Free Questions for PCNSA by dumpshq

Shared by Norton on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

An administrator needs to create a Security policy rule that matches DNS traffic within the LAN zone, and also needs to match DNS traffic within the DMZ zone The administrator does not want to allow traffic between the DMZ and LAN zones.

Which Security policy rule type should they use?

Options:

A- default

B- universal

C- intrazone

D- interzone

Answer:

A

Question 2

An administrator would like to determine the default deny action for the application dns-over-https

Which action would yield the information?

Options:

A- View the application details in beacon paloaltonetworks.com

B- Check the action for the Security policy matching that traffic

C- Check the action for the decoder in the antivirus profile

D- View the application details in Objects > Applications

Answer:

C

Question 3

Question Type: **MultipleChoice**

An address object of type IP Wildcard Mask can be referenced in which part of the configuration?

Options:

A- Security policy rule

B- ACC global filter

C- external dynamic list

D- NAT address pool

Answer:

A

Explanation:

You can use an address object of type IP Wildcard Mask only in a Security policy rule.

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects-addresses

IP Wildcard Mask

---Enter an IP wildcard address in the format of an IPv4 address followed by a slash and a mask (which must begin with a zero); for example, 10.182.1.1/0.127.248.0. In the wildcard mask, a zero (0) bit indicates that the bit being compared must match the bit in the IP address that is covered by the 0. A one (1) bit in the mask is a wildcard bit, meaning the bit being compared need not match the bit in the

IP address that is covered by the 1. Convert the IP address and the wildcard mask to binary. To illustrate the matching: on binary snippet 0011, a wildcard mask of 1010 results in four matches (0001, 0011, 1001, and 1011).

Question 4

Question Type: **MultipleChoice**

An administrator would like to use App-ID's deny action for an application and would like that action updated with dynamic updates as new content becomes available.

Which security policy action causes this?

Options:

A- Reset server

B- Reset both

C- Deny

D- Drop

Answer:

C

Explanation:

Explanation/Reference:

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage- configuration backups/revert-firewall-configuration- changes.html

Question 5

Question Type: MultipleChoice

Which component is a building block in a Security policy rule?

Options:

A- decryption profile

B- destination interface

C- timeout (min)

D- application

Answer:

D

Explanation:

Explanation/Reference:

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/policies- security/buildingblocks-in-a-security-policy-rule.html

Question 6

Question Type: **MultipleChoice**

Which rule type is appropriate for matching traffic both within and between the source and destination zones?

Options:

A- interzone

B- shadowed

C- intrazone

D- universal

Answer:

A

Question 7

Question Type: **MultipleChoice**

You receive notification about new malware that infects hosts through malicious files transferred by FTP.

Which Security profile detects and protects your internal networks from this threat after you update your firewall's threat signature database?

Options:

A- URL Filtering profile applied to inbound Security policy rules.

B- Data Filtering profile applied to outbound Security policy rules.

C- Antivirus profile applied to inbound Security policy rules.

D- Vulnerability Prote

ction profile applied to outbound Security policy rules.

Answer:

C

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

Question 8

Question Type: MultipleChoice

How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

Options:

A- Disable automatic updates during weekdays

B- Automatically "download and install" but with the "disable new applications" option used

C- Automatically "download only" and then install Applications and Threats later, after the administrator approves the update

D- Configure the option for "Threshold"

Answer:

D

Question 9

Question Type: MultipleChoice

What is the main function of Policy Optimizer?

Options:

A- reduce load on the management plane by highlighting combinable security rules

B- migrate other firewall vendors' security rules to Palo Alto Networks configuration

C- eliminate "Log at Session Start" security rules

D- convert port-based security rules to application-based security rules
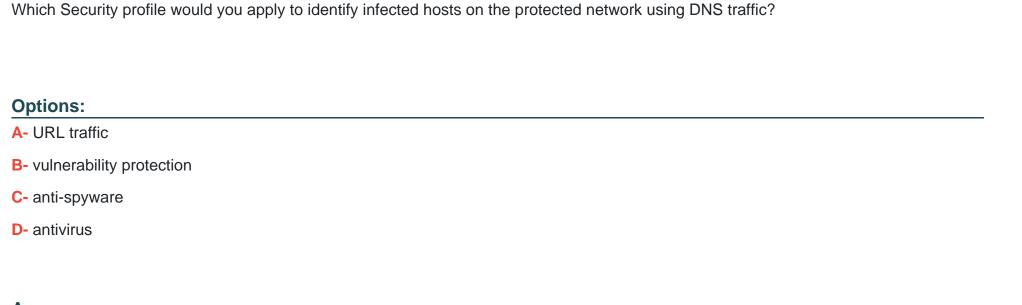
Answer:

D

Explanation:

Explanation/Reference: Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id-features/policy-optimizer.html

Question 10

Question Type: **MultipleChoice**

Which two firewall components enable you to configure SYN flood protection thresholds? (Choose two.)

Options:

A- QoS profile

B- DoS Protection profile

C- Zone Protection profile

D- DoS Protection policy

Answer:

B, C

Explanation:

Explanation

Explanation/Reference:

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

Question 11

Question Type: **MultipleChoice**

Which Security profile would you apply to identify infected hosts on the protected network using DNS traffic?

Options:

A- URL traffic

B- vulnerability protection

C- anti-spyware

D- antivirus

Answer:

C

Question 12

Question Type: **MultipleChoice**

An administrator wants to prevent users from submitting corporate credentials in a phishing attack.

Which Security profile should be applied?

Options:

A- antivirus

B- anti-spyware

C- URL filtering

D- vulnerability protection

Answer:

B