BrainDumps Collection

Free Questions for NSK300 by braindumpscollection

Shared by Cameron on 24-05-2024

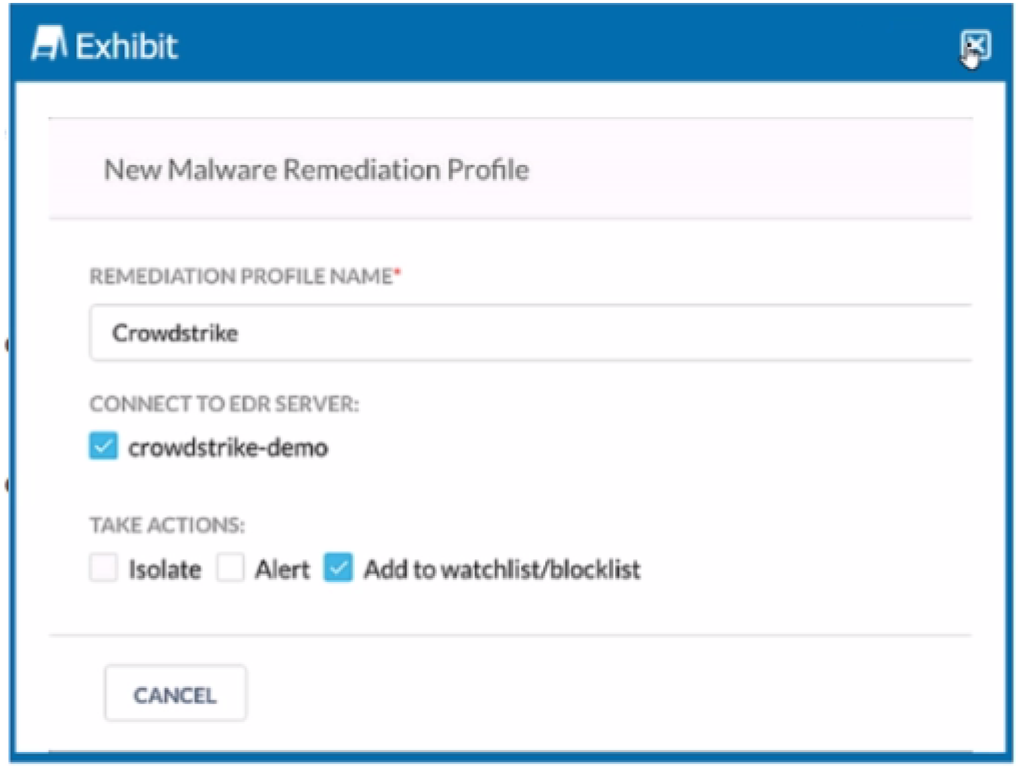
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Review the exhibit.



New Malware Remediation Profile

REMEDIATION PROFILE NAME*

Crowdstrike

CONNECT TO EDR SERVER:

☑ crowdstrike-demo

TAKE ACTIONS:

□ Isolate □ Alert ☑ Add to watchlist/blocklist

You are asked to integrate Netskope with Crowdstrike EDR. You added the Remediation profile shown in the exhibit.

Which action will this remediation profile take?

Options:

A- The endpoint will be isolated.

B- The malware hash will be added as an IOC in Crowdstrike.

C- The malware will be quarantined.

D- The malware hash will be added as an IOC in Netskope.

Answer:

A

Explanation:

The remediation profile shown in the exhibit will take the action of isolating the endpoint. This is indicated by the "Isolate" option being checked under "TAKE ACTIONS" in the configuration settings. When this option is selected, the remediation profile is configured to isolate the endpoint upon detection of a threat, which is a common response to contain a potential security breach and prevent further spread of malware within the network1.

Question 2

Question Type: MultipleChoice

Your client is an NG-SWG customer. They are going to use the Explicit Proxy over Tunnel (EPoT) steering method. They have a specific list of domains that they do not want to steer to the Netskope Cloud.

What would accomplish this task''

Options:

A- Define exception domains in the PAC file.

B- Define exceptions in the Netskope steering configuration

C- Create a real-time policy with a bypass action.

D- Use an SSL decryption policy.

Answer:

A

Explanation:

To accomplish the task of not steering specific domains to the Netskope Cloud while using the Explicit Proxy over Tunnel (EPoT) steering method, you would define exception domains in the PAC file (A). This is because the PAC file is used to specify which domains should bypass the proxy and connect directly, thus allowing for granular control over the traffic that is steered to Netskope1.

Question 3

Question Type: **MultipleChoice**

You are asked to ensure that a Web application your company uses is both reachable and decrypted by Netskope. This application is served using HTTPS on port 6443. Netskope is configured with a default Cloud Firewall configuration and the steering configuration is set for All Traffic.

Which statement is correct in this scenario?

Options:

A- Create a Firewall App in Netskope along with the corresponding Real-time Protection policy to allow the traffic.

B- Nothing is required since Netskope is steering all traffic.

