Free Questions for NSK200 by certscare

Shared by Battle on 22-07-2024

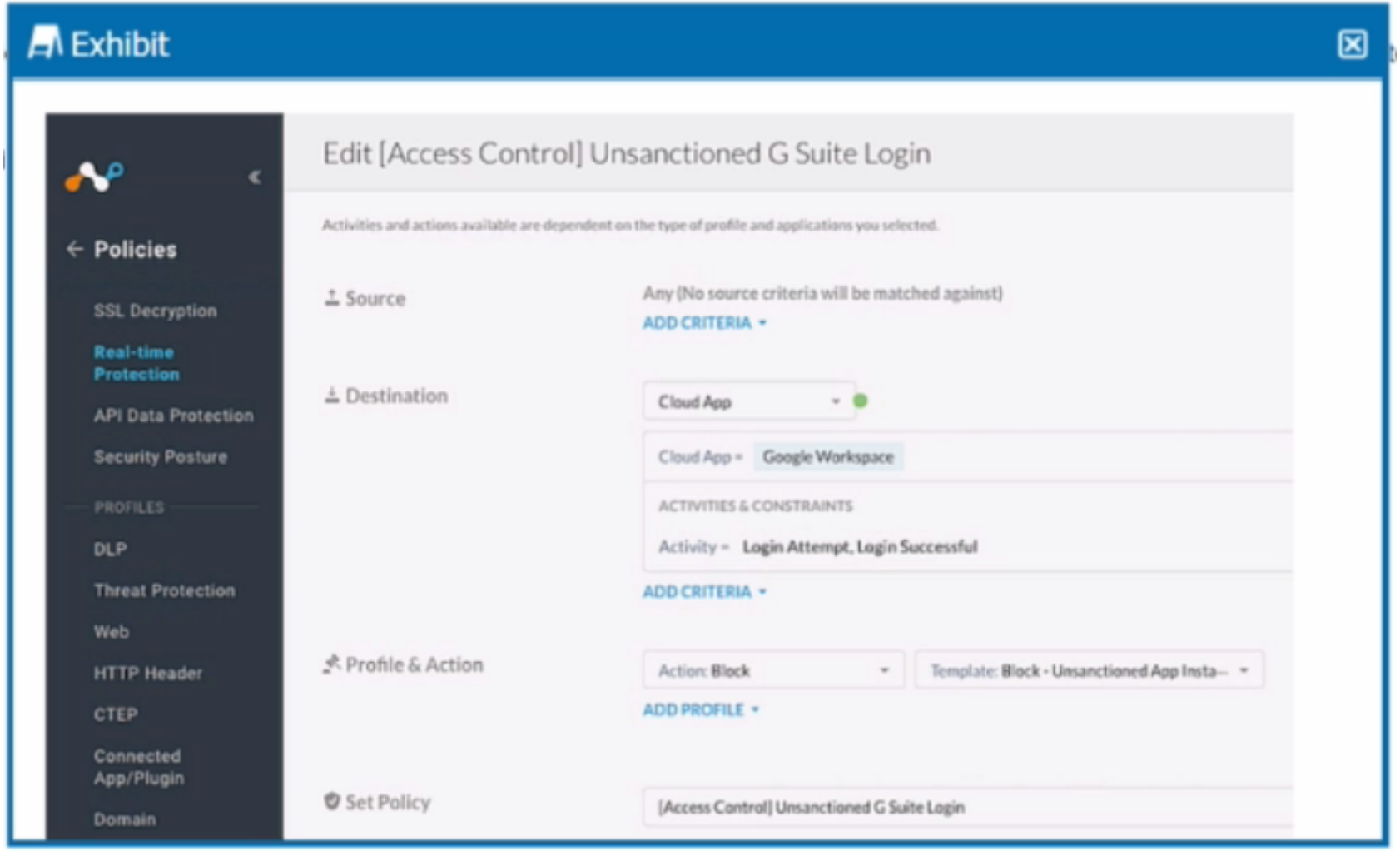
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Review the exhibit.



Your company uses Google as the corporate collaboration suite; however, corporate policy restricts the use of personal Google services. The exhibit provides a partially completed policy to ensure that users cannot log into their personal account.

What should be added to achieve the desired outcome in this scenario?

