FreeCram

FreeCram

Instant Download | 365 Days Free Updates | Money Back Guarantee | Security & Privacy

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

We're not the only ones **happy** about FreeCram Practice Material ...

12514+ customers in 100+ countries use FreeCram Test Engine. Meet our customers.

https://www.freecram.com

Free Exam/Cram Practice Materials.

Exam : **NSK100**

Title : Netskope Certified Cloud Security Administrator (NCCSA)

Vendor : Netskope

Version : DEMO

NO.1 What are two primary advantages of Netskope's Secure Access Service Edge (SASE) architecture? (Choose two.

A. no on-premises hardware required for policy enforcement

B. Bayesian spam filtering

C. Endpoint Detection and Response (EDR)

D. single management console

Answer: A D

Explanation

Two primary advantages of Netskope's Secure Access Service Edge (SASE) architecture are: no on-premises hardware required for policy enforcement and single management console. Netskope's SASE architecture delivers network and security services as cloud-based services that can be accessed from any location and device. This eliminates the need for on-premises hardware appliances such as firewalls, proxies, VPNs, etc., that are costly to maintain and scale. Netskope's SASE architecture also provides a single management console that allows administrators to configure and monitor all the network and security services from one place. This simplifies IT operations and reduces complexity and overhead. References: Netskope SASEWhat is SASE?

NO.2 You want to deploy Netskope's zero trust network access (ZTNA) solution, NPA. In this scenario, which action would you perform to accomplish this task?

A. Create an OAuth identity access control between your users and your applications.

B. Set up a reverse proxy using SAML and an identity provider.

C. Enable Steer all Private Apps in your existing steering configuration(s) from the admin console.

D. Configure SCIM to exchange identity information and attributes with your applications.

Answer: C

Explanation

To deploy Netskope's zero trust network access (ZTNA) solution, NPA, you need to enable Steer all Private Apps in your existing steering configuration(s) from the admin console. This will allow you to create private app profiles and assign them to your applications. NPA will then provide secure and granular access to your applications without exposing them to the internet or requiring VPNs. References: [Netskope Private Access (NPA) Deployment Guide]

NO.3 What correctly defines the Zero Trust security model?

A. least privilege access

B. multi-layered security

C. strong authentication

D. double encryption

Answer: A

Explanation

The term that correctly defines the Zero Trust security model is least privilege access. The Zero Trust security model is a modern security strategy based on the principle: never trust, always verify. Instead of assuming everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an open network. One of the core principles of the Zero Trust model is to use least privilege access, which means granting users or systems only the minimum level of access they need to perform their tasks, and only for a limited

time. This helps reduce the attack surface and minimize the impact of a potential breach. References: Zero Trust Security - microsoft.comWhat is Zero Trust Security?
Principles of the Zero Trust Model

NO.4 You need to provide a quick view under the Skope IT Applications page showing only risky shadow IT cloud applications being used.
In this scenario, which two filter combinations would you use to accomplish this task? (Choose two.)
A. Sanctioned = No
B. CCL = High. Under Research
C. User Device Type = Windows Device
D. CCL = Medium. Low, Poor
Answer: A D
Explanation
To provide a quick view under the Skope IT Applications page showing only risky shadow IT cloud applications being used, you can use two filter combinations: Sanctioned = No and CCL = Medium, Low, Poor. The Sanctioned filter allows you to select whether you want to see only sanctioned or unsanctioned apps in your organization. Sanctioned apps are those that are approved and managed by your IT department, while unsanctioned apps are those that are used without authorization or oversight by your employees. Shadow IT refers to the use ofunsanctioned apps that may pose security or compliance risks for your organization. The CCL filter allows you to select the Cloud Confidence Level (CCL) ratings of the apps you want to see. The CCL rating is a measure of how enterprise-ready a cloud app is based on various criteria such as security, auditability, business continuity, etc. The CCL rating ranges from Excellent to Poor, with Excellent being the most secure and compliant and Poor being the least. Risky cloud apps are those that have a low CCL rating, such as Medium, Low, or Poor. By applying these two filters, you can narrow down the list of apps to only those that are unsanctioned and have a low CCL rating, which indicates that they are risky shadow IT cloud applications being used in your organization. References: SkopeIT ApplicationsNetskope Cloud Confidence Index

NO.5 You want to block access to sites that use self-signed certificates. Which statement is true in this scenario?
A. Certificate-related settings apply globally to the entire customer tenant.
B. Certificate-related settings apply to each individual steering configuration level.
C. Certificate-related settings apply to each individual client configuration level.
D. Self-signed certificates must be changed to a publicly trusted CA signed certificate.
Answer: B
Explanation
The statement that is true in this scenario is: Certificate-related settings apply to each individual steering configuration level. Certificate-related settings are the options that allow you to configure how Netskope handles SSL/TLS certificates for encrypted web traffic. For example, you can choose whether to allow or block self-signed certificates, expired certificates, revoked certificates, etc. You can also choose whether to enable SSL decryption for specific domains or categories. Certificate-related settings apply to each individual steering configuration level, which means that you can have different settings for different types of traffic or devices. For example, you can have one steering configuration for managed devices and another one for unmanaged devices, and apply different

certificate-related settings for each one. This allows you to customize your security policies based on your needs and preferences. References: Netskope SSL DecryptionNetskope Steering Configuration

NO.6 What are two CASB inline interception use cases? (Choose two.)

A. blocking file uploads to a personal Box account

B. running a retroactive scan for data at rest in Google Drive

C. using the Netskope steering client to provide user alerts when sensitive information is posted in Slack

D. scanning Dropbox for credit card information

Answer: A C

Explanation

CASB inline interception use cases are scenarios where you need to apply real-time policies and actions on the traffic between users and cloud applications. For example, you may want to block file uploads to a personal Box account to prevent data leakage or exfiltration. You can use Netskope's inline proxy mode to intercept and inspect the traffic between users and Box, and apply granular policies based on user identity, device type, app instance, file metadata, etc. You can also use Netskope's inline proxy mode to provide user alerts when sensitive information is posted in Slack. For example, you may want to warn users when they share credit card numbers or social security numbers in Slack channels or messages. You can use Netskope's steering client to redirect the traffic between users and Slack to Netskope's inline proxy for inspection and enforcement. You can also use Netskope's DLP engine to detect sensitive data patterns and apply actions such as alerting or blocking. References: Netskope Inline Proxy ModeNetskope Steering Client [Netskope DLP Engine]