Free Questions for NSK101 by dumpshq

Shared by Warren on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What are two pillars of CASB? (Choose two.)

Options:

A- visibility

B- compliance

C- cloud native

D- SASE

Answer:

A, B

Explanation:

Two pillars of CASB are visibility and compliance. CASB stands for Cloud Access Security Broker, which is a solution that provides visibility and control over cloud services and web traffic, as well as data and threat protection for cloud users and devices. Visibility is the capability to identify all cloud services in use and assess their risk factors, such as security, auditability, business continuity, etc.

Compliance is the capability to ensure that cloud services and data meet the regulatory standards and policies of the organization or industry, such as GDPR, HIPAA, PCI DSS, etc.Reference:What Is a Cloud Access Security Broker (CASB)? | MicrosoftCASB Guide: What are the 4 Pillars of CASB? - Security Service Edge

Question 2

Question Type: MultipleChoice

Which three statements are correct about Netskope's NewEdge Security Cloud Network Infrastructure? (Choose three.)

Options:

A- It takes advantage of the public cloud by deploying security services on Google Cloud Platform.

B- It includes direct peering with Microsoft and Google in every data center.

C- It is a private security cloud network that is massively over provisioned, highly elastic, and built for scale.

D- It delivers a single, unified network with no surcharges or reliance on public cloud infrastructure or virtual PoPs.

E- It simplifies the administrator's job by limiting access to pre-defined availability zones.

Answer:

B, C, D

Explanation:

Netskope's NewEdge Security Cloud Network Infrastructure is a global network that powers the Netskope Security Cloud, providing real-time inline and out-of-band API-driven services for cloud and web security. Three statements that are correct about Netskope's NewEdge Security Cloud Network Infrastructure are:

It includes direct peering with Microsoft and Google in every data center. This means that Netskope has established high-speed, low-latency connections with these major cloud service providers, ensuring optimal performance and user experience for their customers. Direct peering also reduces the risk of network congestion, packet loss, or routing issues that may affect the quality of service.

