Free Questions for NSK200

Shared by Hull on 24-10-2023

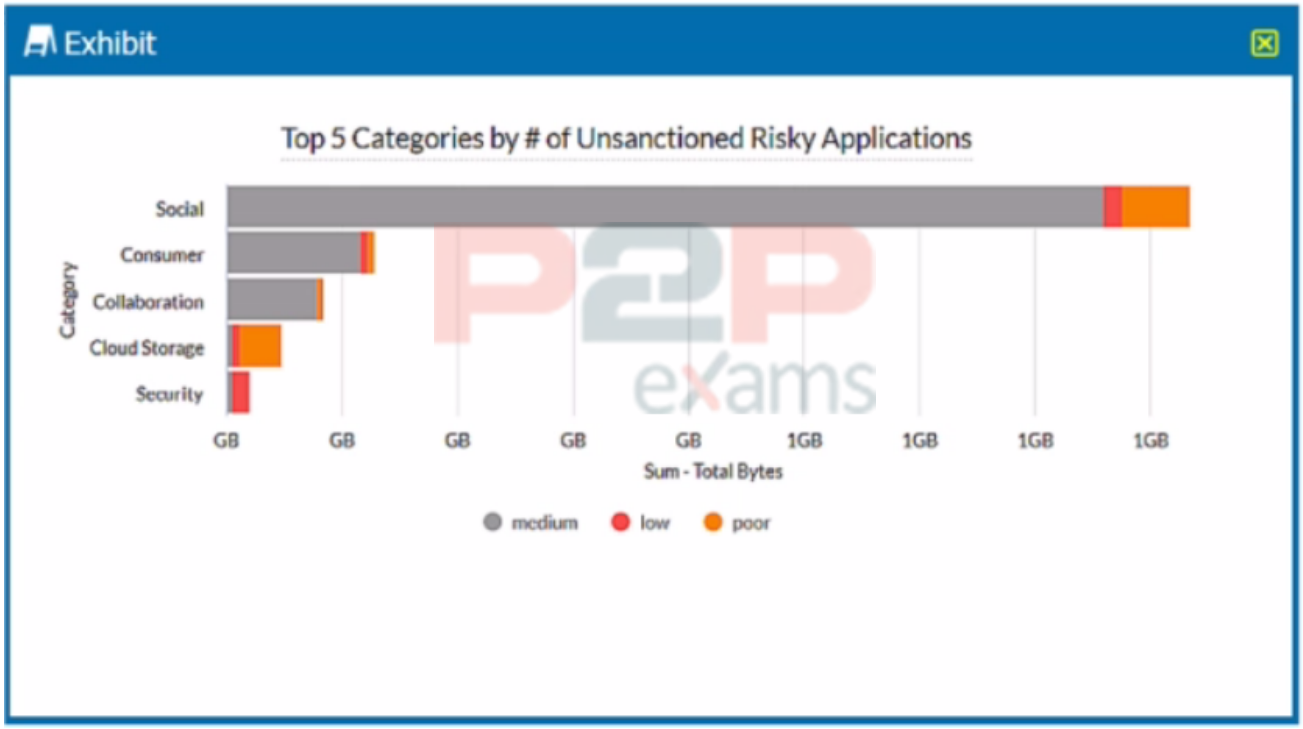
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Review the exhibit.



A security analyst needs to create a report to view the top five categories of unsanctioned applications accessed in the last 90 days. Referring to the exhibit, what are two data collections in Advanced Analytics that would be used to create this report? (Choose two.)

Options:

A- Alerts
B- Application Events
C- Page Events
D- Network Events

Answer:

B, D

Explanation:

To create a report to view the top five categories of unsanctioned applications accessed in the last 90 days, the security analyst would need to use two data collections in Advanced Analytics: Application Events and Network Events. Application Events provide information about the cloud

applications and websites accessed by users, such as app name, app category, app risk score, app instance, app version, and more. Network Events provide information about the network traffic generated by users, such as source IP, destination IP, protocol, port, bytes sent, bytes received, and more. By combining these two data collections, the security analyst can filter the events by app category, app risk score, and time range to create a report that shows the top five categories of unsanctioned applications accessed in the last 90 days. Alerts and Page Events are not relevant for this report. Alerts provide information about the alerts triggered by Real-time Protection or API Data Protection policies, such as alert type, alert severity, alert status, alert description, and more.Page Events provide information about the web pages visited by users, such as page title, page URL, page category, page risk score, page content type, and more.Reference:Advanced Analytics

Question 2

Question Type: MultipleChoice

Your customer implements Netskope Secure Web Gateway to secure all Web traffic. While they have created policies to block certain categories, there are many new sites available dally that are not yet categorized. The customer's users need quick access and cannot wait to put in a request to gain access requiring a policy change or have the site's category changed.

