IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **PCNSE**

Title : Palo Alto Networks Certified Network Security Engineer Exam

Version : DEMO

1.A network engineer has discovered that asymmetric routing is causing a Palo Alto Networks firewall to drop traffic. The network architecture cannot be changed to correct this.
Which two actions can be taken on the firewall to allow the dropped traffic permanently? (Choose two.)
A. Navigate to Network > Zone Protection Click Add
Select Packet Based Attack Protection > TCP/IP Drop Set "Reject Non-syn-TCP" to No Set "Asymmetric Path" to Bypass
B. > set session tcp-reject-non-syn no
C. Navigate to Network > Zone Protection Click Add
Select Packet Based Attack Protection > TCP/IP Drop Set "Reject Non-syn-TCP" to Global Set "Asymmetric Path" to Global
D. # set deviceconfig setting session tcp-reject-non-syn no
Answer: A, D
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClG2CAK

2.A firewall engineer reviews the PAN-OS GlobalProtect application and sees that it implicitly uses web-browsing and depends on SSL.
When creating a new rule, what is needed to allow the application to resolve dependencies?
A. Add SSL and web-browsing applications to the same rule.
B. Add web-browsing application to the same rule.
C. Add SSL application to the same rule.
D. SSL and web-browsing must both be explicitly allowed.
Answer: C
Explanation:
'Implicitly Uses' has web-browsing listed. This means that if you allow facebook-posting, that it will also be allowing the web-browsing application implicitly.. In our case, we dont know which APP the question referes too but 'Implicitly means already uses HTTP.

3.What are three tasks that cannot be configured from Panorama by using a template stack? (Choose three.)
A. Change the firewall management IP address
B. Configure a device block list
C. Add administrator accounts
D. Rename a vsys on a multi-vsys firewall
E. Enable operational modes such as normal mode, multi-vsys mode, or FIPS-CC mode
Answer: A, D, E

4.DRAG DROP
Match the terms to their corresponding definitions

Answer Area

management plane		provides configuration, logging, and reporting separate processor, RAM, and hard drive
signature matching		stream-based, uniform signature matching in exploits (IPS), virus, spyware, CC#, and SSN
security processing		high-density parallel processing for flexible standardized complex functions
network processing		network processing hardware-accelerated per-packet route lookup, MAC lookup, and NAT

Answer:

Answer Area

management plane	management plane	provides configuration, logging, and reporting separate processor, RAM, and hard drive
signature matching	signature matching	stream-based, uniform signature matching in exploits (IPS), virus, spyware, CC#, and SSN
security processing	security processing	high-density parallel processing for flexible standardized complex functions
network processing	network processing	network processing hardware-accelerated per-packet route lookup, MAC lookup, and NAT

Explanation:

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

5.Given the following snippet of a WildFire submission log did the end-user get access to the requested information and why or why not?

TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT
wildfire	web-browsing	allow	General Web Infrastructure	af55edec-93...		high			malicious
url	web-browsing	alert	General Web Infrastructure	af55edec-93...		informational	private-ip-addresses	private-ip-addresses	

A. Yes, because the action is set to alert

B. No, because this is an example from a defeated phishing attack

C. No, because the severity is high and the verdict is malicious.

D. Yes, because the action is set to allow.

Answer: D

Explanation:

https://live.paloaltonetworks.com/t5/general-topics/wildfire-submission-entries-with-severity-high-showing-action/td-p/143516