ITCertTest

ITCERTTEST
IT Exam study guide / simulations

http://www.itcerttest.com

IT exam study guide / simulations

Exam : **NSK200**

Title : Netskope Certified Cloud Security Integrator (NCCSI)

Vendor : Netskope

Version : DEMO

NO.1 Your organization has three main locations with 30.000 hosts in each location. You are planning to deploy Netskope using iPsec tunnels for security.
What are two considerations to make a successful connection in this scenario? (Choose two.)
A. browsers in use
B. operating systems
C. redundant POPs
D. number of hosts
Answer: C D
Explanation:
To deploy Netskope using IPSec tunnels for security in this scenario, two considerations to make a successful connection are C. redundant POPs and D. number of hosts. Redundant POPs are Points of Presence that are geographically distributed data centers that host the Netskope cloud platform. You need to consider redundant POPs to ensure high availability and resiliency of your IPSec tunnels in case of a failure or outage in one of the POPs. You can configure multiple IPSec tunnels from your network to different POPs and use dynamic routing protocols such as BGP to load balance and failover the traffic1. Number of hosts is the number of devices or endpoints that will use the IPSec tunnels to access the cloud services. You need to consider the number of hosts to estimate the bandwidth and throughput requirements of your IPSec tunnels and choose the appropriate POPs that can handle the traffic volume. You can use the Netskope Bandwidth Calculator tool to estimate the bandwidth and throughput based on the number of hosts, locations, and cloud services2.
Therefore, options C and D are correct and the other options are incorrect. References: IPSec - Netskope Knowledge Portal, Netskope Bandwidth Calculator

NO.2 A customer wants to use Netskope to prevent PCI data from leaving the corporate sanctioned OneDrive instance. In this scenario. which two solutions would assist in preventing data exfiltration? (Choose two.)
A. API Data Protection
B. Cloud Firewall (CFW)
C. SaaS Security Posture Management (SSPM)
D. Real-time Protection
Answer: A D
Explanation:
To prevent PCI data from leaving the corporate sanctioned OneDrive instance, the customer can use API Data Protection and Real-time Protection. API Data Protection is a feature that allows you to discover, classify, and protect data that is already resident in your cloud services, such as OneDrive. You can create a policy that matches the PCI data based on criteria such as users, content, activity, or DLP profiles. Then, you can choose an action to prevent the PCI data from being shared or exfiltrated, such as remove external collaborators, remove public links, or quarantine3. Real-time Protection is a feature that allows you to inspect and control data in transit between your users and cloud services, such as OneDrive. You can create a policy that matches the PCI data based on criteria such as users, devices, locations, categories, or DLP profiles. Then, you can choose an action to prevent the PCI data from being uploaded or downloaded, such as block, alert, encrypt, or watermark4. Therefore, options A and D are correct and the other options are incorrect. References: API Data Protection - Netskope Knowledge Portal, Real-time Protection - Netskope Knowledge Portal

NO.3 You are having issues with fetching user and group Information periodically from the domain controller and posting that information to your tenant instance in the Netskope cloud. To begin the troubleshooting process, what would you Investigate first in this situation?

A. On-Premises Log Parser

B. Directory Importer

C. DNS Connector

D. AD Connector

Answer: B

Explanation:

The Directory Importer is a component of the Netskope Adapters that connects to the domain controller and periodically fetches user and group information to post that info to your tenant instance in the Netskope cloud1. If you are having issues with this process, the first thing you should investigate is the Directory Importer itself. You can check the status of the Directory Importer service, the configuration file, the logs, and the connectivity to the domain controller and the Netskope cloud2. Therefore, option B is correct and the other options are incorrect. References: Configure Directory Importer - Netskope Knowledge Portal, Troubleshooting Directory Importer - Netskop e Knowledge Portal

NO.4 You are an administrator writing Netskope Real-time Protection policies and must determine proper policy ordering.

Which two statements are true in this scenario? (Choose two.)

A. You must place Netskope private access malware policies in the middle.

B. You do not need to create an "allow all" Web Access policy at the bottom.

C. You must place DLP policies at the bottom.

D. You must place high-risk block policies at the top.

Answer: B D

Explanation:

To determine proper policy ordering for Netskope Real-time Protection policies, you need to follow these two statements: B. You do not need to create an "allow all" Web Access policy at the bottom. D. You must place high-risk block policies at the top. These statements are based on the best practices for policy ordering recommended by Netskope3. An "allow all" Web Access policy at the bottom is not necessary because any traffic that does not match any policy will be allowed by default. However, you can create a "monitor all" Web Access policy at the bottom if you want to log all the traffic that is not matched by any other policy4.

