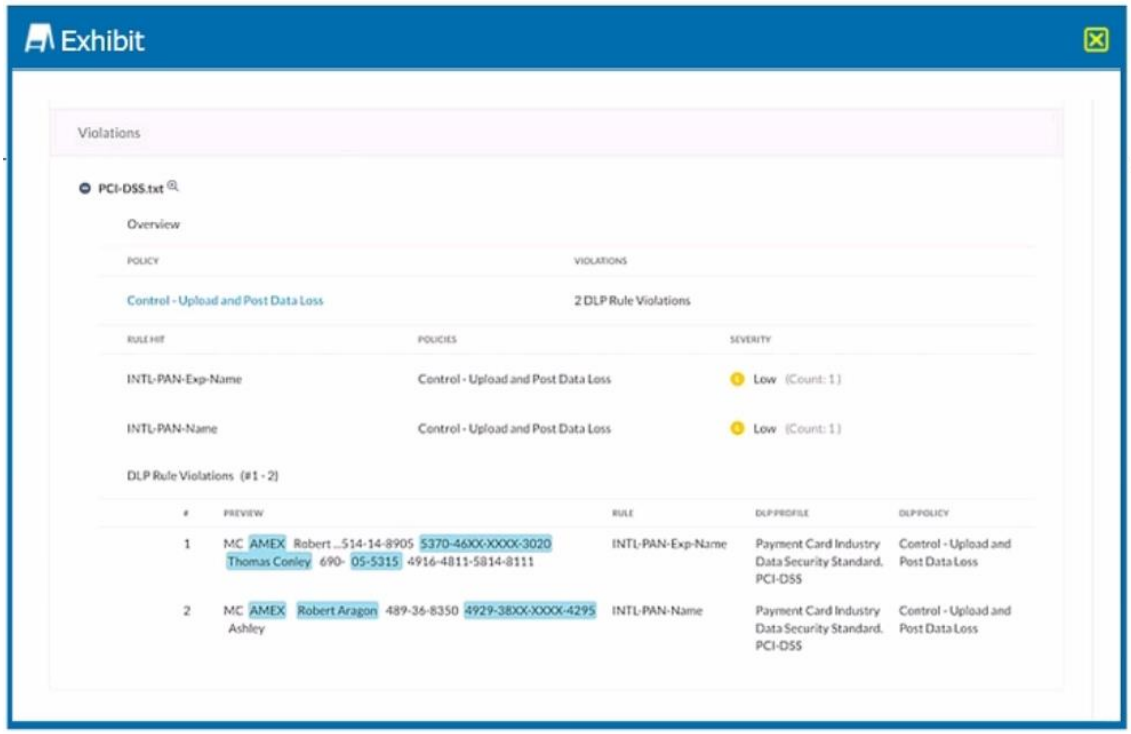
Vendor: Netskope

Exam Code: NSK100

Exam Name: Netskope Certified Cloud Security Administrator Exam

Version: DEMO

QUESTION 1
Referring to the exhibit. 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?



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.

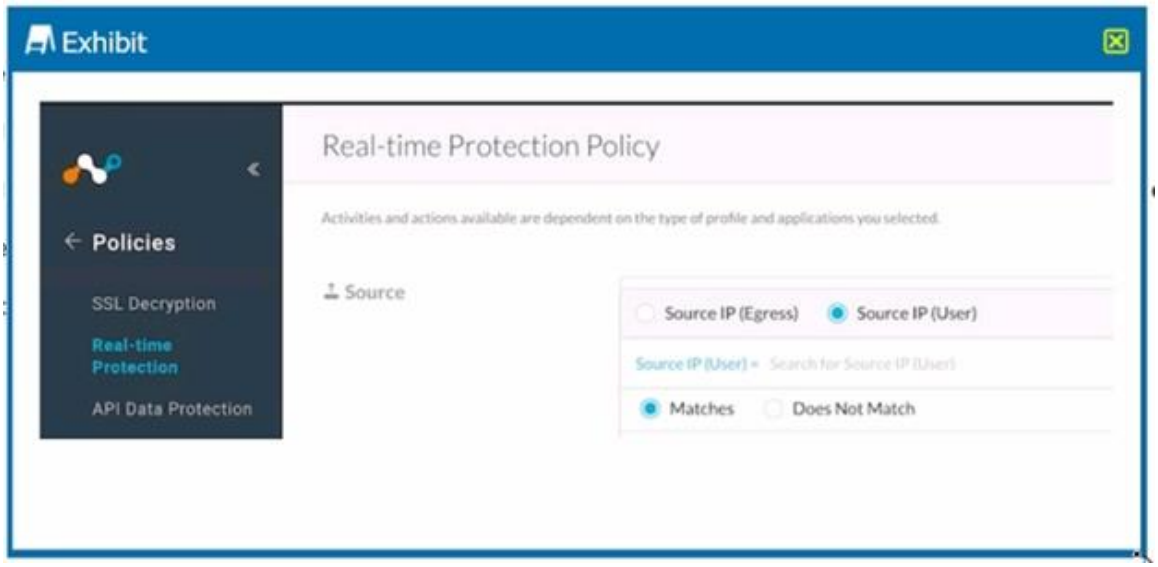
QUESTION 2
What are two primary advantages of Netskope's Secure Access Service Edge (SASE) architecture? (Choose two.)

