



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

Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 11.x





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

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

<https://www.passapply.com/pcnse.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

As a best practice, which URL category should you target first for SSL decryption\*?

- A. Online Storage and Backup
- B. High Risk
- C. Health and Medicine
- D. Financial Services

Correct Answer: B

<https://docs.paloaltonetworks.com/best-practices/10-0/decryption-best-practices/decryption-best-practices/plan-ssl-decryption-best-practice-deployment.html> Phase in decryption. Plan to decrypt the riskiest traffic first (URL Categories most likely to harbor malicious traffic, such as gaming or high-risk)

---

### QUESTION 2

An administrator is using Panorama and multiple Palo Alto Networks NGFWs. After upgrading all devices to the latest PAN-OS software, the administrator enables log forwarding from the firewalls to Panorama. Pre-existing logs from the firewalls are not appearing in Panorama.

Which action would enable the firewalls to send their pre-existing logs to Panorama?

- A. Use the import option to pull logs into Panorama.
- B. A CLI command will forward the pre-existing logs to Panorama.
- C. Use the ACC to consolidate pre-existing logs.
- D. The log database will need to be exported from the firewalls and manually imported into Panorama.

Correct Answer: B

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/management-features/pa-7000-series-firewall-log-forwarding-to-panorama> <https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/set-up-panorama/installcontent-and-software-updates-for-panorama/migrate-panorama-logs-to-new-log-format>

---

### QUESTION 3

An engineer is tasked with configuring SSL forward proxy for traffic going to external sites.

Which of the following statements is consistent with SSL decryption best practices?

- A. The forward trust certificate should not be stored on an HSM.
- B. The forward untrust certificate should be signed by a certificate authority that is trusted by the clients.
- C. Check both the Forward Trust and Forward Untrust boxes when adding a certificate for use with SSL decryption



D. The forward untrust certificate should not be signed by a Trusted Root CA

Correct Answer: B

According to the PCNSE Study Guide<sup>1</sup>, SSL forward proxy is a feature that allows the firewall to decrypt and inspect SSL traffic going to external sites. The firewall acts as a proxy between the client and the server, generating a certificate on

the fly for each site.

The best practices for configuring SSL forward proxy are<sup>23</sup>:

Use a forward trust certificate that is signed by a certificate authority (CA) that is trusted by the clients. This certificate is used to sign certificates for sites that have valid certificates from trusted CAs. The clients will not see any certificate errors

if they trust the forward trust certificate.

Use a forward untrust certificate that is not signed by a trusted CA. This certificate is used to sign certificates for sites that have invalid or untrusted certificates. The clients will see certificate errors if they do not trust the forward untrust

certificate. This helps alert users of potential risks and prevent man-in-the-middle attacks. Do not store the forward trust or untrust certificates on an HSM (hardware security module). The HSM does not support on-the-fly signing of certificates,

which is required for SSL forward proxy.

---

#### QUESTION 4

Several offices are connected with VPNs using static IPv4 routes. An administrator has been tasked with implementing OSPF to replace static routing. Which step is required to accomplish this goal?

- A. Assign an IP address on each tunnel interface at each site
- B. Enable OSPFv3 on each tunnel interface and use Area ID 0.0.0.0
- C. Assign OSPF Area ID 0.0.0.0 to all Ethernet and tunnel interfaces
- D. Create new VPN zones at each site to terminate each VPN connection

Correct Answer: C

---

#### QUESTION 5

SD-WAN is designed to support which two network topology types? (Choose two.)

- A. ring
- B. point-to-point
- C. hub-and-spoke



D. full-mesh

Correct Answer: CD

<https://docs.paloaltonetworks.com/plugins/vm-series-and-panorama-plugins-release-notes/panorama-plugin-for-sd-wan/sd-wan-plugin-200/features-introduced-in-sd-wan-2-0.html>

[https://www.paloaltonetworks.nl/apps/pan/public/downloadResource?pagePath=/content/pan/en\\_US/resources/guides/pan-os-secure-sd-wan-deployment-guide](https://www.paloaltonetworks.nl/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/guides/pan-os-secure-sd-wan-deployment-guide)

[Latest PCNSE Dumps](#)

[PCNSE PDF Dumps](#)

[PCNSE Practice Test](#)