Free Questions for PCNSE by dumpssheet

Shared by Aguirre on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Where is Palo Alto Networks Device Telemetry data stored on a firewall with a device certificate installed?

Options:

A- On Palo Alto Networks Update Servers

B- M600 Log Collectors

C- Cortex Data Lake

D- Panorama

Answer:

A

Explanation:

Palo Alto Networks Device Telemetry data, collected from firewalls with a device certificate installed, is stored on Palo Alto Networks Update Servers. This telemetry data includes information about threats, device health, and other operational metrics that are crucial for the continuous improvement of security services and threat intelligence. The collected data is anonymized and securely transmitted to

Palo Alto Networks, where it is used to enhance the overall effectiveness of threat identification and prevention capabilities across all deployed devices. This collaborative approach helps in keeping the security ecosystem updated and resilient against emerging threats.

Question 2

Question Type: MultipleChoice

When you troubleshoot an SSL Decryption issue, which PAN-OS CL1 command do you use to check the details of the Forward Trust certificate. Forward Untrust certificate, and SSL Inbound Inspection certificate?

Options:

A- show system setting ssl-decrypt certificate

B- show system setting ssl-decrypt certs

C- debug dataplane show ssl-decrypt ssl-certs

D- show system setting ssl-decrypt certificate-cache

Answer:

C

Explanation:

To troubleshoot SSL Decryption issues and check the details of the Forward Trust certificate, Forward Untrust certificate, and SSL Inbound Inspection certificate, the PAN-OS CLI command debug dataplane show ssl-decrypt ssl-certs is used. This command provides detailed information about the SSL certificates involved in decryption and inspection processes, allowing administrators to verify certificate validity, issuer details, and other critical parameters. Understanding the certificate details is crucial in diagnosing issues related to SSL decryption, such as certificate validation errors or misconfigurations that could lead to decryption failures.

Question 3

Question Type: MultipleChoice

PBF can address which two scenarios? (Choose two.)

Options:

A- Routing FTP to a backup ISP link to save bandwidth on the primary ISP link

B- Providing application connectivity the primary circuit fails

C- Enabling the firewall to bypass Layer 7 inspection

D- Forwarding all traffic by using source port 78249 to a specific egress interface

Answer:

A, B

Explanation:

Policy-Based Forwarding (PBF) on Palo Alto Networks firewalls allows administrators to define forwarding decisions based on criteria other than the destination IP address, such as the application, source address, or user. It can address scenarios like:

A) Routing FTP to a backup ISP link to save bandwidth on the primary ISP link: PBF can be configured to identify FTP traffic and route it through a different ISP, preserving bandwidth on the primary link for other critical applications.

B) Providing application connectivity when the primary circuit fails: PBF can be used for failover purposes, directing traffic to an alternate path if the primary connection goes down, ensuring continuous application availability.

PBF is not designed to bypass Layer 7 inspection or forward traffic based solely on source port, as these tasks are managed through different mechanisms within the firewall's operating system.

Question 4

Question Type: MultipleChoice

A company is deploying User-ID in their network. The firewall team needs to have the ability to see and choose from a list of usernames and user groups directly inside the Panorama policies when creating new security rules.

How can this be achieved?

Options:

A- By configuring Data Redistribution Client in Panorama > Data Redistribution

B- By configuring User-ID group mapping in Panorama > User Identification

C- By configuring User-ID source device in Panorama > Managed Devices

D- By configuring Master Device in Panorama > Device Groups

Answer:

B

Explanation:

To enable the firewall team to view and select from a list of usernames and user groups directly within Panorama policies for new security rule creation, User-ID group mapping should be configured in Panorama under User Identification. This feature allows Panorama to collect user and group information from various sources (like Active Directory) and use this information to create policies.

By setting up User-ID group mapping, administrators can leverage user identity as criteria in security rules, enabling more granular access control and policy enforcement based on user or group membership, thereby enhancing the overall security posture.

