PassQueen
a.k.a dumpsqueen.com

Netskope Certified Cloud Security Architect Exam

Netskope NSK300

Version Demo

Total Demo Questions: 11

Total Premium Questions: 111

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Netskope Platform	23
Topic 2, Traffic Steering	31
Topic 3, Web Security	13
Topic 4, Cloud Security	20
Topic 5, Private Access	11
Topic 6, Data Protection	13
Total	111

QUESTION NO: 1

A company maintains a relational database containing active customer account numbers. Employees need to use the customer service application, but the company must identify and block attempts to upload actual account numbers to unsanctioned cloud storage.

Which DLP detection technique is best suited to this requirement?

A. Document fingerprinting

B. Exact Data Match

C. Regular expression

D. Machine learning

ANSWER: B

Explanation:

Exact Data Match is designed to identify specific known sensitive values from an authoritative data source. The organization can use the customer account-number data set to create protected fingerprints, allowing Netskope to detect disclosures of real account numbers rather than merely values that resemble an account-number pattern.

A regular expression can identify a format, but it is more likely to match unrelated values with the same structure. Document fingerprinting is better suited to identifying known documents or document content, while machine learning is not the primary control for matching an authoritative list of exact data values.

QUESTION NO: 2

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: B

Explanation:

Configure the SSL Do Not Decrypt policy to not decrypt traffic for domains used by the native application. This is the appropriate configuration for a certificate-pinned application because it preserves the end-to-end TLS session between the application and its destination. Certificate pinning causes an application to compare the server certificate it receives with a certificate or public key that the application already trusts. If a security proxy decrypts TLS traffic, it terminates the original TLS session and presents a substitute certificate to the application; that certificate does not match the pinned value, so the application rejects the connection. A narrowly scoped SSL Do Not Decrypt rule prevents this TLS interception for the application's required destination domains while the Netskope Client still forwards the traffic to Netskope. Consequently, the application can validate the genuine destination certificate and operate normally, while the organization maintains the intended traffic-steering path. The rule should be limited to the confirmed FQDNs or domains used by the application and placed with suitable policy priority to ensure it is evaluated before a broader SSL decryption rule. See the Netskope Documentation portal and the Netskope Support Knowledge Portal for the applicable SSL decryption-policy configuration guidance.

QUESTION NO: 3

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: A C

Explanation:

"In the Client Configuration, set Upgrade Client Automatically to Latest Release." is required because the tenant-side Client Configuration determines the upgrade policy that enrolled Netskope Clients follow. Selecting the latest-release automatic-upgrade setting allows clients to receive Netskope's currently released client version without requiring the software deployment team to package and distribute each subsequent client installer through SCCM. This is the policy control that keeps the deployed population aligned to the most current supported release.

"Set the autoupdate-on flag during the original Install." is also required because automatic upgrades must be enabled in the client's initial installation configuration. In an SCCM deployment, that installation-time setting permits the installed client to accept and apply the automatic-upgrade policy delivered from the Netskope tenant. Together, the installation flag and the Client Configuration policy provide the endpoint enablement and administrative release-selection controls needed for ongoing client upgrades. Netskope's documentation portal contains the current Netskope Client deployment and client-configuration guidance: Netskope Documentation. Additional product and release resources are available from Netskope Resources.

QUESTION NO: 4

You are onboarding a supported SaaS application through Netskope API-enabled Protection. The organization requires one connection to scan data at rest for sensitive content and another connection to collect application activity for user behavior analysis.

Which two API-enabled Protection instance types should be configured? (Choose two.)

A. API Data Protection

B. Behavior Analytics

C. Forensic

D. Quarantine

E. DLP Scan

ANSWER: A B

Explanation:

API Data Protection is the appropriate instance type for scanning data stored in a supported SaaS application for sensitive content and policy violations. It provides the API-based inspection workflow for data at rest.

Behavior Analytics is the appropriate instance type for collecting relevant SaaS activity and context for user and entity behavior analysis. Forensic is intended for forensic collection and investigation workflows, while Quarantine and DLP Scan are not API-enabled Protection instance types.

QUESTION NO: 5

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 task? (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: A C

Explanation:

Setting *Upgrade Client Automatically* to *Latest Release* in Client Configuration establishes the tenant-side policy that directs enrolled Netskope Clients to update to Netskope's current supported release. This is the appropriate policy when the administrator's objective is to keep the SCCM-installed clients continuously current rather than hold them to a controlled version. The client must also have been installed with the `autoupdate=on` MSI property. That installation-time property enables the client's self-update capability, allowing it to receive and apply the upgrade policy subsequently configured in the Netskope tenant. Together, the original installer setting and the Client Configuration update policy transfer ongoing upgrade management from the original SCCM deployment process to Netskope administration. The setting is especially useful for endpoints that may not regularly connect to the corporate management infrastructure but can reach the Netskope tenant. Netskope's client-management guidance describes automatic client-upgrade controls and release management; see the Netskope Client Management documentation and the Netskope Client documentation.