Options:

A- Google Gmail app

B- User Constraint

C- DLP profile

D- Device classification

Answer:

B

Explanation:

In order to restrict users from logging into their personal Google accounts, the policy should include a user constraint. This will ensure that only users with corporate accounts can access the corporate collaboration suite. The user constraint can be added by selecting the "User" option in the "Source" field and then choosing the appropriate user group or identity provider. The other options are not relevant for this scenario.Reference: [Creating a Policy to Block Personal Google Services], [Policy Creation], [User Constraint]

Question 2

Question Type: MultipleChoice

To which three event types does Netskope's REST API v2 provide access? (Choose three.)

Options:

A- application

B- alert

C- client

D- infrastructure

E- user

Answer:

A, B, D

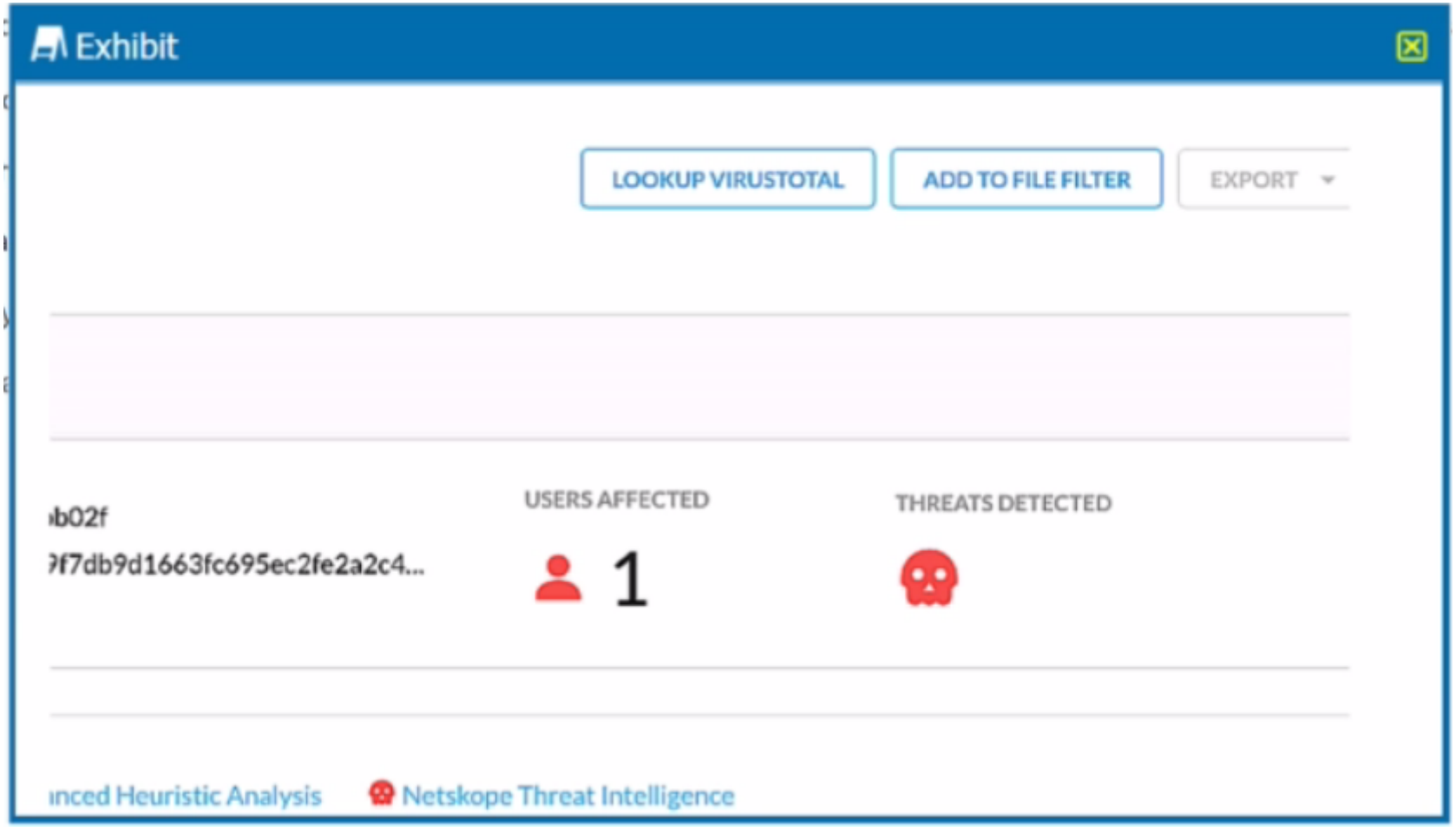
Explanation:

