Free Questions for PCNSE by ebraindumps

Shared by Carson on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **DragDrop**

Match the terms to their corresponding definitions

Image not found or type unknown

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcnse-study-guide.pdf page 83

Answer:

Image not found or type unknown

Question 2

Question Type: **MultipleChoice**

Image not found or type unknown

Which log type will help the engineer verify whether packet buffer protection was activated?

Image not found or type unknown

Options:

Image not found or type unknown

A) Data Filtering

B) Configuration

C) Threat

D) Traffic

Answer:

C

Explanation:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNGFCA4

Question 3

Question Type: MultipleChoice

An organization conducts research on the benefits of leveraging the Web Proxy feature of PAN-OS 11.0.

What are two benefits of using an explicit proxy method versus a transparent proxy method? (Choose two.)

. No client configuration is required for explicit proxy, which simplifies the deployment complexity.

Options:

B) Explicit proxy supports interception of traffic using non-standard HTTPS ports.

C) It supports the X-Authenticated-User (XAU) header, which contains the authenticated username in the outgoing request.

D) Explicit proxy allows for easier troubleshooting, since the client browser is aware of the existence of the proxy.

Answer:

C, D

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/secure-mobile-users-with-prisma-access/explicit-proxy/explicit-proxy-how-it-works

https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/networking-features/web-proxy

Question 4

Question Type: MultipleChoice

Refer to the diagram. Users at an internal system want to ssh to the SSH server The server is configured to respond only to the ssh requests coming from IP 172.16.16.1.

In order to reach the SSH server only from the Trust zone, which Security rule and NAT rule must be configured on the firewall?

Image not found or type unknown

Options:

A) NAT Rule:

Source Zone: Trust -

Source IP: Any -

Destination Zone: Server -

Destination IP: 172.16.15.10 -

Source Translation: Static IP / 172.16.15.1

Security Rule:

Source Zone: Trust -

Source IP: Any -

Destination Zone: Trust -

Destination IP: 172.16.15.10 -

Application: ssh

B) NAT Rule:

Source Zone: Trust -

Source IP: 192.168.15.0/24 -

Destination Zone: Trust -

Destination IP: 192.168.15.1 -

Destination Translation: Static IP / 172.16.15.10

Security Rule:

Source Zone: Trust -

Source IP: 192.168.15.0/24 -

Destination Zone: Server -

Destination IP: 172.16.15.10 -

Application: ssh

C) NAT Rule:

Source Zone: Trust -

Source IP: Any -

Destination Zone: Trust -

Destination IP: 192.168.15.1 -

Destination Translation: Static IP /172.16.15.10

Security Rule:

Source Zone: Trust -

Source IP: Any -

Destination Zone: Server -

Destination IP: 172.16.15.10 -

Application: ssh

D) NAT Rule:
Source Zone: Trust -
Source IP: Any -
Destination Zone: Server -
Destination IP: 172.16.15.10 -
Source Translation: dynamic-ip-and-port / ethernet1/4
Security Rule:
Source Zone: Trust -
Source IP: Any -
Destination Zone: Server -
Destination IP: 172.16.15.10 -
Application: ssh

Answer:

D

Explanation:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClhwCAC

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/nat/source-nat-and-destination-nat/source-nat

Question 5

Question Type: **MultipleChoice**

Using multiple templates in a stack to manage many firewalls provides which two advantages? (Choose two.)

Options:

A) inherit address-objects from templates

B) define a common standard template configuration for firewalls

C) standardize server profiles and authentication configuration across all stacks

D) standardize log-forwarding profiles for security polices across all stacks

Answer:

B, C

Explanation:

Using multiple templates in a stack to manage many firewalls provides the advantages of defining a common standard template configuration for firewalls and standardizing server profiles and authentication configuration across all stacks. A template stack is a container for multiple templates that you can assign to firewalls and firewall groups. The templates in a stack are prioritized so that the settings in a higher-priority template override the same settings in a lower-priority template. This allows you to create a hierarchy of templates that define common settings for all firewalls and specific settings for different groups of firewalls. Reference: https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-templates-and-template-stacks

Question 6

Question Type: MultipleChoice

A network administrator wants to use a certificate for the SSL/TLS Service Profile.

Which type of certificate should the administrator use?

Options:

A) certificate authority (CA) certificate

B) client certificate

C) machine certificate

D) server certificate

Answer:

D

Explanation:

Use only signed certificates, not CA certificates, in SSL/TLS service profiles. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/configure-an-ssltls-service-profile.html

A server certificate is used for the SSL/TLS Service Profile. The server certificate identifies the firewall to clients that initiate SSL/TLS connections to it. Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/certificates-and-keys/server-certificates

Question 7

Question Type: MultipleChoice

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

Options:

A) Radius

B) LDAP

C) Kerberos

D) Local

Answer:

D

Explanation:

Authentication: Certificates Authorization: Local The administrative accounts are local to the firewall, but authentication to the web interface is based on client certificates. You use the firewall to manage role assignments but access domains are not supported.

Question 8

Question Type: MultipleChoice

A network security engineer must implement Quality of Service policies to ensure specific levels of delivery guarantees for various applications in the environment They want to ensure that they know as much as they can about QoS before deploying.

Which statement about the QoS feature is correct?

Options:

A) QoS is only supported on firewalls that have a single virtual system configured

B) QoS can be used in conjunction with SSL decryption

C) QoS is only supported on hardware firewalls

D) QoS can be used on firewalls with multiple virtual systems configured

Answer:

D

Explanation:

The correct answer is D - QoS can be used on firewalls with multiple virtual systems configured. QoS is a feature that enables network administrators to prioritize and manage network traffic to ensure that critical applications receive the necessary bandwidth and quality of service. This feature can be used on firewalls with multiple virtual systems, allowing administrators to configure policies on a per-Virtual System basis. Additionally, QoS can be used in conjunction with SSL decryption to ensure that applications running over SSL receive appropriate treatment.

Question 9

Question Type: **MultipleChoice**

A network security engineer is attempting to peer a virtual router on a PAN-OS firewall with an external router using the BGP protocol. The peer relationship is not establishing.

What command could the engineer run to see the current state of the BGP state between the two devices?

Options:

A) show routing protocol bgp state

B) show routing protocol bgp peer

C) show routing protocol bgp summary

D) show routing protocol bgp rib-out

Answer:

C

Explanation:

The show routing protocol bgp summary command displays the current state of the BGP peer relationship between the firewall and other BGP routers. The output includes the peer IP address, AS number, uptime, prefix count, state, and status codes. Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-cli-quick-start/use-the-cli/show-the-routing-table-and-statistics