QUESTION NO: 6

Your company purchased Netskope's Next Gen Secure Web Gateway You are working with your network administrator to create GRE tunnels to send traffic to Netskope Your network administrator has set up the tunnel, keepalives. and a policy-based route on your corporate router to send all HTTP and HTTPS traffic to Netskope. You want to validate that the tunnel is configured correctly and that traffic is flowing.

In this scenario, which two statements are correct? (Choose two.)

A. You can use your local router or network device to verify that keepalives are being received and traffic is flowing to Netskope.

B. You must use your own monitoring tools to verify that the tunnel is up.

C. You can verify that the tunnel is up and receiving traffic in the Netskope UI under Settings > Security Cloud Platform > GRE.

D. You can verify that the tunnel is up in the Netskope Trust portal at https://trust netskope.com/.

ANSWER: A C

Explanation:

"You can use your local router or network device to verify that keepalives are being received and traffic is flowing to Netskope." is correct because the enterprise router is the GRE tunnel endpoint on the customer side. Its operational commands, tunnel-interface counters, GRE encapsulation and decapsulation statistics, routing information, and keepalive state provide direct evidence that the tunnel is established and that selected web traffic is being forwarded into it. This is an important first validation point after configuring policy-based routing for HTTP and HTTPS traffic.

"You can verify that the tunnel is up and receiving traffic in the Netskope UI under Settings > Security Cloud Platform > GRE." is also correct. Netskope provides GRE tunnel visibility in the tenant UI, allowing an administrator to confirm that Netskope sees the configured tunnel as active and is receiving traffic. Checking both the customer-side device and the

Netskope tenant gives end-to-end confirmation: the router is transmitting through the intended GRE path, and the Netskope Security Cloud Platform is receiving that traffic for SWG processing. Netskope documentation and product information are available at Netskope Documentation and Netskope Next Gen Secure Web Gateway.

QUESTION NO: 7

You receive a report from your endpoint team that a device may no longer be running the Netskope Client. You only know the hostname of the machine in question. You want to remotely verify whether the client is still installed and steering traffic and which user is assigned to the device. In this scenario, how would you accomplish this task?

A. Enable IP restrictions for a sanctioned application and see if any users report an access problem.

B. Under Skope IT Users, look at the Users Over Time graph for any anomalies.

C. Under the Netskope Client Devices page, search for the hostname in question and identify the current Client Status and User information.

D. Under Skope IT Applications Events, query by hostname and determine the last event date and time.

ANSWER: C

Explanation:

Under the Netskope Client Devices page, search for the hostname in question and identify the current Client Status and User information. This is the appropriate operational workflow because the Client Devices inventory is designed to provide endpoint-specific visibility for Netskope Client deployments. Searching with the known hostname locates the device record without needing interactive access to the endpoint. The resulting record provides the client's reported status and associated user details, allowing an administrator to determine whether the endpoint is continuing to communicate with the Netskope tenant and whether it is in a state consistent with active traffic steering. This also supports practical incident triage: the administrator can validate the endpoint identity, inspect the last-known client information, and correlate the device with its user assignment before deciding whether remediation, reinstall, or further endpoint investigation is needed. Netskope documents the Netskope Client as the endpoint component that directs traffic to the Netskope Security Cloud, while device-management views provide centralized administration and monitoring of deployed clients. See the Netskope Client documentation and the Netskope Documentation portal for product documentation and current administrative guidance.

QUESTION NO: 8

Review the exhibit.

Netskope has been deployed using Cloud Explicit Proxy and PAC files. Authentication using Active Directory Federation Services (ADFS) has been configured for SAML Forward Proxy auth. When the users open their browser and try to go to a site, they receive the error shown in the exhibit.

What is a reason for this error?

A. The group attribute was not set in the Netskope SAML Forward Proxy configuration.

B. The Netskope nsauth proxy cannot reach the identity provider.

C. Netskope is not compatible with the identity provider.

D. There is an issue with the formatting of the ADFS certificate that was uploaded to the Netskope tenant for SAML Forward Proxy configuration.