A. no on-premises hardware required for policy enforcement
B. Bayesian spam filtering
C. Endpoint Detection and Response (EDR)

D. single management console

Answer: AD
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.

QUESTION 3
Referring to the exhibit, which statement accurately describes the difference between Source IP (Egress) and Source IP (User) address?



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.

QUESTION 4
Which three statements are correct about Netskope's NewEdge Security Cloud Network Infrastructure? (Choose three.)

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: BCD
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 5
What are two pillars of CASB? (Choose two.)

A. visibility
B. compliance
C. cloud native
D. SASE

Answer: AB
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.

QUESTION 6
You want to set up a Netskope API connection to Box.
What two actions must be completed to enable this connection? (Choose two.)

A. Install the Box desktop sync client.
B. Authorize the Netskope application in Box.
C. Integrate Box with the corporate IdP.
D. Configure Box in SaaS API Data protection.

Answer: BD
Explanation:
To set up a Netskope API connection to Box, two actions that must be completed are: authorize the Netskope application in Box and configure Box in SaaS API Data protection. Authorizing the Netskope application in Box allows Netskope to access the Box API and perform out-of-band inspection and enforcement of policies on the data that is already stored in Box. Configuring Box in SaaS API Data protection allows you to specify the Box instance details, such as domain name, admin email, etc., and enable features such as retroactive scan, event stream, etc.

QUESTION 7
When using an out-of-band API connection with your sanctioned cloud service, what are two capabilities available to the administrator? (Choose two.)

A. to quarantine malware
B. to find sensitive content
C. to block uploads
D. to allow real-time access

Answer: AB
Explanation:
When using an out-of-band API connection with your sanctioned cloud service, two capabilities available to the administrator are: to quarantine malware and to find sensitive content. An out-of-band API connection is a method of integrating Netskope with your cloud service provider using the APIs exposed by the cloud service. This allows Netskope to access the data that is already stored in the cloud service and perform retrospective inspection and enforcement of policies. One capability that the administrator can use with an out-of-band API connection is to quarantine malware. This means that Netskope can scan the files in the cloud service for malware, ransomware, phishing, and other threats, and move them to a quarantine folder or delete them if they are found to be malicious. Another capability that the administrator can use with an out-of-band API connection is to find sensitive content. This means that Netskope can scan the files in the cloud service for sensitive data, such as personal information, intellectual property, or regulated data, and apply data loss prevention (DLP) policies to protect them. For example, Netskope can encrypt, redact, or watermark the files that contain sensitive content, or notify the administrator or the file owner about the exposure.

QUESTION 8
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.

QUESTION 9
How do you provision users to your customer's Netskope tenant? (Choose two.)

A. Use Microsoft Intune.
B. Use the AD Connector.
C. Use SCIM.
D. Use the Directory Importer.

Answer: BD
Explanation:
To provision users to your customer's Netskope tenant, two methods that you can use are: use the AD Connector and use SCIM. The AD Connector is a tool that allows you to synchronize users and groups from your Active Directory (AD) domain to your Netskope tenant. The AD Connector runs as a Windows service on a machine that has access to your AD domain controller. The AD Connector periodically queries your AD domain for any changes in users and groups and updates them in your Netskope tenant accordingly. The AD Connector also supports filtering users and groups based on attributes or organizational units (OUs). SCIM stands for System for Cross-domain Identity Management, which is a standard protocol for managing user identities across different applications and services. SCIM allows you to provision users and groups from your identity provider (IdP), such as Azure AD or Okta, to your Netskope tenant using APIs. SCIM also supports creating, updating, deleting, and searching users and groups in your Netskope tenant based on your IdP's configuration.

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**