Free Questions for PCNSE

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

An engineer is configuring a Protection profile to defend specific endpoints and resources against malicious activity.

The profile is configured to provide granular defense against targeted flood attacks for specific critical systems that are accessed by users from the internet.

Which profile is the engineer configuring?

Options:

A- Packet Buffer Protection
B- Zone Protection
C- Vulnerability Protection
D- DoS Protection

Answer:

D

Explanation:

The engineer is configuring a DoS Protection profile to defend specific endpoints and resources against malicious activity. A DoS Protection profile is a feature that enables the firewall to detect and prevent denial-of-service (DoS) attacks that attempt to overwhelm network resources or disrupt services. A DoS Protection profile can provide granular defense against targeted flood attacks for specific critical systems that are accessed by users from the internet, such as web servers, DNS servers, or VPN gateways.A DoS Protection profile can be applied to a security policy rule that matches the traffic to and from the protected systems, and can specify the thresholds and actions for different types of flood attacks, such as SYN, UDP, ICMP, or other IP floods12.Reference:DoS Protection, PCNSE Study Guide (page 58)

Question 2

Question Type: MultipleChoice

When you import the configuration of an HA pair into Panorama, how do you prevent the import from affecting ongoing traffic?

Options:

A- Set the passive link state to shutdown'.
B- Disable config sync.
C- Disable the HA2 link.
D- Disable HA.

Answer:

B

Explanation:

To prevent the import from affecting ongoing traffic when you import the configuration of an HA pair into Panorama, you should disable config sync on both firewalls. Config sync is a feature that enables the firewalls in an HA pair to synchronize their configurations and maintain consistency. However, when you import the configuration of an HA pair into Panorama, you want to avoid any changes to the firewall configuration until you verify and commit the imported configuration on Panorama.Therefore, you should disable config sync before importing the configuration, and re-enable it after committing the changes on Panorama12.Reference:Migrate a Firewall HA Pair to Panorama Management, PCNSE Study Guide (page 50)

Question 3

Question Type: MultipleChoice

During the process of developing a decryption strategy and evaluating which websites are required for corporate users to access, several sites have been identified that cannot be decrypted due to technical reasons. In this case, the technical reason is unsupported ciphers Traffic to these sites will therefore be blocked if decrypted.

How should the engineer proceed?

Options:

A- Install the unsupported cipher into the firewall to allow the sites to be decrypted
B- Allow the firewall to block the sites to improve the security posture.
C- Add the sites to the SSL Decryption Exclusion list to exempt them from decryption.
D- Create a Security policy to allow access to those sites.

Answer:

C

Explanation:

If some sites cannot be decrypted due to technical reasons, such as unsupported ciphers, and blocking them is not an option, then the engineer should add the sites to the SSL Decryption Exclusion list to exempt them from decryption. The SSL Decryption Exclusion list is a predefined list of sites that are not subject to SSL decryption by the firewall. The list includes sites that use certificate pinning, mutual authentication, or unsupported cipher suites.The engineer can also add custom sites to the list if they have a valid business reason or technical limitation for not decrypting them34. Adding the sites to the SSL Decryption Exclusion list will allow the traffic to pass through without being decrypted or blocked by the firewall.Reference:SSL Decryption Exclusion,Troubleshoot Unsupported Cipher Suites

Question 4

Question Type: MultipleChoice

A threat intelligence team has requested more than a dozen Short signatures to be deployed on all perimeter Palo Alto Networks firewalls. How does the firewall engineer fulfill this request with the least time to implement?

Options:

A- Use Expedition to create custom vulnerability signatures, deploy them to Panorama using API and push them to the firewalls.
B- Create custom vulnerability signatures manually on one firewall export them, and then import them to the rest of the firewalls
C- Use Panorama IPs Signature Converter to create custom vulnerability signatures, and push them to the firewalls.
D- Create custom vulnerability signatures manually in Panorama, and push them to the firewalls

Answer:

C

Question 5

Question Type: MultipleChoice

An administrator needs to assign a specific DNS server to an existing template variable. Where would the administrator go to edit a template variable at the device level?

Options:

A- 'Managed Devices > Device Association'
B- PDF Export under 'Panorama > Templates'
C- Variable CSV export under 'Panorama > Templates'
D- Manage variables under 'Panorama > Templates'

Answer:

D

Question 6

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.

Question 7

Question Type: MultipleChoice

You are auditing the work of a co-worker and need to verify that they have matched the Palo Alto Networks Best Practices for Anti-Spyware Profiles.

For which three severity levels should single-packet captures be enabled to meet the Best Practice standard? (Choose three.)

Options:

A- Low
B- High
C- Critical
D- Informational
E- Medium

Answer:

B, C, E

Explanation:

https://docs.paloaltonetworks.com/best-practices/10-2/data-center-best-practices/data-center-best-practice-security-policy/how-to-create-data-center-best-practice-security-profiles/create-the-data-center-best-practice-anti-spyware-profile

The Palo Alto Networks Best Practices for Anti-Spyware Profiles recommend enabling single-

packet captures (PCAP) for medium, high, and critical severity threats. This allows for capturing the first packet of the malicious traffic for further analysis and investigation.PCAP should not be enabled for low and informational severity threats, as they generate a relatively high volume of traffic and are not particularly useful compared to potential threats2.Reference:Create the Data Center Best Practice Anti-Spyware Profile,Security Profile: Anti-Spyware, PCNSE Study Guide (page 57)

Question 8

Question Type: MultipleChoice

A firewall administrator is configuring an IPSec tunnel between Site A and Site B. The Site A firewall uses a DHCP assigned address on the outside interface of the firewall, and the Site B firewall uses a static IP address assigned to the outside interface of the firewall. However, the use of dynamic peering is not working.

Refer to the two sets of configuration settings provided. Which two changes will allow the configurations to work? (Choose two.)

Site A configuration:

Options:

A- Enable NAT Traversal on Site B firewall
B- Configure Local Identification on Site firewall
C- Disable passive mode on Site A firewall
D- Match IKE version on both firewalls.

Answer:

C, D

Explanation:

The image shows an IKE Gateway configuration where Site B is set to IKEv1 only mode, and passive mode is not enabled. For dynamic peering to work when Site A is using a DHCP assigned address:

Passive mode on Site A needs to be disabled. In passive mode, the firewall will not initiate the IKE negotiation and will only respond to negotiation requests from the peer. Since Site A has a dynamic IP, it must be able to initiate the connection to Site B, which has a static IP.

Matching the IKE version between Site A and Site B is also necessary for successful IPSec tunnel establishment. Since Site B is set to IKEv1 only mode, Site A also needs to be configured to use IKEv1 to ensure that both sites are using the same version for the IKE negotiation process.

NAT Traversal is used when there are NAT devices between the two endpoints, but there's no indication that this is the case here. Additionally, local identification on Site A is not necessarily related to the issue with dynamic peering not working.

P2P exams