ANSWER: D

Explanation:

There is an issue with the formatting of the ADFS certificate that was uploaded to the Netskope tenant for SAML Forward Proxy configuration. In a SAML Forward Proxy authentication flow, Netskope relies on the identity provider's signing certificate to validate the digital signature on the SAML assertion returned by ADFS. The certificate configured in the

Netskope tenant must therefore be the correct ADFS token-signing certificate and must be supplied in the expected PEM/Base64 X.509 format. If the certificate was copied with malformed PEM boundaries, contains invalid or extraneous characters, is incomplete, or is not the certificate corresponding to the signing key used by ADFS, Netskope cannot validate the assertion. The authentication transaction fails before the user can establish an authenticated proxy session, causing browser access attempts through the explicit proxy to fail. Re-exporting the currently active ADFS token-signing certificate in a supported format and carefully uploading its complete contents to the SAML Forward Proxy configuration restores signature validation. Certificate rollover should also be managed by updating the Netskope configuration whenever ADFS begins signing assertions with a replacement certificate. Netskope documents SAML-based authentication configuration and certificate requirements in its SAML authentication documentation; Microsoft describes the role of the AD FS token-signing certificate in its AD FS token-signing certificate guidance.

QUESTION NO: 9

Your organization uses the Netskope Client with dynamic steering. A financial SaaS application allows access only from the company's public egress IP address. Users can access the application while they are on the corporate network, but access fails when the application traffic is sent through the Netskope cloud.

You must preserve Netskope steering for all other Internet traffic. Which action would satisfy this requirement?

A. Configure a steering exception for the application FQDN and IP address.

B. Configure an SSL Do Not Decrypt policy for the application FQDN.

C. Create a Real-time Protection policy with an Allow action for the application.

D. Configure a Cloud Log Shipper destination for the application events.

ANSWER: A

Explanation:

Configure a steering exception for the financial SaaS application's required FQDN and IP address. A steering exception prevents the Netskope Client from forwarding matching traffic through the Netskope Security Cloud. When the user is on-premises, the excluded traffic follows the enterprise network's normal route and is translated to the corporate public egress IP address that the SaaS provider expects.

An SSL decryption exception would only prevent TLS inspection; it would not change the source IP seen by the SaaS provider. A Real-time Protection policy also cannot alter the traffic path or source IP. Source IP Anchoring can address similar requirements, but is not necessary when on-premises users can reach the destination through the existing corporate egress path.

QUESTION NO: 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

ANSWER: C

Explanation:

Enterprise Egress IPv4 is the correct source address. A dynamic-steering bypass tells the Netskope Client not to send matching application traffic through the Netskope Security Cloud/data plane. When an on-premises user accesses the IP-

restricted application, that bypassed traffic follows the enterprise's normal local network routing path. As it leaves the organization for the internet, the enterprise firewall, proxy, or NAT gateway translates the internal client address to the organization's public egress IPv4 address. This is therefore the address that the destination application must allowlist.

This behavior is particularly important for SaaS applications or partner services that enforce source-IP restrictions. Their allowlist should include the public IPv4 address or addresses used by the relevant enterprise internet egress points, rather than a Netskope data-plane address. Dynamic steering enables the client to make this steering decision according to the configured destination and network context, while a bypass preserves the direct enterprise path for the matching traffic. Netskope documentation for client and traffic-steering capabilities is available through the Netskope Documentation portal; additional product context for endpoint traffic steering is available on the Netskope One Client page.

QUESTION NO: 11

You need to monitor the health of configured IPsec or GRE tunnels.

In this scenario, which two methods are supported by Netskope to accomplish this task? (Choose two.)

A. Use Layer 4 health checks.

B. Use Dead Peer Detection.

C. Use ICMP keepalive probing.

D. Use Netskope Trust Portal.

ANSWER: A B

Explanation:

Netskope supports **Layer 4 health checks** and **Dead Peer Detection** for tunnel-health monitoring. Layer 4 health checks actively validate reachability through the configured tunnel by using transport-layer probes. This provides an operational indication that traffic can traverse the tunnel and reach the configured destination, rather than merely showing that a tunnel configuration exists. It is therefore useful for monitoring data-path availability and for steering or failover decisions where tunnel reachability is important.

Dead Peer Detection is an IPsec/IKE mechanism that periodically checks whether the remote IPsec peer remains responsive. If DPD messages are not acknowledged within the configured behavior and timers, the peer is treated as unavailable and the IPsec tunnel can be cleared or re-established. Together, active Layer 4 validation and IKE peer liveness detection provide complementary monitoring of configured tunnel connectivity. Netskope documentation and product resources are available through the Netskope Documentation portal and the Netskope Support Knowledge Portal, including deployment guidance for IPsec/GRE connectivity and tunnel monitoring.