[Q11-Q26 Get 100% Real NSK300 Accurate & Verified Answers As Seen in the Real Exam!

Digital
Marketing
[Q11-Q26] Get 100% Real NSK300 Accurate &
Verified Answers As Seen in the Real Exam!

Get 100% Real NSK300 Exam Questions, Accurate & Verified Answers As Seen in the Real Exam! NSK300 Premium Files Updated Sep-2024 Practice Valid Exam Dumps Question NEW QUESTION 11

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?
* Restart the tunnel to stop the tunnel from flapping.
* Downgrade from IKE v2 to IKE v1.
* Install the Netskope root and intermediate certificates on the end-user devices.
* Disable Perfect Forward Secrecy on the tunnel configuration.
When applications steered through an IPsec tunnel are non-functional, it is often due to the lack of proper trust establishment between the end-user devices and the Netskope data plane. The solution is to install the Netskope root and intermediate certificates on the end-user devices . This ensures that the devices recognize and trust the encrypted connection established by the IPsec tunnel, allowing the HTTPS SaaS applications to function correctly. Without these certificates, the devices may not be able to verify the security of the connection, leading to application failures.

NEW QUESTION 12

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?

- Steering: Cloud Apps Only, All Traffic Policy type: Real-time Protection Constraint: Storage. Bucket Does Not Match -ALLAccounts Action: Block
- Steering: Cloud Apps Only Policy type: Real-time Protection

Constraint: Storage. Bucket Does Not Match *@myorganization.com Action: Block

- Steering: Cloud Apps Only. All Traffic Policy type: Real-time Protection Constraint: Storage. Bucket Does Match -ALLAccounts Action: Allow
- Steering: All Web Traffic Policy type: API Data Protection Constraint: Storage, Bucket Does Match *@myorganization.com Action: Allow

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

NEW QUESTION 13

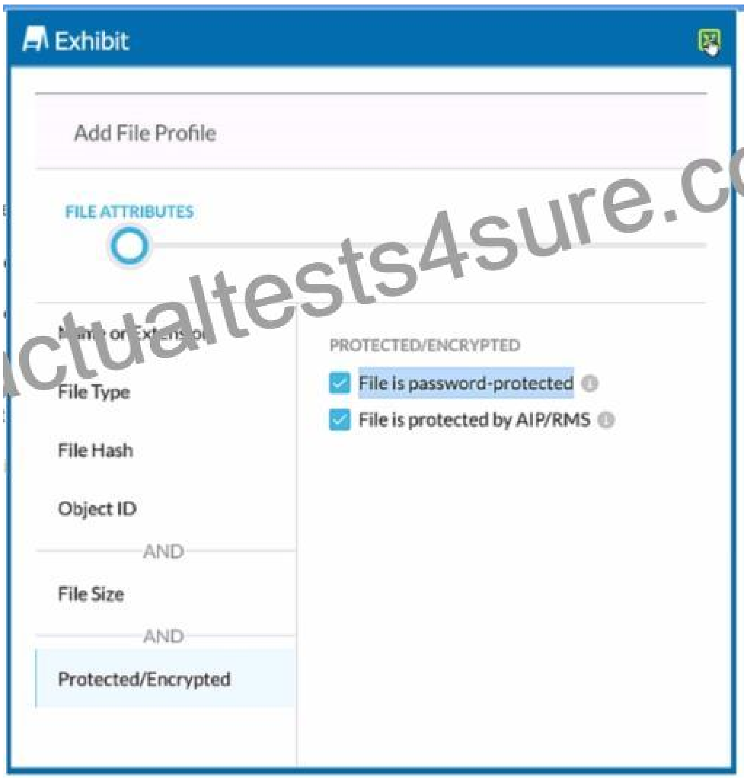
You are currently designing a policy for AWS S3 bucket scans with a custom DLP profile Which policy action(s) are available for this policy?

- Alert, Quarantine. Block, User Notification
- Alert, User Notification

* Alert only
* Alert, Quarantine
When designing a policy for AWS S3 bucket scans with a custom DLP profile in Netskope, the available policy actions are Alert and Quarantine. These actions allow you to be notified when a policy violation occurs and to quarantine sensitive data to prevent potential data loss or exposure. The Alert action will notify the designated personnel or system when a match to the DLP profile is found during the scan. The Quarantine action will move the offending file to a secure location where it can be reviewed and dealt with appropriately1.

NEW QUESTION 14

Review the exhibit.



Exhibit

Add File Profile

FILE ATTRIBUTES

Name or Extension

File Type

File Hash

Object ID

AND

File Size

AND

Protected/Encrypted

PROTECTED/ENCRYPTED

☑ File is password-protected

☑ File is protected by AIP/RMS

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?
* Add the profile to a DLP profile that is used in a Real-time Protection policy.
* Add the profile to a Malware Detection profile that is used in a Real-time Protection policy.
* Add the profile directly to a Real-time Protection policy as a Constraint.
* Add the profile to a Constraint profile that is used in a Real-time Protection policy.
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.