High-risk block policies at the top are important because they prevent any traffic that poses a serious threat or violates a critical compliance standard from reaching its destination. These policies should have higher priority than other policies that may allow or modify the traffic5. Therefore, options B and D are correct and the other options are incorrect. References: Real-time Protection Policies - Netskope Knowledge Portal, Create a Real-time Protection Policy for Web Categories - Netskope Knowledge Portal, Best Practices:

Real-time Protection Policies (1 of 2) - Netskope

NO.5 You are troubleshooting an issue with Microsoft where some users complain about an issue accessing OneDrive and SharePoint Online. The configuration has the Netskope client deployed and active for most users, but some Linux machines are routed to Netskope using GRE tunnels. You need

to disable inspection for all users to begin troubleshooting the issue.
In this scenario, how would you accomplish this task?

A. Create a Real-time Protection policy to isolate Microsoft 365.

B. Create a Do Not Decrypt SSL policy for the Microsoft 365 App Suite.

C. Create a steering exception for the Microsoft 365 domains.

D. Create a Do Not Decrypt SSL policy for OneDrive.

Answer: B

Explanation:
To disable inspection for all users accessing Microsoft 365, you need to create a Do Not Decrypt SSL policy for the Microsoft 365 App Suite. This policy will prevent Netskope from decrypting and analyzing the traffic for any Microsoft 365 app, regardless of the access method (Netskope client or GRE tunnel)3. This policy will also allow SNI-based policies to apply, but no deep analysis performed via Real-time Protection policies4. Therefore, option B is correct and the other options are incorrect. References: Add a Policy for SSL Decryption - Netskope Knowledge Portal, Default Microsoft appsuite SSL do not decrypt rule - Netskope Community

NO.6 Netskope is being used as a secure Web gateway. Your organization's URL list changes frequently. In this scenario, what makes It possible for a mass update of the URL list in the Netskope platform?

A. REST API v2

B. Assertion Consumer Service URL

C. Cloud Threat Exchange

D. SCIM provisioning

Answer: A

Explanation:
The method that makes it possible for a mass update of the URL list in the Netskope platform is A. REST API v2. REST API v2 is a feature that allows you to use an auth token to make authorized calls to the Netskope API and access resources via URI paths5. You can use REST API v2 to update a URL list with new values by providing the name of an existing URL list and a comma-separated list of URLs or IP addresses6. This can help you automate or script the management of your URL lists and keep them up-to-date. Therefore, option A is correct and the other options are incorrect. References: REST API v2 Overview - Netskope Knowledge Portal, Update a URL List - Netskope Knowledge Portal

NO.7 Your customer currently only allows users to access the corporate instance of OneDrive using SSO with the Netskope client. The users are not permitted to take their laptops when vacationing, but sometimes they must have access to documents on OneDrive when there is an urgent request. The customer wants to allow employees to remotely access OneDrive from unmanaged devices while enforcing DLP controls to prohibit downloading sensitive files to unmanaged devices.
Which steering method would satisfy the requirements for this scenario?

A. Use a reverse proxy integrated with their SSO.

B. Use proxy chaining with their cloud service providers integrated with their SSO.

C. Use a forward proxy integrated with their SSO.

D. Use a secure forwarder integrated with an on-premises proxy.

Answer: A

Explanation:
A reverse proxy integrated with their SSO would satisfy the requirements for this scenario. A reverse proxy intercepts requests from users to cloud apps and applies policies based on user identity, device posture, app, and data context. It can enforce DLP controls to prohibit downloading sensitive files to unmanaged devices. It can also integrate with the customer's SSO provider to authenticate users and allow access only to the corporate instance of OneDrive. The other steering methods are not suitable for this scenario because they either require the Netskope client or do not provide granular control over cloud app activities.

NO.8 You want to secure Microsoft Exchange and Gmail SMTP traffic for DLP using Netskope. Which statement is true about this scenario when using the Netskope client?