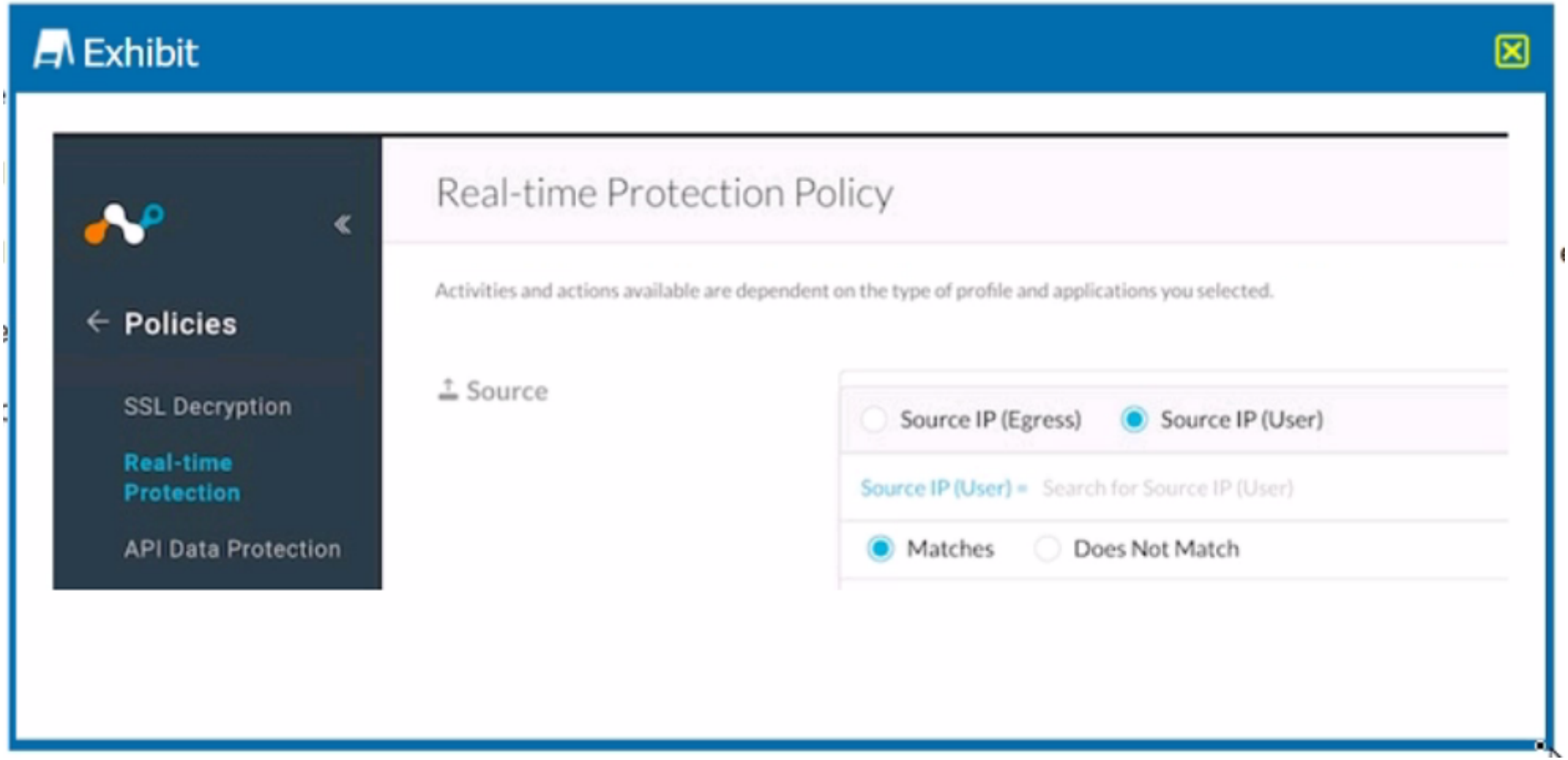
It is a private security cloud network that is massively over provisioned, highly elastic, and built for scale. This means that Netskope owns and operates its own network infrastructure, without relying on third-party providers or public cloud platforms. Netskope has invested over $150 million to build the world's largest and fastest security private cloud, with data centers in more than 65 regions and growing. Netskope can dynamically scale its network capacity and resources to meet the growing demand and traffic volume of its customers, without compromising on security or performance.

It delivers a single, unified network with no surcharges or reliance on public cloud infrastructure or virtual PoPs. This means that Netskope provides a consistent and transparent network service to its customers, regardless of their location or device. Netskope does not charge any additional fees or hidden costs for accessing its network services, unlike some other providers that may impose surcharges based on geography or bandwidth usage. Netskope also does not use virtual points of presence (PoPs) that are hosted on public cloud platforms, which may introduce latency, complexity, or security risks.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



Click the Exhibit button.

Referring to the exhibit, which statement accurately describes the difference between Source IP (Egress) and Source IP (User) address?

Options:

A- Source IP (Egress) is the IP address of the destination Web server while Source IP (User) is the IP address assigned to your network.

B- Source IP (Egress) is the IP address assigned to the endpoint host IP address while Source IP (User) is the public IP address of your Internet edge router.

C- You must always leave the source IP fields blank and configure the user identity as a source criteria.

D- Source IP (Egress) is the public IP address of your Internet edge router while Source IP (User) is the address assigned to the endpoint.

Answer:

D

Explanation:

The statement that accurately describes the difference between Source IP (Egress) and Source IP (User) address is: Source IP (Egress) is the public IP address of your Internet edge router while Source IP (User) is the address assigned to the endpoint. Source IP (Egress) is the IP address that is visible to external networks when you send traffic from your network to the Internet. It is usually the IP address of your Internet edge router or gateway that performs NAT (Network Address Translation). Source IP (User) is the IP address that is assigned to your endpoint device, such as a laptop or a smartphone, within your network. It is usually a private IP address that is not routable on the Internet. You can use these two criteria to filter traffic based on where it originates from within your network or outside your network.Reference:Source Address / Source Port vs Destination Address / Destination PortHow to explain Source IP Address, Destination IP Address & Service in easy way

Question 4

Question Type: MultipleChoice

What are two primary advantages of Netskope's Secure Access Service Edge (SASE) architecture? (Choose two.

