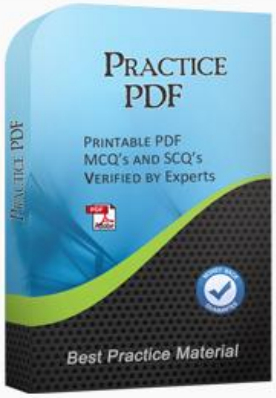
ActualtestsQuiz

ActualtestsQuiz

- Online Tool, Convenient, easy to study.
- Instant Online Access
- Supports All Web Browsers
- Practice Online Anytime
- Test History and Performance Review
- Supports Windows / Mac / Android / iOS, etc.

- Installable Software Application
- Simulates Real Exam Environment
- Builds Exam Confidence
- Supports MS Operating System
- Two Modes For Practice
- Practice Offline Anytime



- Printable PDF Format
- Prepared by IT Experts
- Instant Access to Download
- Study Anywhere, Anytime
- 365 Days Free Updates
- Free PDF Demo Available

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 90 days after purchasing. And Free get any another product.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

Exam : **NSK100-JPN**

Title : Netskope Certified Cloud Security Administrator (NCCSA) (NSK100日本語版)

Vendor : Netskope

Version : DEMO

QUESTION NO: 1
Netskopeのセキュアアクセスサービスエッジ(SASE)アーキテクチャの主な利点は2つあります。
A. ポリシー適用にオンプレミスのハードウェアは不要です
B. ベイズ型スパムフィルタリング
C. エンドポイント検出および対応 (EDR)
D.単一管理コンソール
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?

QUESTION NO: 2
Netskopeのゼロトラストネットワークアクセス(ZTNA)ソリューションであるNPAを導入したいとします。この場合、このタスクを完了するためにどのような操作を実行しますか？
A. ユーザーとアプリケーション間のOAuth IDアクセス制御を作成します。
B. SAMLとIDプロバイダを使用してリバースプロキシを設定します。
C.
管理コンソールから、既存のステアリング設定で「すべてのプライベートアプリをステアリングする」を有効にします。
D.SCIMを設定して、アプリケーションとID情報および属性を交換するようにします。
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]

QUESTION NO: 3
ゼロトラストセキュリティモデルを正しく定義するものは何ですか？
A. 最小権限アクセス
B. 多層セキュリティ
C. 強力な認証
D. 二重暗号化
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

QUESTION NO: 4
Skope
ITアプリケーションページの下に、リスクの高いシャドウITクラウドアプリケーションのみを表示するクイックビューを提供する必要があります。
このシナリオでは、このタスクを達成するためにどの2つのフィルターの組み合わせを使用しますか？(2つ選択してください。)
A. 承認済み = いいえ
B. CCL = 高。研究中。
C. ユーザーデバイスの種類 = Windowsデバイス
D. CCL = 中程度。低、不良
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

QUESTION NO: 5
自己署名証明書を使用しているサイトへのアクセスをブロックしたい場合、次のうちどれが正しいでしょうか？
A.証明書関連の設定は、顧客テナント全体にグローバルに適用されます。
B.証明書関連の設定は、各ステアリング構成レベルごとに適用されます。

C.証明書関連の設定は、個々のクライアント構成レベルごとに適用されます。
D.
自己署名証明書は、公的に信頼された認証局が署名した証明書に変更する必要があります。
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

QUESTION NO: 6
CASBのインライン傍受における2つのユースケースを挙げてください。(2つ選択してください。)
A. 個人用Boxアカウントへのファイルアップロードをブロックする
B. Googleドライブに保存されているデータの遡及スキャンを実行中
C.
Netskopeステアリングクライアントを使用して、Slackに機密情報が投稿された際にユーザーにアラートを提供する
D.Dropboxをスキャンしてクレジットカード情報を取得中
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]