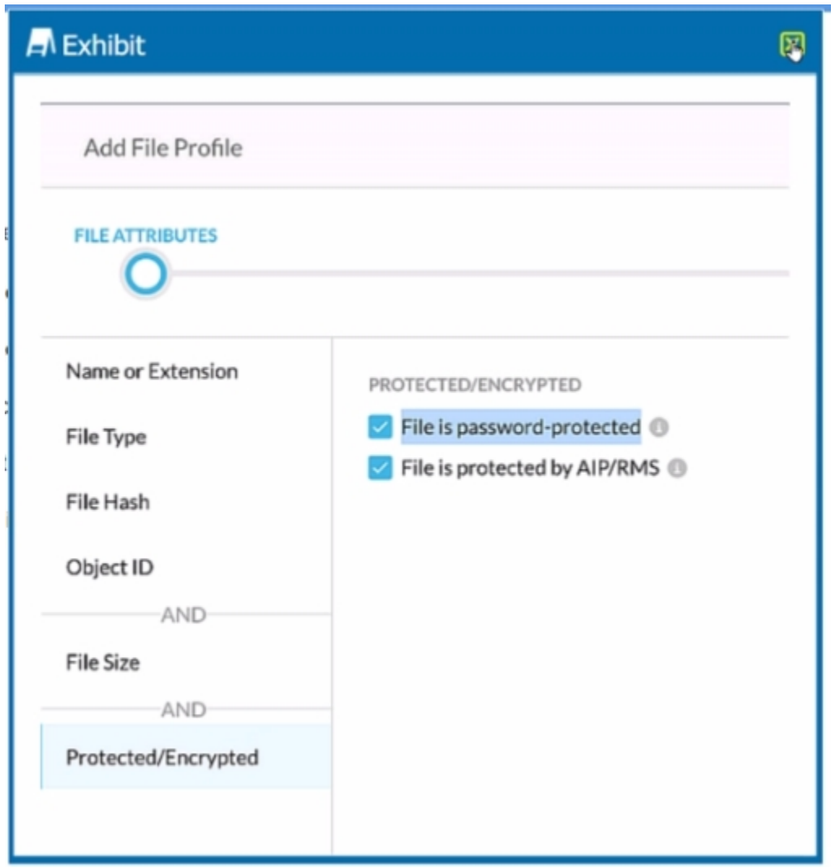
QUESTION 21
You are building an architecture plan to roll out Netskope for on-premises devices. You determine that tunnels are the best way to achieve this task due to a lack of support for explicit proxy in some instances and IPsec is the right type of tunnel to achieve the desired security and steering.
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

Correct Answer: A, B, D
Section:
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.

QUESTION 22

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.

Correct Answer: A
Section:
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.

QUESTION 23
You have enabled CASB traffic steering using the Netskope Client, but have not yet enabled a Real-time 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.

Correct Answer: B
Section:
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.

QUESTION 24
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

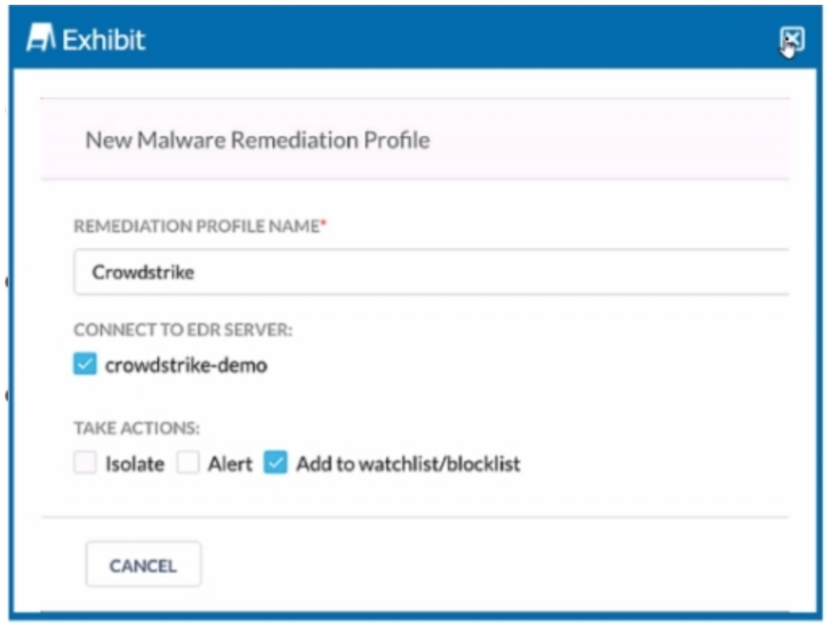
Correct Answer: C
Section:
Explanation:
To ensure that the web application using HTTPS on port 6443 is both reachable and decrypted by Netskope, the correct action is to enable ''Steer non-standard ports'' in the steering configuration and add the domain and port as a new non-standard port. This is because 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.

QUESTION 25
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.

Correct Answer: A
Section:
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.

QUESTION 26
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.

Correct Answer: A
Section:
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.

QUESTION 27
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

Correct Answer: D
Section:
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.

QUESTION 28
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.

Correct Answer: D
Section:
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.

QUESTION 29
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 venfy 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.

Correct Answer: D
Section:
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.

QUESTION 30
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

Correct Answer: A
Section:
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.

QUESTION 31
What is a Fast Scan component of Netskope Threat Detection?

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

Correct Answer: B
Section:
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.