Options:

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.Reference:Netskope SASEWhat is SASE?

Question 5

Question Type: **MultipleChoice**

Exhibit

Exhibit

Violations

PCI-DSS.txt

Overview

POLICY	VIOLATIONS
Control - Upload and Post Data Loss	2 DLP Rule Violations

RULE HIT	POLICIES	SEVERITY
INTL-PAN-Exp-Name	Control - Upload and Post Data Loss	Low (Count: 1)
INTL-PAN-Name	Control - Upload and Post Data Loss	Low (Count: 1)

DLP Rule Violations (#1 - 2)

#	PREVIEW	RULE	DLP PROFILE	DLP POLICY
1	MC AMEX Robert ...514-14-8905 5370-46XX-XXXX-3020 Thomas Conley 690- 05-5315 4916-4811-5814-8111	INTL-PAN-Exp-Name	Payment Card Industry Data Security Standard. PCI-DSS	Control - Upload and Post Data Loss
2	MC AMEX Robert Aragon 489-36-8350 4929-38XX-XXXX-4295 Ashley	INTL-PAN-Name	Payment Card Industry Data Security Standard. PCI-DSS	Control - Upload and Post Data Loss

Which portion of the interface shown in the exhibit allows an administrator to set severity, assign ownership, track progress, and perform forensic analysis with excerpts of violating content?

Options:

A- Skope IT-> Alerts

B- Incidents -> DLP

C- API-enabled Protection -> Inventory

D- Reports -> New Report

Answer:

B

Explanation:

The portion of the interface shown in the exhibit that allows an administrator to set severity, assign ownership, track progress, and perform forensic analysis with excerpts of violating content is Incidents -> DLP. The Incidents dashboard provides a comprehensive view of all the incidents that have occurred in your cloud environment, such as DLP violations, malware infections, anomalous activities, etc. You can filter the incidents by various criteria, such as app name, incident type, severity, user name, etc. You can also drill down into each incident to see more details, such as file name, file path, file owner, file size, file type, etc. You can also assign an owner to an incident, change its status and severity, add notes or comments, and view the excerpts of the violating content that triggered the DLP

policy.Reference:Netskope Incidents Dashboard

Question 6

Question Type: MultipleChoice

You want to prevent Man-in-the-Middle (MITM) attacks on an encrypted website or application. In this scenario, which method would you use?

Options:

A- Use a stronger encryption algorithm.

B- Use certificate pinning.

C- Use a proxy for the connection.

D- Use a weaker encryption algorithm.

Answer:

B

Explanation:

To prevent Man-in-the-Middle (MITM) attacks on an encrypted website or application, one method that you can use is certificate pinning. Certificate pinning is a technique that restricts which certificates are considered valid for a particular website or application, limiting risk. Instead of allowing any trusted certificate to be used, operators 'pin' the certificate authority (CA) issuer(s), public keys or even end-entity certificates of their choice. Certificate pinning helps to prevent MITM attacks by validating the server certificates against a hardcoded list of certificates in the website or application. If an attacker tries to intercept or modify the traffic using a fraudulent or compromised certificate, it will be rejected by the website or application as invalid, even if it is signed by a trusted CA.Reference:Certificate pinning - IBMCertificate and Public Key Pinning | OWASP Foundation

Question 7

Question Type: MultipleChoice

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.)

Options:

A- Sanctioned = No

B- CCL = High. Under Research

B- 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 of unsanctioned 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.Reference:SkopeIT ApplicationsNetskope Cloud Confidence Index

Question 8

Question Type: MultipleChoice

In which scenario would you use a SAML reverse proxy?

Options:

A- When the API-enabled protection exceeds the Cloud App API usage limits and cannot be used anymore.

B- When the organization wants to perform inline inspection of cloud application traffic for roaming users that do not have the Netskope agent installed.

C- When there are multiple SAML IdPs in use and the SAML reverse proxy can help federate them all together.

D- When PAC files or explicit proxies can be used to steer traffic to the Netskope platform.