Question 5

Question Type: MultipleChoice

Four configuration choices are listed, and each could be used to block access to a specific URL.

If you configured each choice to block the same URL, then which choice would be evaluated last in the processing order to block access to the URL?

Options:

A- Custom URL category in URL Filtering profile

B- EDL in URL Filtering profile

C- PAN-DB URL category in URL Filtering profile

D- Custom URL category in Security policy rule

Answer:

D

Explanation:

In Palo Alto Networks firewalls, the order of evaluation for blocking access to specific URLs involves several components, including URL Filtering profiles and Security policy rules. Among the options listed, the Custom URL category in a Security policy rule is evaluated last in the processing order. This is because the firewall processes Security policy rules after URL Filtering profiles. If a URL matches a Custom URL category in a Security policy rule, this rule will override any allow actions in URL Filtering profiles due to the hierarchical nature of policy evaluation. Security policies provide the final verdict on whether traffic is allowed or denied, making them the last line of evaluation for access control, including URL blocking.

Question 6

Question Type: MultipleChoice

A firewall administrator needs to check which egress interface the firewall will use to route the IP 10.2.5.3.

Which command should they use?

Options:

A- test routing route ip 10.2.5.3 *

B- test routing route ip 10.2.5.3 virtual-router default

C- test routing fib-lookup ip 10.2.5.0/24 virtual-router default

D- test routing fib-lookup ip 10.2.5.3 virtual-router default

Answer:

D

Explanation:

To determine the egress interface a Palo Alto Networks firewall will use to route a specific IP address, the appropriate command is test routing fib-lookup ip 10.2.5.3 virtual-router default. This command performs a Forwarding Information Base (FIB) lookup for the specified IP address within the context of the specified virtual router, which in this case is the default virtual router. The FIB lookup process checks the routing table and the associated forwarding information to determine the next-hop and the egress interface for the given IP address. This command is instrumental for troubleshooting and verifying routing decisions made by the firewall to ensure that traffic is routed as expected through the network infrastructure.

Question 7

Question Type: MultipleChoice

When using certificate authentication for firewall administration, which method is used for authorization?

Options:

A- Local

B- Radius

C- Kerberos

D- LDAP

Answer:

A

Explanation:

When using certificate authentication for firewall administration on Palo Alto Networks devices, the method used for authorization is typically the Local database. Certificate authentication ensures that the entity attempting to access the firewall is in possession of a valid certificate. Once the certificate is validated for authentication, the authorization process determines what level of access or permissions the authenticated entity has. This is usually managed locally on the firewall, where administrators can define roles and permissions associated with different users or certificates. Thus, the authorization process, in this case, leverages the Local database to enforce access controls and permissions, aligning with best practices for secure management of network devices.

Question 8

Question Type: MultipleChoice

How should an administrator enable the Advance Routing Engine on a Palo Alto Networks firewall?

Options:

A- Enable Advanced Routing Engine in Device > Setup > Session > Session Settings, then commit and reboot.

B- Enable Advanced Routing in Network > Virtual Routers > Router Settings > General, then commit and reboot.

C- Enable Advanced Routing in General Settings of Device > Setup > Management, then commit and reboot.

D- Enable Advanced Routing in Network > Virtual Routers > Redistribution Profiles and then commit.

Answer:

B

Explanation:

The Advanced Routing Engine in Palo Alto Networks firewalls enhances the capabilities of routing functionalities, allowing for more complex and robust routing configurations. To enable the Advanced Routing Engine on a Palo Alto Networks firewall, an administrator needs to navigate to the Network tab, select Virtual Routers, and then access the settings for the specific virtual router they wish to configure. Within the Router Settings under the General tab, there's an option to enable Advanced Routing features. After enabling this option, the administrator must commit the changes and perform a system reboot for the changes to take effect. This process allows the firewall to utilize advanced routing protocols and features, enhancing its ability to manage and route traffic more efficiently across different network segments.