Vendor: Palo Alto Networks

Exam Code:PCNSA

Exam Name: Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)

Version: Demo

QUESTION 1

Which Security profile generates an alert based on a threshold when the action is set to Alert?

A. Vulnerability Protection

B. Antivirus

C. DoS protection

D. Anti-Spyware

Correct Answer: A

Reference: https://docs.paloaltonetworks.com/network-security/security-policy/security-profiles/security-profile-vulnerability-protection#:~:text=Typically%20the%20default%20action%20is,the%20threat%20or%20Antivirus% 20signature.andtext=action%20does%20not%20generate%20logs%20related%20to%20the%20signatures%20or%20profiles

---

QUESTION 2

Why should a company have a File Blocking profile that is attached to a Security policy?

A. To block uploading and downloading of specific types of files

B. To detonate files in a sandbox environment

C. To analyze file types

D. To block uploading and downloading of any type of files

Correct Answer: A

QUESTION 3

Which profile must be applied to the Security policy rule to block spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers?

A. Anti-spyware

B. File blocking

C. WildFire

D. URL filtering

Correct Answer: D

QUESTION 4

Which attribute can a dynamic address group use as a filtering condition to determine its membership?

A. tag

B. wildcard mask

C. IP address

D. subnet mask

Correct Answer: A

Dynamic Address Groups: A dynamic address group populates its members dynamically using looks ups for tags and tag-based filters. Dynamic address groups are very useful if you have an extensive virtual infrastructure where changes in virtual machine location/IP address are frequent. For example, you have a sophisticated failover setup or provision new virtual machines frequently and would like to apply policy to traffic from or to the new machine without modifying the configuration/rules on the firewall. https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects- address-groups

---

QUESTION 5

The NetSec Manager asked to create a new firewall Local Administrator profile with customized privileges named NewAdmin. This new administrator has to authenticate without inserting any username or password to access the WebUI. What steps should the administrator follow to create the New_Admin Administrator profile?

A. 1. Select the "Use only client certificate authentication" check box.

2.

Set Role to Role Based.

3.

Issue to the Client a Certificate with Common Name = NewAdmin

B. 1. Select the "Use only client certificate authentication" check box.

2.

Set Role to Dynamic.

3.

Issue to the Client a Certificate with Certificate Name = NewAdmin

C. 1. Set the Authentication profile to Local.

2.

Select the "Use only client certificate authentication" check box.

3.

Set Role to Role Based.

D. 1. Select the "Use only client certificate authentication" check box.

2.

Set Role to Dynamic.

3.

Issue to the Client a Certificate with Common Name = New Admin

Correct Answer: B

QUESTION 6

Where within the firewall GUI can all existing tags be viewed?

A. Network > Tags

B. Monitor > Tags

C. Objects > Tags

D. Policies > Tags

Correct Answer: C

Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-tags-to-group-and-visually-distinguish-objects/create-and-apply-tags

---

QUESTION 7

Which two App-ID applications will need to be allowed to use Facebook-chat? (Choose two.)

A. facebook

B. facebook-chat

C. facebook-base

D. facebook-email

Correct Answer: BC

QUESTION 8

Which built-in IP address EDL would be useful for preventing traffic from IP addresses that are verified as unsafe based on WildFire analysis Unit 42 research and data gathered from telemetry?

A. Palo Alto Networks CandC IP Addresses

B. Palo Alto Networks Bulletproof IP Addresses

C. Palo Alto Networks High-Risk IP Addresses

D. Palo Alto Networks Known Malicious IP Addresses

Correct Answer: D

Palo Alto Networks Known Malicious IP Addresses --Contains IP addresses that are verified malicious based on WildFire analysis, Unit 42 research, and data gathered from telemetry (Share ThreatIntelligence with Palo Alto Networks). Attackers use these IP addresses almost exclusively to distribute malware, initiate command-and-control activity, and launch attacks.

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external- dynamic-list-in-policy/built-in-edls

---

QUESTION 9

Given the screenshot, what are two correct statements about the logged traffic? (Choose two.)

TYPE	FROM ZONE	TO ZONE	INGRESS I/F	SOURCE	NAT APPLIED	EGRESS I/F	DESTINATION	TO PORT	APPLICATION	ACTION	SESSION END REASON	BYTES	ACTION SOURCE	LOG ACTION	BYTES SENT	BYTES RECEIVED	LOG TYPE
end	LAN	Internet	ethernet1/2	192.168.200.100	yes	ethernet1/5	198.54.12.97	443	web-browsing	allow	threat	3.3k	from-policy	default	2.7k	541	traffic

A. The web session was unsuccessfully decrypted.

B. The traffic was denied by security profile.

C. The traffic was denied by URL filtering.

D. The web session was decrypted.

Correct Answer: BD

QUESTION 10

Which interface does not require a MAC or IP address?

A. Virtual Wire

B. Layer3

C. Layer2

D. Loopback

Correct Answer: A

QUESTION 11

You receive notification about a new malware that infects hosts An infection results in the infected host attempting to contact a command-and-control server Which Security Profile when applied to outbound Security policy rules detects and prevents this threat from establishing a command-and-control connection?

A. Antivirus Profile

B. Data Filtering Profile

C. Vulnerability Protection Profile

D. Anti-Spyware Profile

Correct Answer: D

Anti-Spyware Security Profiles block spyware on compromised hosts from trying to communicate with external command-and-control (C2) servers, thus enabling you to detect malicious traffic leaving the network from infected clients.

QUESTION 12

Which User Credential Detection method should be applied within a URL Filtering Security profile to check for the submission of a valid corporate username and the associated password?

A. Domain Credential

B. IP User

C. Group Mapping

D. Valid Username Detected Log Severity

Correct Answer: C