Answer:

C

Explanation:

A SAML reverse proxy is a service that acts as an intermediary between a SAML service provider (SP) and one or more SAML identity providers (IdPs). It can perform various functions, such as authentication, authorization, load balancing, caching, etc. One scenario

where you would use a SAML reverse proxy is when there are multiple SAML IdPs in use and the SAML reverse proxy can help federate them all together. For example, suppose you have an internal application that needs to authenticate users from different domains or organizations, each with their own SAML IdP. Instead of configuring the application to trust each IdP separately, you can use a SAML reverse proxy to act as a single SP for the application and a single IdP for the users. The SAML reverse proxy can then redirect the users to their respective IdPs for authentication and relay the SAML assertions back to the application. This way, you can simplify the integration and management of multiple SAML IdPs and provide a seamless user experience.Reference:SAML Reverse ProxyWhat is application proxy & SAML SSO?

Question 9

Question Type: MultipleChoice

Which two use cases would be considered examples of Shadow IT within an organization? (Choose two.)

Options:

A- a sanctioned Salesforce account used by a contractor to upload non-sensitive data

B- a sanctioned Wetransfer being used by a corporate user to share sensitive data

C- an unsanctioned Microsoft 365 OneDrive account being used by a corporate user to upload sensitive data

D- an unsanctioned Google Drive account used by a corporate user to upload non-sensitive data

Answer:

C, D

Explanation:

Shadow IT is the term for the unauthorized use of IT resources and functions by employees within an organization. It can include cloud services, software, and hardware that are not approved or managed by the IT department. Two use cases that would be considered examples of shadow IT within an organization are: an unsanctioned Microsoft 365 OneDrive account being used by a corporate user to upload sensitive data and an unsanctioned Google Drive account used by a corporate user to upload non-sensitive data. In both cases, the corporate user is using a personal cloud storage service that is not sanctioned by the organization to store work-related data. This can introduce security risks, such as data leakage, data loss, compliance violations, malware infections, etc. The IT department may not have visibility or control over these cloud services or the data stored in them.Reference:What is shadow IT? | CloudflareWhat is Shadow IT? | IBM

Question 10

Question Type: MultipleChoice

A customer wants to detect misconfigurations in their AWS cloud instances.

In this scenario, which Netskope feature would you recommend to the customer?

Options:

A- Netskope Secure Web Gateway (SWG)

B- Netskope Cloud Security Posture Management (CSPM)

C- Netskope Advanced DLP and Threat Protection

D- Netskope SaaS Security Posture Management (SSPM)

Answer:

B

Explanation:

If a customer wants to detect misconfigurations in their AWS cloud instances, the Netskope feature that I would recommend to them is Netskope Cloud Security Posture Management (CSPM). Netskope CSPM is a service that provides continuous assessment and remediation of public cloud deployments for risks, threats, and compliance issues. Netskope CSPM leverages the APIs available from AWS and other cloud service providers to scan the cloud infrastructure for misconfigurations, such as insecure permissions, open ports, unencrypted data, etc. Netskope CSPM also provides security posture policies, profiles, and rules that can be customized to match the customer's security standards and best practices. Netskope CSPM can also alert, report, or remediate the misconfigurations automatically or manually.Reference:Netskope CSPMCloud Security Posture Management

Question 11

Question Type: MultipleChoice

Which two functions are available for both inline and API protection? (Choose two.)

Options:

A- multi-factor authentication

B- threat protection

C- DLP

D- Cloud Security Posture Management (CSPM)

Answer:

B, C

Explanation:

Netskope provides both inline and API protection for cloud applications and web traffic. Inline protection refers to the real-time inspection and enforcement of policies on the traffic between users and cloud applications, using Netskope's inline proxy mode. API protection refers to the retrospective inspection and enforcement of policies on the data that is already stored in cloud applications, using Netskope's API connectors. Two functions that are available for both inline and API protection are threat protection and DLP. Threat protection is the capability to detect and block malware, ransomware, phishing, and other cyber threats that may compromise cloud data or users. DLP is the capability to detect and protect sensitive data, such as personal information, intellectual property, or regulated data, that may be exposed or leaked through cloud applications.Reference:Netskope Inline Proxy ModeNetskope API ProtectionNetskope Threat ProtectionNetskope DLP Engine