

## PCNSA<sup>Q&As</sup>

Palo Alto Networks Certified Network Security Administrator

### Pass Palo Alto Networks PCNSA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.lead4pass.com/pcnsa.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



## QUESTION 1

Which statement best describes a common use of Policy Optimizer?

- A. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications.
- B. Policy Optimizer can add or change a Log Forwarding profile for each Security policy selected.
- C. Policy Optimizer can display which Security policies have not been used in the last 90 days.
- D. Policy Optimizer can be used on a schedule to automatically create a disabled Layer 7 App-ID Security policy for every Layer 4 policy that exists. Admins can then manually enable policies they want to keep and delete ones they want to remove.

Correct Answer: C

---

## QUESTION 2

Which path in PAN-OS 10.0 displays the list of port-based security policy rules?

- A. Policies> Security> Rule Usage> No App Specified
- B. Policies> Security> Rule Usage> Port only specified
- C. Policies> Security> Rule Usage> Port-based Rules
- D. Policies> Security> Rule Usage> Unused Apps

Correct Answer: A

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/security-policy-rule-optimization/migrate-port-based-to-app-id-based-security-policy-rules.html>

---

## QUESTION 3

Which two security profile types can be attached to a security policy? (Choose two.)

- A. antivirus
- B. DDoS protection
- C. threat
- D. vulnerability

Correct Answer: AD

---

## QUESTION 4

Complete the statement. A security profile can block or allow traffic\_\_\_\_\_

- A. on unknown-tcp or unknown-udp traffic
- B. after it is matched by a security policy that allows traffic
- C. before it is matched by a security policy
- D. after it is matched by a security policy that allows or blocks traffic

Correct Answer: B

Security profiles are objects added to policy rules that are configured with an action of allow.

---

#### QUESTION 5

Which User-ID agent would be appropriate in a network with multiple WAN links, limited network bandwidth, and limited firewall management plane resources?

- A. Windows-based agent deployed on the internal network
- B. PAN-OS integrated agent deployed on the internal network
- C. Citrix terminal server deployed on the internal network
- D. Windows-based agent deployed on each of the WAN Links

Correct Answer: A

Another reason to choose the Windows agent over the integrated PAN-OS agent is to save processing cycles on the firewall's management plane.

---

#### QUESTION 6

Which protocol used to map username to user groups when user-ID is configured?

- A. SAML
- B. RADIUS
- C. TACACS+
- D. LDAP

Correct Answer: D

---

#### QUESTION 7

Which two settings allow you to restrict access to the management interface? (Choose two )

- A. enabling the Content-ID filter

- B. administrative management services
- C. restricting HTTP and telnet using App-ID
- D. permitted IP addresses

Correct Answer: AC

---

#### QUESTION 8

Which action results in the firewall blocking network traffic with out notifying the sender?

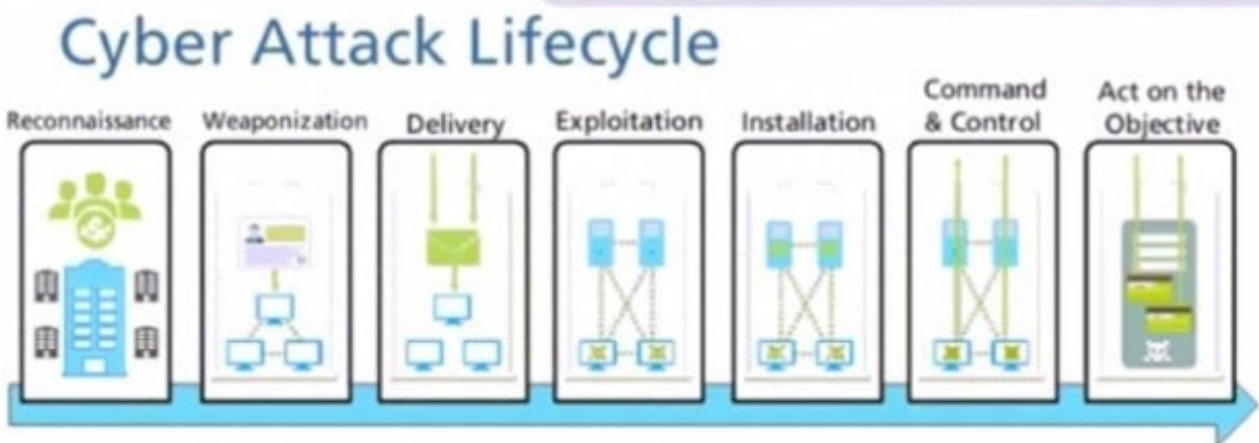
- A. Drop
- B. Deny
- C. Reset Server
- D. Reset Client

Correct Answer: B

---

#### QUESTION 9

At which stage of the cyber-attack lifecycle would the attacker attach an infected PDF file to an email?



- A. delivery
- B. command and control
- C. exploitation
- D. reinsurance
- E. installation

Correct Answer: A

---

**QUESTION 10**

Choose the option that correctly completes this statement. A Security Profile can block or allow traffic \_\_\_\_\_.

- A. on either the data plane or the management plane.
- B. after it is matched by a security policy rule that allows traffic.
- C. before it is matched to a Security policy rule.
- D. after it is matched by a security policy rule that allows or blocks traffic.

Correct Answer: B

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-policy.html>

After a packet has been allowed by the Security policy, Security Profiles are used to scan packets for threats, vulnerabilities, viruses, spyware, malicious URLs, data exfiltration, and exploitation software.

**QUESTION 11**

DRAG DROP

Match the Palo Alto Networks Security Operating Platform architecture to its description. (Match each feature to the DoS Protection Policy or the DoS Protection Profile.)

Select and Place:

<b>Threat Intelligence Cloud</b>	Drag answer here	Identifies and inspects all traffic to block known threats.
<b>Next-Generation Firewall</b>	Drag answer here	Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.
<b>Advanced Endpoint Protection</b>	Drag answer here	Inspects processes and files to prevent known and unknown exploits.

Correct Answer:

**Threat Intelligence Cloud**

Identifies and inspects all traffic to block known threats.

**Next-Generation Firewall**

Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.

**Advanced Endpoint Protection**

Inspects processes and files to prevent known and unknown exploits.

**QUESTION 12**

What is a recommended consideration when deploying content updates to the firewall from Panorama?

- A. Before deploying content updates, always check content release version compatibility.
- B. Content updates for firewall A/P HA pairs can only be pushed to the active firewall.
- C. Content updates for firewall A/A HA pairs need a defined master device.
- D. After deploying content updates, perform a commit and push to Panorama.

Correct Answer: D

Reference: <https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-licenses-and-updates/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama/schedule-a-content-update-usingpanorama.html>

**QUESTION 13**

An administrator is implementing an exception to an external dynamic list by adding an entry to the list manually. The administrator wants to save the changes, but the OK button is grayed out.

What are two possible reasons the OK button is grayed out? (Choose two.)

- A. The entry contains wildcards.
- B. The entry is duplicated.
- C. The entry doesn't match a list entry.

D. The entry matches a list entry.

Correct Answer: BC

### QUESTION 14

How often does WildFire release dynamic updates?

- A. every 5 minutes
- B. every 15 minutes
- C. every 60 minutes
- D. every 30 minutes

Correct Answer: A

### QUESTION 15

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

[PCNSA VCE Dumps](#)

[PCNSA Exam Questions](#)

[PCNSA Braindumps](#)