Free Questions for PCNSE by go4braindumps

Shared by Knight on 24-05-2024

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

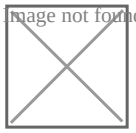
Refer to the exhibit.

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown



Review the images. A firewall policy that permits web traffic includes the global-logs policy is depicted

What is the result of traffic that matches the 'Alert - Threats' Profile Match List?

Options:

A) The source address of SMTP traffic that matches a threat is automatically blocked as BadGuys for 180 minutes.

B) The source address of traffic that matches a threat is automatically blocked as BadGuys for 180 minutes.

C) The source address of traffic that matches a threat is automatically tagged as BadGuys for 180 minutes.

D) The source address of SMTP traffic that matches a threat is automatically tagged as BadGuys for 180 minutes.

Answer:

C

Question 3

Question Type: **MultipleChoice**

When you navigate to Network: > GlobalProtect > Portals > Method section, which three options are available? (Choose three)

Options:

A) user-logon (always on)

B) pre-logon then on-demand

C) on-demand (manual user initiated connection)

D) post-logon (always on)

E) certificate-logon

Answer:

A, B, C

Explanation:

The Method section of the GlobalProtect portal configuration allows you to specify how users connect to the portal. The options are:

user-logon (always on): The agent connects to the portal as soon as the user logs in to the endpoint.

pre-logon then on-demand: The agent connects to the portal before the user logs in to the endpoint and then switches to on-demand mode after the user logs in.

on-demand (manual user initiated connection): The agent connects to the portal only when the user initiates the connection manually.
Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/globalprotect/configure-the-globalprotect-portal/configure-the-agent/configure-the-app-tab.html

Question 4

Question Type: MultipleChoice

An engineer must configure the Decryption Broker feature

Which Decryption Broker security chain supports bi-directional traffic flow?

Options:

A) Layer 2 security chain

B) Layer 3 security chain

C) Transparent Bridge security chain

D) Transparent Proxy security chain

Answer:

B

Explanation:

Together, the primary and secondary interfaces form a pair of decryption forwarding interfaces. Only interfaces that you have enabled to be Decrypt Forward interfaces are displayed here. Your security chain type (Layer 3 or Transparent Bridge) and the traffic flow direction (unidirectional or bidirectional) determine which of the two interfaces forwards allowed, clear text traffic to the security chain, and which interface receives the traffic back from the security chain after it has undergone additional enforcement.

Question 5

Question Type: MultipleChoice

What happens when an A/P firewall cluster synchronies IPsec tunnel security associations (SAs)?

Options:

A) Phase 2 SAs are synchronized over HA2 links

B) Phase 1 and Phase 2 SAs are synchronized over HA2 links

C) Phase 1 SAs are synchronized over HA1 links

D) Phase 1 and Phase 2 SAs are synchronized over HA3 links

Answer:

A

Explanation:

From the Palo Alto documentation below, 'when a VPN is terminated on a Palo Alto firewall HA pair, not all IPSEC related information is synchronized between the firewalls... This is an expected behavior. IKE phase 1 SA information is NOT synchronized between the HA firewalls.'

And from the second link, 'Data link (HA2) is used to sync sessions, forwarding tables, IPSec security associations, and ARP tables between firewalls in the HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive). It flows from the active firewall to the passive firewall.'

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&lang=en_US%E2%80%A9&refURL=http%3A

Question 6

Question Type: MultipleChoice

When configuring forward error correction (FEC) for PAN-OS SD-WAN, an administrator would turn on the feature inside which type of SD-WAN profile?

Options:

A) Certificate profile

B) Path Quality profile

C) SD-WAN Interface profile

D) Traffic Distribution profile

Answer:

C

Explanation:

To enable forward error correction (FEC) for PAN-OS SD-WAN, you need to create an SD-WAN Interface Profile that specifies Eligible for Error Correction Profile interface selection and apply the profile to one or more interfaces. Then you need to create an Error Correction Profile to implement FEC or packet duplication. Reference: https://docs.paloaltonetworks.com/sd-wan/2-0/sd-wan-admin/configure-sd-wan/create-an-error-correction-profile

Question 7

Question Type: MultipleChoice

A standalone firewall with local objects and policies needs to be migrated into Panorama. What procedure should you use so Panorama is fully managing the firewall?

Options:

A) Use the 'import Panorama configuration snapshot' operation, then perform a device-group commit push with 'include device and network templates'

B) Use the 'import device configuration to Panorama' operation, then 'export or push device config bundle' to push the configuration

C) Use the 'import Panorama configuration snapshot' operation, then 'export or push device config bundle' to push the configuration

D) Use the 'import device configuration to Panorama' operation, then perform a device-group commit push with 'include device and network templates'

Answer:

B

Explanation:

https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/transition-a-firewall-to-panorama-management/migrate-a-firewall-to-panorama-management.html

Question 8

Question Type: MultipleChoice

A prospect is eager to conduct a Security Lifecycle Review (SLR) with the aid of the Palo Alto Networks NGFW.

Which interface type is best suited to provide the raw data for an SLR from the network in a way that is minimally invasive?

Options:

A) Layer 3

B) Virtual Wire

C) Tap

D) Layer 2

Answer:

C

Explanation:

A tap interface is best suited to provide the raw data for an SLR from the network in a way that is minimally invasive. A tap interface allows the firewall to passively monitor network traffic without affecting the flow of traffic. The firewall can analyze the traffic and generate reports based on the application, user, content, and threat information. Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/networking/configure-interfaces/configure-a-tap-interface

Question 9

Question Type: MultipleChoice

Before you upgrade a Palo Alto Networks NGFW, what must you do?

Options:

A) Make sure that the PAN-OS support contract is valid for at least another year

B) Export a device state of the firewall

C) Make sure that the firewall is running a version of antivirus software and a version of WildFire that support the licensed subscriptions.

D) Make sure that the firewall is running a supported version of the app + threat update

Answer:

D

Explanation:

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/pan-os-upgrade-checklist#id53a2bc2b-f86e-4ee5-93d7-b06aff837a00 'Verify the minimum content release version.'

Before you upgrade, make sure the firewall is running a version of app + threat (content version) that meets the minimum requirement of the new PAN-OS https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRrCAK

Question 10

Question Type: MultipleChoice

A remote administrator needs firewall access on an untrusted interface. Which two components are required on the firewall to configure certificate-based administrator authentication to the web UI? (Choose two)

Options:

A) client certificate

B) certificate profile

C) certificate authority (CA) certificate

D) server certificate

Answer:

B, C

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-certificate-based-administrator-authentication-to-the-web-interface.html