To solve this problem, which Netskope feature would provide quick, safe access to these types of sites?

Options:

A- Netskope Cloud Firewall (CFW)
B- Netskope Remote Browser Isolation (RBI)
C- Netskope Continuous Security Assessment (CSA)
D- Netskope SaaS Security Posture Management (SSPM)

Answer:

B

Explanation:

To solve the problem of providing quick, safe access to uncategorized and risky websites, the Netskope feature that the customer should use is Netskope Remote Browser Isolation (RBI). Netskope RBI is a part of the Netskope Secure Web Gateway offering that intercepts a user's browsing session to a website, acting as a proxy that fetches the content for that user and

renders the content in an isolated browsing instance. The rendered content is delivered to the user's browser as a safe stream of pixels.This safely silos the end user's device and the enterprise network and systems, separating it from their browsing activity and restricting the ability of an attacker to establish control and / or breach other systems and exfiltrate data1.Netskope RBI can be easily invoked with an 'isolate' policy action within the Netskope Security Cloud for any website category or domain2. Therefore, option B is correct and the other options are incorrect.Reference:Remote Browser Isolation - Netskope Knowledge Portal,Netskope Remote Browser Isolation - Netskope

Question 3

Question Type: MultipleChoice

Review the exhibit.

While diagnosing an NPA connectivity issue, you notice an error message in the Netskope client logs.

Referring to the exhibit, what does this error represent?

Options:

A- The Netskope client has been load-balanced to a different data center.

B- The primary publisher is unavailable or cannot be reached.

C- There Is an EDNS or LDNS resolution error.
D- There Is an upstream device trying to intercept the NPA TLS connection.

Answer:

D

Explanation:

The error message in the exhibit represents that there is an upstream device trying to intercept the NPA TLS connection. The error message is ''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 establish a secure connection to the NPA service and access the private applications4.To solve this problem, you need to either bypass or trust the upstream device that is performing SSL decryption, such as a firewall or proxy5. Therefore, option D is correct and the other options are incorrect.Reference:Troubleshooting Netskope Client - Netskope Knowledge Portal,Netskope Client Troubleshooting Guide - The Netskope Community

Question 4

Question Type: MultipleChoice

You are having issues with fetching user and group Information periodically from the domain controller and posting that information to your tenant instance in the Netskope cloud. To begin the troubleshooting process, what would you Investigate first in this situation?

Options:

A- On-Premises Log Parser
B- Directory Importer
C- DNS Connector
D- AD Connector

Answer:

B

Explanation:

The Directory Importer is a component of the Netskope Adapters that connects to the domain controller and periodically fetches user and group information to post that info to your tenant instance in the Netskope cloud1. If you are having issues with this process, the first thing you should investigate is the Directory Importer itself.You can check the status of the Directory Importer service, the configuration file, the logs, and the connectivity to the domain controller and the Netskope cloud2. Therefore, option B is correct and the other options are incorrect.Reference:Configure Directory Importer - Netskope Knowledge Portal,Troubleshooting Directory Importer - Netskope Knowledge Portal

Question 5

Question Type: MultipleChoice

You are an administrator writing Netskope Real-time Protection policies and must determine proper policy ordering.

Which two statements are true in this scenario? (Choose two.)

Options:

A- You must place Netskope private access malware policies in the middle.
B- You do not need to create an 'allow all' Web Access policy at the bottom.
C- You must place DLP policies at the bottom.
D- You must place high-risk block policies at the top.

Answer:

B, D

Explanation:

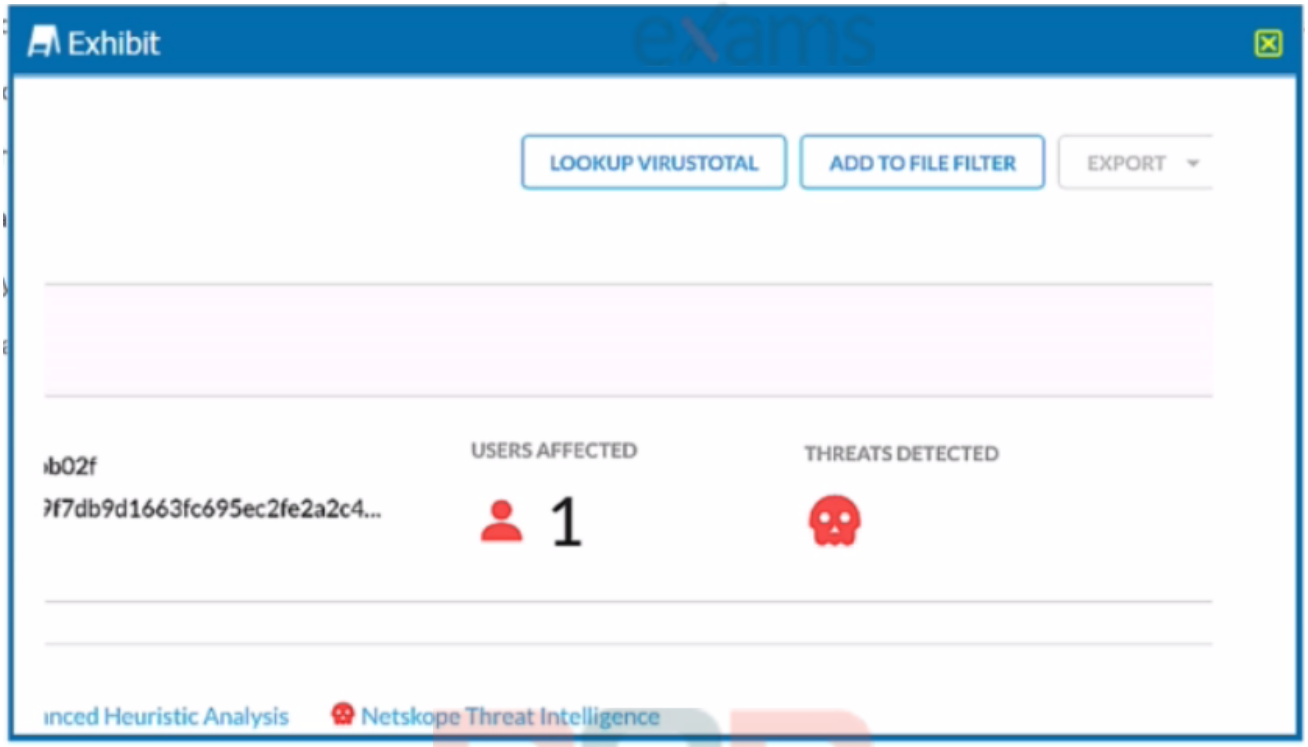
To determine proper policy ordering for Netskope Real-time Protection policies, you need to follow these two statements: B. You do not need to create an ''allow all'' Web Access policy at the bottom. D. You must place high-risk block policies at the top.These statements are based on the best practices for policy ordering recommended by Netskope3. An ''allow all'' Web Access policy at the bottom is not necessary because any traffic that does not match any policy will be allowed by default.However, you can create a ''monitor all'' Web Access policy at the bottom if you want to log all the traffic that is not matched by any other policy4. High-risk block policies at the top are important because they prevent any traffic that poses a serious threat or violates a critical

compliance standard from reaching its destination.These policies should have higher priority than other policies that may allow or modify the traffic5. Therefore, options B and D are correct and the other options are incorrect.Reference:Real-time Protection Policies - Netskope Knowledge Portal,Create a Real-time Protection Policy for Web Categories - Netskope Knowledge Portal,Best Practices: Real-time Protection Policies (1 of 2) - Netskope

Question 6

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 7

Question Type: MultipleChoice

Netskope is being used as a secure Web gateway. Your organization's URL list changes frequently. In this scenario, what makes It possible for a mass update of the URL list in the Netskope platform?

Options:

A- REST API v2
B- Assertion Consumer Service URL
C- Cloud Threat Exchange
D- SCIM provisioning

Answer:

A

Explanation:

The method that makes it possible for a mass update of the URL list in the Netskope platform is A. REST API v2.REST API v2 is a feature that allows you to use an auth token to make authorized calls to the Netskope API and access resources via URI paths5.You can use REST API v2 to update a URL list with new values by providing the name of an existing URL list and a comma-separated list of URLs or IP addresses6. This can help you automate or script the management of your URL lists and keep them up-to-date. Therefore, option A is correct and the other options are incorrect.Reference:REST API v2 Overview - Netskope Knowledge Portal,Update a URL List - Netskope Knowledge Portal

Question 8

Question Type: MultipleChoice

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.)

Options:

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:

B, D

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.