IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

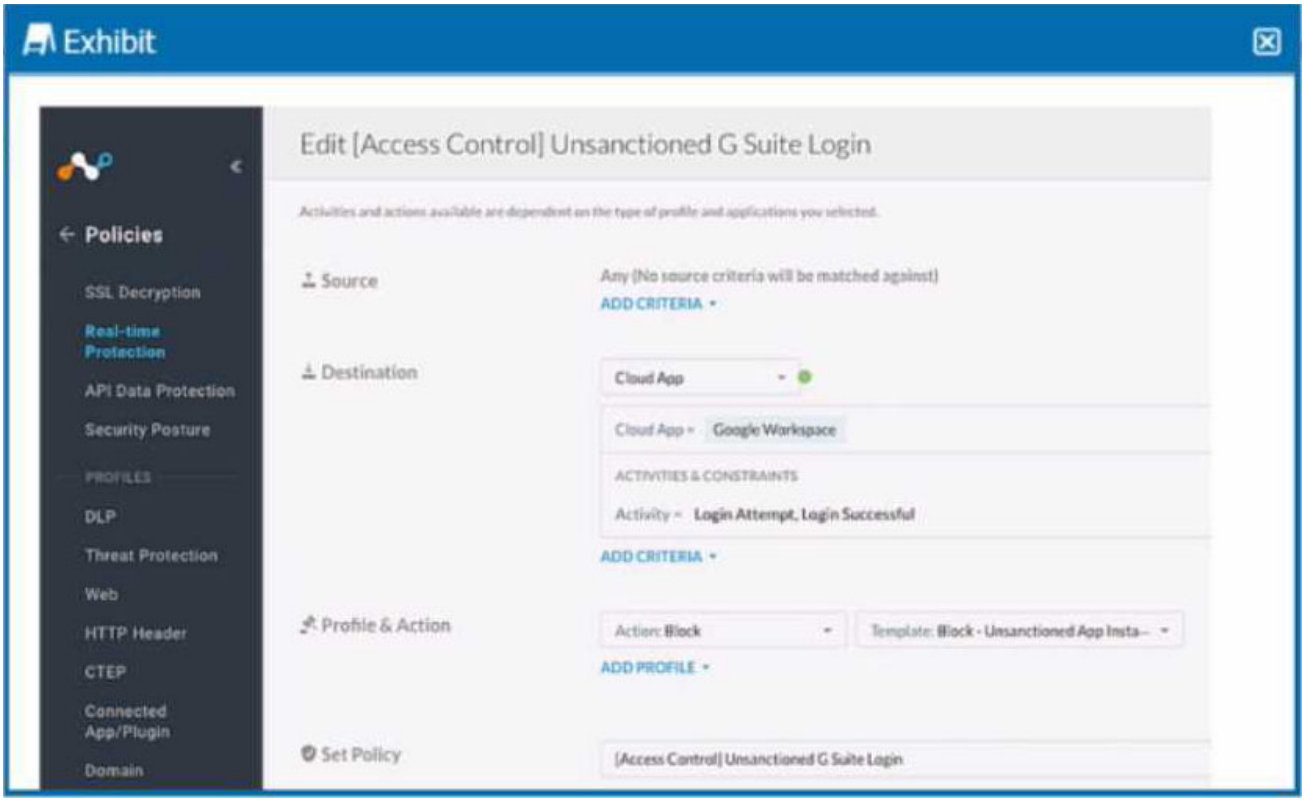
Exam : **NSK200**

Title : Netskope Certified Cloud Security Integrator (NCCSI)

Version : DEMO

1.To which three event types does Netskope's REST API v2 provide access? (Choose three.)
A. application
B. alert
C. client
D. infrastructure
E. user
Answer: ABD
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

2.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?
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]

3.You have deployed a development Web server on a public hosting service using self-signed SSL certificates. After some troubleshooting, you determined that when the Netskope client is enabled, you are unable to access the Web server over SSL. The default Netskope tenant steering configuration is in place.
In this scenario, which two settings are causing this behavior? (Choose two.)
A. SSL pinned certificates are blocked.
B. Untrusted root certificates are blocked.
C. Incomplete certificate trust chains are blocked.
D. Self-signed server certificates are blocked.
Answer: BD
Explanation:
The default Netskope tenant steering configuration blocks untrusted root certificates and self-signed server certificates. These settings are intended to prevent man-in-the-middle attacks and ensure the validity of the SSL connection. However, they also prevent the access to the development Web server that uses self-signed SSL certificates. To allow access to the Web server, the settings need to be changed or an exception needs to be added for the Web server domain.

4.Your customer currently only allows users to access the corporate instance of OneDrive using SSO with the Netskope client. The users are not permitted to take their laptops when vacationing, but sometimes they must have access to documents on OneDrive when there is an urgent request. The customer wants to allow employees to remotely access OneDrive from unmanaged devices while enforcing DLP controls to prohibit downloading sensitive files to unmanaged devices.
Which steering method would satisfy the requirements for this scenario?
A. Use a reverse proxy integrated with their SSO.
B. Use proxy chaining with their cloud service providers integrated with their SSO.
C. Use a forward proxy integrated with their SSO.
D. Use a secure forwarder integrated with an on-premises proxy.
Answer: A
Explanation:
A reverse proxy integrated with their SSO would satisfy the requirements for this scenario. A reverse proxy intercepts requests from users to cloud apps and applies policies based on user identity, device posture, app, and data context. It can enforce DLP controls to prohibit downloading sensitive files to unmanaged devices. It can also integrate with the customer’s SSO provider to authenticate users and allow access only to the corporate instance of OneDrive. The other steering methods are not suitable for this scenario because they either require the Netskope client or do not provide granular control over

cloud app activities.

5.An engineering firm is using Netskope DLP to identify and block sensitive documents, including schematics and drawings. Lately, they have identified that when these documents are blocked, certain employees may be taking screenshots and uploading them. They want to block any screenshots from being uploaded.
Which feature would you use to satisfy this requirement?
A. exact data match (EDM)
B. document fingerprinting
C. ML image classifier
D. optical character recognition (OCR)
Answer: C
Explanation:
To block any screenshots from being uploaded, the engineering firm should use the ML image classifier feature of Netskope DLP. This feature uses machine learning to detect sensitive information within images, such as screenshots, whiteboards, passports, driver’s licenses, etc. The firm can create a DLP policy that blocks any image upload that matches the screenshot classifier. This will prevent employees from circumventing the DLP controls by taking screenshots of sensitive documents.
Reference: Improved DLP Image Classifiers, Netskope Data Loss Prevention, The Importance of a Machine Learning-Based Source Code Classifier