Netskope's REST API v2 provides access to various event types via URI paths. The event types include application, alert, infrastructure, audit, incident, network, and page. These event types can be used to retrieve data from Netskope's cloud security platform. The event types client and user are not supported by the REST API v2.Reference:REST API v2 Overview,Cribl Netskope Events and Alerts Integration,REST API Events and Alerts Response Descriptions

Question 3

Question Type: MultipleChoice

Review the exhibit.



You are at the Malware Incident page. A virus was detected by the Netskope Heuristics Engine. Your security team has confirmed that the virus was a test data file You want to allow the security team to use this file

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

Options:

A- Click the 'Add To File Filter button to add the IOC to a file list.

B- Contact the CrowdStrike administrator to have the file marked as safe.

C- Click the "Lookup VirusTotal' button to verify if this IOC is a false positive.

D- Create a malware detection profile and update the file hash list with the IOC.

Answer:

A, C

Explanation:

To allow the security team to use the test data file that was detected as a virus by the Netskope Heuristics Engine, the following two steps are correct:

Click the "Add To File Filter" button to add the IOC to a file list. This will exclude the file from future malware scans and prevent false positive alerts.The file list can be managed in the Settings > File Filter page1.

Click the "Lookup VirusTotal" button to verify if this IOC is a false positive. This will open a new tab with the VirusTotal report for the file hash. VirusTotal is a service that analyzes files and URLs for viruses, worms, trojans, and other kinds of malicious content.The report will show how many antivirus engines detected the file as malicious and provide additional information about the file2.

https://docs.netskope.com/en/netskope-help/admin-console/incidents/

Question 4

Question Type: MultipleChoice

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.)

Options:

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.Reference:IPSec - Netskope Knowledge Portal,Netskope Bandwidth Calculator

Question 5

Question Type: MultipleChoice

Review the exhibit.

You receive a service request from a user who indicates that their Netskope client is in a disabled state. The exhibit shows an excerpt (rom the affected client nsdebuglog.log.

What is the problem in this scenario?

Options:

A- User authentication failed during IdP-based enrollment.

B- The Netskope client connection is being decrypted.

C- Custom installation parameters are incorrectly specified

D- The user's account has not been provisioned into Netskope.

Answer:

B

Explanation:

The problem in this scenario is that the Netskope client connection is being decrypted by a network security device. This is evident from the log message "ERROR SSL certificate verification failed: self signed certificate in certificate chain". This means that the Netskope client is receiving a certificate that is not issued by Netskope, but by a device that is intercepting and decrypting the traffic between the client and the Netskope cloud.This can cause the client to fail to download the required configuration and remain in a disabled state1. Therefore, option B is correct and the other options are incorrect.Reference:Troubleshooting Netskope Client - Netskope Knowledge Portal,Using Netskope Client - Netskope Knowledge Portal

Question 6

Question Type: MultipleChoice

Which object would be selected when creating a Malware Detection profile?

Options:

A- DLP profile

B- File profile

C- Domain profile

D- User profile

Answer:

B

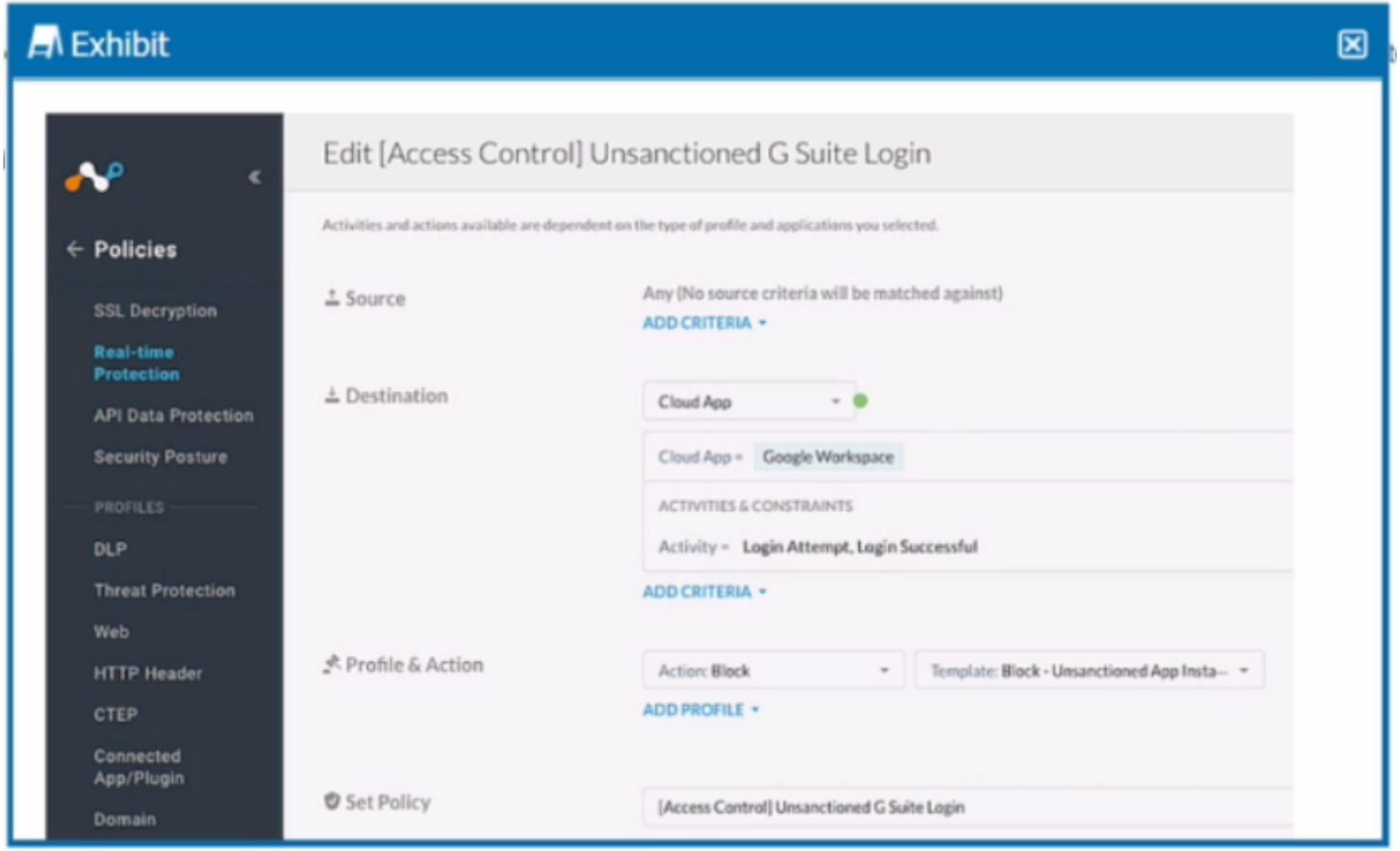
Explanation:

A file profile is an object that contains a list of file hashes that can be used to create a malware detection profile. A file profile can be configured as an allowlist or a blocklist, depending on whether the files are known to be benign or malicious.A file profile can be created in the Settings > File Profile page1. A malware detection profile is a set of rules that define how Netskope handles malware incidents.A malware detection profile can be created in the Policies > Threat Protection > Malware Detection Profiles page2. To create a malware detection profile, one needs to select a file profile as an allowlist or a blocklist, along with the Netskope malware scan option. The other options are not objects that can be selected when creating a malware detection profile.

Question 7

Question Type: MultipleChoice

Review the exhibit.



Your company uses Google as the corporate collaboration suite; however, corporate policy restricts the use of personal Google services. The exhibit provides a partially completed policy to ensure that users cannot log into their personal account.

What should be added to achieve the desired outcome in this scenario?

Options:

A- Google Gmail app

B- User Constraint

C- DLP profile

D- Device classification

Answer:

B

Explanation:

In order to restrict users from logging into their personal Google accounts, the policy should include a user constraint. This will ensure that only users with corporate accounts can access the corporate collaboration suite. The user constraint can be added by selecting the "User" option in the "Source" field and then choosing the appropriate user group or identity provider. The other options are not relevant for this scenario.Reference: [Creating a Policy to Block Personal Google Services], [Policy Creation], [User Constraint]