C- Enable 'Steer non-standard ports' in the steering configuration and add the domain and port as a new non-standard port

D- Enable 'Steer non-standard ports' in the steering configuration and create a corresponding Real-time Protection policy to allow the traffic

Answer:

C

Explanation:

To ensure that the web application using HTTPS on port 6443 is both reachable and decrypted by Netskope, the correct action is to enable "Steer non-standard ports" in the steering configuration and add the domain and port as a new non-standard port. This is because Netskope's default configuration steers standard HTTP/HTTPS traffic, typically on ports 80 and 443. Since port 6443 is a non-standard port for HTTPS traffic, it requires explicit configuration to be steered through Netskope1.

Question 4

Question Type: MultipleChoice

You have enabled CASB traffic steering using the Netskope Client, but have not yet enabled a Real-time Protection policy. What is the default behavior of the traffic in this scenario?

Options:

A- Traffic will be blocked and logged.

B- Traffic will be allowed and logged.

C- Traffic will be blocked, but not logged.

D- Traffic will be allowed, but not logged.

Answer:

B

Explanation:

In the scenario where CASB traffic steering is enabled using the Netskope Client without a Real-time Protection policy being activated, the default behavior of the traffic is to allow and log it (B). This means that the traffic will not be blocked; instead, it will be permitted to pass through and will be recorded for monitoring and analysis purposes. This default setting ensures visibility into the traffic and user activities without immediately enforcing a block, allowing for a period of observation and policy tuning before potentially more restrictive actions are taken1.

Question 5

Question Type: **MultipleChoice**

A hospital has a patient form that they share with their patients over Gmail. The blank form can be freely shared among anyone. However, if the form has any information filled out. the document is considered confidential.

Which rule type should be used in the DLP profile to match such a document?

Options:

A- Use fingerprint classification.

B- Use a dictionary rule for all your patient names.

C- Use Exact Match with patient names

D- Use predefined DLP Rule(s) that match the patient name.

Answer:

A

Explanation:

The appropriate rule type to use in the DLP profile for a document that is considered confidential when filled out is fingerprint classification. Fingerprinting is a method used to identify and protect sensitive data within documents. It works by creating a digital fingerprint of a file, which can then be used to detect any copies or derivatives of that file. In this case, fingerprinting would allow the hospital to differentiate between the blank patient form, which can be freely shared, and the same form with patient information filled out, which is confidential1.

Question 6

Question Type: **MultipleChoice**

Your company has a large number of medical forms that are allowed to exit the company when they are blank. If the forms contain sensitive data, the forms must not leave any company data centers, managed devices, or approved cloud environments. You want to create DLP rules for these forms.

Which first step should you take to protect these forms?

Options:

A- Use Netskope Secure Forwarder to create EDM hashes of all forms.

B- Use Netskope Secure Forwarder to create an MIP tag for all forms.

C- Use Netskope Secure Forwarder to create fingerprints of all forms.

D- Use Netskope Secure Forwarder to create an ML Model of all forms

Answer:

C

Explanation:

The first step to protect the medical forms containing sensitive data is to create fingerprints of all forms using Netskope Secure Forwarder. Fingerprints are unique identifiers that can be used to detect when a form contains sensitive data. By creating fingerprints, you can set up DLP (Data Loss Prevention) rules that will allow blank forms to exit the company but will prevent forms with sensitive data from leaving the protected environments. This method ensures that only forms without sensitive information are allowed to be shared externally.

Question 7

Question Type: **MultipleChoice**

You successfully configured Advanced Analytics to identify policy violation trends Upon further investigation, you notice that the activity is NULL. Why is this happening in this scenario?

Options:

A- The SSPM policy was not configured during setup.

B- The REST API v1 token has expired.

C- A policy violation was identified using API Protection.

D- A user accessed a static Web page.

Answer:

D

Explanation:

The reason for the activity being NULL in this scenario is likely because a user accessed a static Web page. In Netskope's Advanced Analytics, when the activity is reported as NULL, it often indicates that there was no dynamic interaction or transaction to record, which is typical when a static web page is accessed1. Static web pages do not generate the kind of events or activities that are tracked by policies, hence they appear as NULL in the activity field.

Question 8

Question Type: MultipleChoice

A company's architecture includes a server subnet that is logically isolated from the rest of the network with no Internet access, no default gateway, and no access to DNS. New resources can only be provisioned on virtual resources in that segment and there is a firewall that is tunnel-capable securing the perimeter of the segment. The only requirement is to have content filtering for any server that might access the Internet using a browser.

Which two Netskope deployment methods would achieve this requirement? (Choose two.)

Options:

A- Deploy a mobile profile on the servers.

B- Deploy Data Plane on Premises (DPoP) with a proxy configuration on the servers.

C- Deploy IPsec or GRE tunnels in the segment to steer traffic from the servers to Netskope.