A. Netskope can inspect outbound SMTP traffic for Microsoft Exchange and Gmail.

B. Enable Cloud Firewall to Inspect Inbound SMTP traffic for Microsoft Exchange and Gmail.

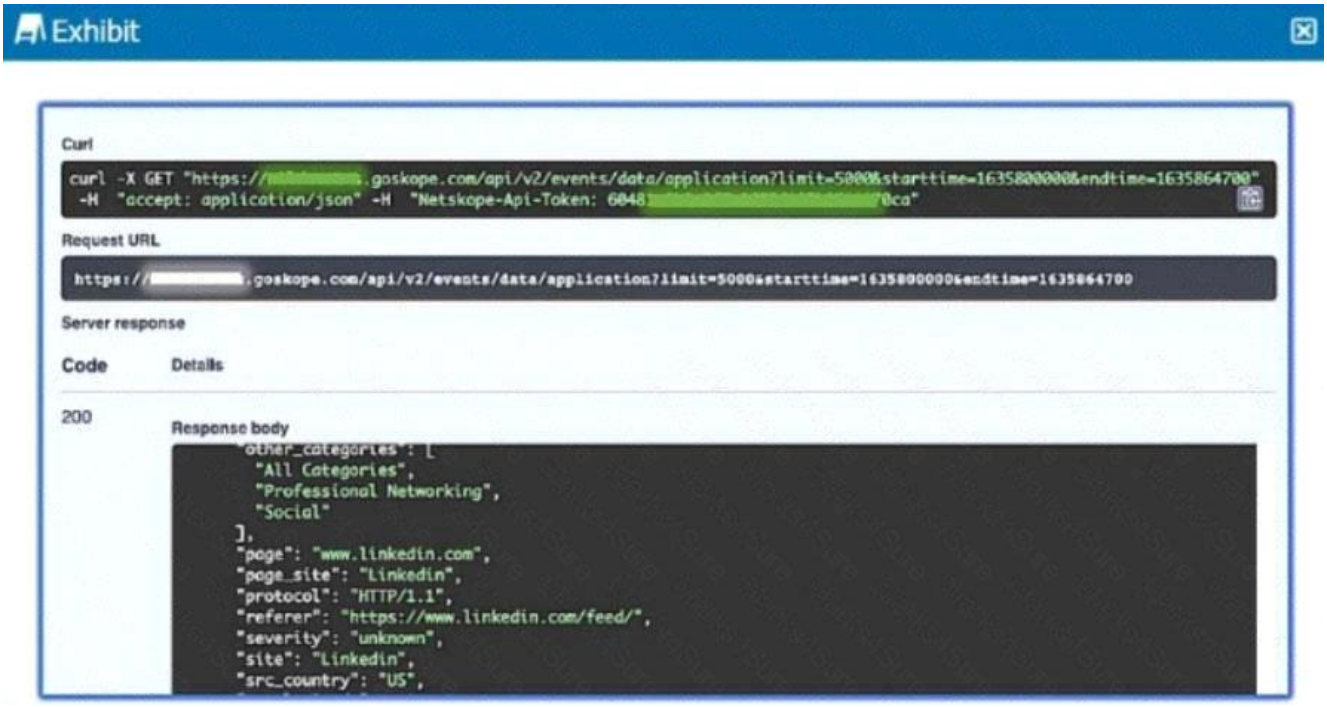
C. Netskope can inspect inbound and outbound SMTP traffic for Microsoft Exchange and Gmail.

D. Enable REST API v2 to Inspect inbound SMTP traffic for Microsoft Exchange and Gmail.

Answer: A

Explanation:
Netskope can inspect outbound SMTP traffic for Microsoft Exchange and Gmail using the Netskope client.
The Netskope client intercepts the SMTP traffic from the user's device and forwards it to the Netskope cloud for DLP scanning. The Netskope client does not inspect inbound SMTP traffic, as this is handled by the cloud email service or the MTA. Therefore, option A is correct and the other options are incorrect. References: Configure Netskope SMTP Proxy with Microsoft O365 Exchange, Configure Netskope SMTP Proxy with Gmail, SMTP DLP, Best Practices for Email Security with SMTP proxy

NO.9 Review the exhibit.



Referring to the exhibit, which three statements are correct? (Choose three.)

A. The request was processed successfully.

B. A request was submitted to extract application event details.
C. An invalid token was used.
D. The request was limited to the first 5000 records.
E. The request was confined to only the "Professional Networking and Social" category.
Answer: A B D
Explanation:
The "200" response code confirms that the request was processed successfully. The request URL indicates that it was set to retrieve application event data with a limit of 5000 records. Additionally, the response includes categories such as "Professional Networking and Social," verifying that these were part of the requested data.

NO.10 You are currently migrating users away from a legacy proxy to the Netskope client in the company's corporate offices. You have deployed the client to a pilot group; however, when the client attempts to connect to Netskope, it fails to establish a tunnel.
In this scenario, what would cause this problem?
A. The legacy proxy is intercepting SSL/TLS traffic to Netskope.
B. The corporate firewall is blocking UDP port 443 to Netskope.
C. The corporate firewall is blocking the Netskope EPoT address.
D. The client cannot reach dns.google for EDNS resolution.
Answer: B
Explanation:
The corporate firewall blocking UDP port 443 to Netskope could cause tunnel establishment failures. Netskope clients rely on this port for secure tunneling (via DTLS), so ensuring UDP port 443 is open is essential for connectivity. Additionally, legacy proxies intercepting traffic could also disrupt the SSL/TLS traffic necessary for the Netskope tunnel.