NEW QUESTION 15

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.)
* cipher support on tunnel-initiating devices
* bandwidth considerations
* the categories to be blocked
* the impact of threat scanning performance
* Netskope Client behavior when on-premises

When using IPsec tunnels, especially in the context of deploying Netskope for on-premises devices, several factors must be considered to ensure a secure and efficient architecture:

Cipher support on tunnel-initiating devices (A): It is crucial to ensure that the devices initiating the IPsec tunnels support the ciphers used by Netskope. This compatibility is necessary for establishing secure connections.

Bandwidth considerations (B): The bandwidth available for the IPsec tunnels will affect the data throughput and performance of the connection. Adequate bandwidth must be allocated to handle the expected traffic without causing bottlenecks.

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

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

NEW QUESTION 16

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.)
* Change Safe Search to Disabled
* Change Untrusted Root Certificate to Block.
* Change the No SNI setting to Block.
* Change &#8220;Disallow concurrent logins by an Admin&#8221; to Enabled.

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 &#8220;Disallow concurrent logins by an Admin&#8221; 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&#8217;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.

NEW QUESTION 17

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?
* Use IPsec tunnels from the AWS Virtual Private Gateway.
* Use GRE tunnels from the AWS Transit Gateway.
* Use GRE tunnels from the AWS Virtual Private Gateway
* Use IPsec tunnels from the AWS Transit Gateway.

The best approach to deploy Netskope for machine traffic across multiple VPCs in an AWS account with the least amount of tunnels while providing connectivity for all VPCs is to use IPsec tunnels from the AWS Transit Gateway. This method allows you to use the same Site-to-Site VPN connection to Netskope for multiple VPCs, thus minimizing the number of tunnels required12. The AWS Transit Gateway acts as a network transit hub, enabling you to connect your VPCs and on-premises networks through a central point of management and control. Using IPsec tunnels with the AWS Transit Gateway ensures that all VPCs connected to it utilize the same IPsec tunnel between the transit gateway and Netskope POP1.

NEW QUESTION 18

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 &#8220;marketing-users&#8221; 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?
* There is a missing group name in the SAML response.
* The username in the name ID field is not in the format of the e-mail address.
* There is an invalid certificate in the SAML response.
* The username in the name ID field does not have the &#8220;marketing-users&#8221; group name.

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 &#8220;marketing-users&#8221; group name should be present in the SAML response to enforce the policy that blocks login activity for this group. If the group name is missing, the policy will not apply, and users will not be blocked as intended.

NEW QUESTION 19

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?
* Use Netskope Secure Forwarder to create EDM hashes of all forms.
* Use Netskope Secure Forwarder to create an MIP tag for all forms.
* Use Netskope Secure Forwarder to create fingerprints of all forms.
* Use Netskope Secure Forwarder to create an ML Model of all forms

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.

NEW QUESTION 20

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?

* Advanced Analytics
* Behavior Analytics
* Applications in Skope IT
* Cloud Confidence Index (CCI)

To obtain a list of aggregated users, applications, and instance IDs, especially when dealing with non-sanctioned Cloud Storage platforms, the Advanced Analytics (A) tool within Netskope would be used. Advanced Analytics provides in-depth visibility into cloud app usage and activities. It allows security teams to create detailed reports and dashboards that can help identify risks and ensure compliance with company policies by analyzing user behavior, application access, and data movement across the organization1.

NEW QUESTION 21

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 Ul would you change to solve this problem?

* Disable the default Microsoft appsuite SSL rule.
* Disable the default certificate-pinned application
* Remove the default steering exception for domains.
* Remove the default steering exception for Cloud Storage.

When deploying Netskope and steering all traffic, if you find that the Real-time Protection policies for Microsoft OneDrive are not being enforced, the likely issue is with the default steering exceptions. To resolve this, you should remove the default steering exception for domains . This is because the default exceptions may include domains related to Microsoft services, which could prevent the Real-time Protection policies from being applied to traffic directed towards OneDrive. By removing these exceptions, you ensure that all traffic, including that to OneDrive, is subject to the policies you have set up.

NEW QUESTION 22

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?

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

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.

NEW QUESTION 23

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&#8217;s instance of Microsoft 365 be steered to Netskope for inspection.

How would you achieve this scenario from a steering perspective?

* Use IPsec and GRE tunnels.

* Use reverse proxy.
* Use explicit proxy and the Netskope Client
* Use DPoP and Secure Forwarder

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&#8217;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.

NEW QUESTION 24

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.)

* Use Cloud Ticket Orchestrator.
* Use Cloud Log Shipper.
* Stream directly to syslog.
* Use the REST API.

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:

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.

NEW QUESTION 25

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.)

* Reachability Via Publisher in the App Definitions page
* Troubleshooter tool in the App Definitions page
* Applications in Skope IT
* Clear Private App Auth under Users in Skope IT

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&#8217;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 &#8211; This tool allows you to check if the application is reachable through the configured Publishers. It is essential to ensure that the application&#8217;s connectivity is intact and that there are no issues with the Publishers themselves.

B . Troubleshooter tool in the App Definitions page &#8211; 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.

NEW QUESTION 26

A company&#8217;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.)

* Deploy a mobile profile on the servers.
* Deploy Data Plane on Premises (DPoP) with a proxy configuration on the servers.
* Deploy IPsec or GRE tunnels in the segment to steer traffic from the servers to Netskope.
* Install the Netskope Client on the servers

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&#8217;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.