D- Install the Netskope Client on the servers

Answer:

B, C

Explanation:

For a server subnet that is isolated and requires content filtering for any server that might access the Internet using a browser, the two Netskope deployment methods that would meet this requirement are:

B . Deploy Data Plane on Premises (DPoP) with a proxy configuration on the servers: Deploying DPoP would allow the isolated servers to connect to the Netskope cloud for content filtering through a proxy configuration. This setup would enable the servers to have controlled access to the Internet for content filtering purposes without requiring direct Internet access1.

C . Deploy IPsec or GRE tunnels in the segment to steer traffic from the servers to Netskope: By deploying IPsec or GRE tunnels, the traffic from the servers can be securely directed to Netskope for content filtering. This method is suitable for environments where servers do not have direct Internet access, as the tunnel provides a secure path for traffic to reach Netskope's cloud services1.

These deployment methods are designed to work in environments with strict network isolation and provide the necessary content filtering capabilities for servers accessing the Internet.

Question 9

Question Type: **MultipleChoice**

You are implementing Netskope Cloud Exchange in your company lo include functionality provided by third-party partners. What would be a reason for using Netskope Cloud Risk Exchange in this scenario?

Options:

A- to ingest events and alerts from a Netskope tenant

B- to feed SOC with detection and response services

C- to map multiple scores to a normalized range

D- to automate service tickets from alerts of interest

Answer:

D

Explanation:

The reason for using Netskope Cloud Risk Exchange in this scenario is to automate service tickets from alerts of interest. Netskope Cloud Risk Exchange (CRE) is designed to ingest user, device, and application risk scores, creating a dashboard view of contributors to your company's overall risk score and trend. One of the key functionalities of CRE is to trigger risk-reducing actions through business rules that are tuned to a weighted score. Automating service tickets from alerts of interest is a part of this functionality, as it allows for the automatic creation of tickets in response to specific alerts, streamlining the process of addressing potential security issues12.

Question 10

Question Type: **MultipleChoice**

You deployed IPsec tunnels to steer on-premises traffic to Netskope. You are now experiencing problems with an application that had previously been working. In an attempt to solve the issue, you create a Steering Exception in the Netskope tenant tor that application:

however, the problems are still occurring

Which statement is correct in this scenario?

Options:

A- You must create a private application to steer Web application traffic to Netskope over an IPsec tunnel.

B- Exceptions only work with IP address destinations

C- Steering bypasses for IPsec tunnels must be applied at your edge network device.

D- You must deploy a PAC file to ensure the traffic is bypassed pre-tunnel

Answer:

C

Explanation:

In the scenario where you have deployed IPsec tunnels to steer on-premises traffic to Netskope and are experiencing issues with an application, the correct statement is C: Steering bypasses for IPsec tunnels must be applied at your edge network device. This means that to effectively bypass the steering for a specific application, the configuration must be done on the network device that is establishing the IPsec tunnel, such as a firewall or router. This device controls the traffic before it enters the tunnel, so applying the bypass there ensures that the application's traffic does not get directed through the tunnel and can reach its destination directly.

Question 11

Question Type: **MultipleChoice**

You are implementing a solution to deploy Netskope for machine traffic in an AWS account across multiple VPCs. You want to deploy the least amount of tunnels while providing connectivity for all VPCs.

How would you accomplish this task?

Options:

A- Use IPsec tunnels from the AWS Virtual Private Gateway.

B- Use GRE tunnels from the AWS Transit Gateway.

C- Use GRE tunnels from the AWS Virtual Private Gateway

D- Use IPsec tunnels from the AWS Transit Gateway.

Answer:

D

Explanation:

The best approach to deploy Netskope for machine traffic across multiple VPCs in an AWS account with the least amount of tunnels while providing connectivity for all VPCs is to use IPsec tunnels from the AWS Transit Gateway. This method allows you to use the same Site-to-Site VPN connection to Netskope for multiple VPCs, thus minimizing the number of tunnels required12. The AWS Transit Gateway acts as a network transit hub, enabling you to connect your VPCs and on-premises networks through a central point of management and control. Using IPsec tunnels with the AWS Transit Gateway ensures that all VPCs connected to it utilize the same IPsec tunnel between the transit gateway and Netskope POP1.

Question 12

Question Type: MultipleChoice

You are currently designing a policy for AWS S3 bucket scans with a custom DLP profile Which policy action(s) are available for this policy?

Options:

A- Alert, Quarantine. Block, User Notification

B- Alert, User Notification

C- Alert only

D- Alert, Quarantine

Answer:

D

Explanation:

When designing a policy for AWS S3 bucket scans with a custom DLP profile in Netskope, the available policy actions are Alert and Quarantine. These actions allow you to be notified when a policy violation occurs and to quarantine sensitive data to prevent potential data loss or exposure. The Alert action will notify the designated personnel or system when a match to the DLP profile is found during the scan. The Quarantine action will move the offending file to a secure location where it can be reviewed and dealt with appropriately1.

To Get Premium Files for NSK300 Visit

https://www.p2pexams.com/products/nsk300

For More Free Questions Visit

https://www.p2pexams.com/netskope/pdf/nsk300

20%
DISCOUNT