Question 1

Which profile or policy should be applied to protect against port scans from the internet?

Options:

A- An App-ID security policy rule to block traffic sourcing from the untrust zone

B- Security profiles to security policy rules for traffic sourcing from the untrust zone

C- Interface management profile on the zone of the ingress interface

D- Zone protection profile on the zone of the ingress interface

Answer:

D

Question 2

Which functionality is available to firewall users with an active Threat Prevention subscription, but no WildFire license?

Options:

A- PE file upload to WildFire

B- WildFire hybrid deployment

C- 5 minute WildFire updates to threat signatures

D- Access to the WildFire API

Answer:

C

Question 3

Question Type: **MultipleChoice**

In which two cases should the Hardware offering of Panorama be chosen over the Virtual Offering? (Choose two)

Options:

A- Dedicated Logger Mode is required

B- Logs per second exceed 10,000

C- Appliance needs to be moved into data center

D- Device count is under 100

Answer:

A, B

Question 4

Question Type: MultipleChoice

Which design objective could be satisfied by vsys functionality?

Options:

A- Separation of routing tables used by different departments in company

B- Provide same-device high availability functionality for different departments in a company

C- Administrative separation of firewall policies used by different departments in company

D- Allocate firewall hardware resources to different departments in a company

Answer:

C

Question 5

What two advantages of the DNS Sinkholing feature? (Choose two)

Options:

A- It can be deployed independently of an Anti-Spyware Profile.

B- It is monitoring DNS requests passively for malware domains.

C- It can work upstream from the internal DNS server.

D- It is forging DNS replies to known malicious domains.

Answer:

C, D

Explanation:

https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/threat-prevention/dns-sinkholing

Question 6

Question Type: **MultipleChoice**

Which two features are found in a next-generation firewall but are absent in a legacy firewall product? (Choose two)

Options:

A- Identification of application is possible on any port

B- Traffic is separated by zones

C- Traffic control is based on IP, port, and protocol

D- Policy match is a based on application

E- Onboard SSL decryption capability is used

Answer:

A, D

Question 7

Question Type: MultipleChoice

What is the recommended way to ensure that firewalls have the most current set of signatures for up-to-date protection?

Options:

A- Store updates on an intermediary server and point all the firewalls to it

B- Monitor update announcements and manually push updates to firewalls

C- Utilize dynamic updates with an aggressive update schedule

D- Run a Perl script to regularly check for updates and alert when one in released

Answer:

B

Question 8

Where are three tuning considerations when building a security policy to protect against modern day attacks? (Choose three)

Options:

A- Create an anti-spyware profile to block all spyware

B- Create a vulnerability protection profile to block all the vulnerabilities with severity low and higher

C- Create an SSL Decryption policy to decrypt 100% of the traffic

D- Create an antivirus profile to block all content that matches and antivirus signature

E- Create a WildFire profile to schedule file uploads during low network usage windows

Answer:

B, C, E