

# PCNSE8<sup>Q&As</sup>

Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 8.0

## Pass Palo Alto Networks PCNSE8 Exam with 100% Guarantee

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

<https://www.leads4pass.com/pcnse8.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

A firewall administrator is troubleshooting problems with traffic passing through the Palo Alto Networks firewall. Which method shows the global counters associated with the traffic after configuring the appropriate packet filters?

- A. From the CLI, issue the show counter global filter pcap yes command.
- B. From the CLI, issue the show counter global filter packet-filter yes command.
- C. From the GUI, select show global counters under the monitor tab.
- D. From the CLI, issue the show counter interface command for the ingress interface.

Correct Answer: B

---

## QUESTION 2

Which Zone Pair and Rule Type will allow a successful connection for a user on the internet zone to a web server hosted in the DMZ zone? The web server is reachable using a destination Nat policy in the Palo Alto Networks firewall.

- A. Zone Pair: Source Zone: Internet Destination Zone: DMZ Rule Type: "intrazone"
- B. Zone Pair: Source Zone: Internet Destination Zone: DMZ Rule Type: "intrazone" or "universal"
- C. Zone Pair: Source Zone: Internet Destination Zone: Internet Rule Type: "intrazone" or "universal"
- D. Zone Pair: Source Zone: Internet

Destination Zone: Internet

Rule Type:

"intrazone"

Correct Answer: B

---

## QUESTION 3

An administrator encountered problems with inbound decryption. Which option should the administrator investigate as part of triage?

- A. Security policy rule allowing SSL to the target server
- B. Firewall connectivity to a CRL
- C. Root certificate imported into the firewall with "Trust" enabled
- D. Importation of a certificate from an HSM

Correct Answer: A

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssl-inbound-inspection>

---

#### QUESTION 4

A Palo Alto Networks firewall is being targeted by an NTP Amplification attack and is being flooded with tens thousands of bogus UDP connections per second to a single destination IP address and port. Which option when enabled with the correction threshold would mitigate this attack without dropping legitimate traffic to other hosts inside the network?

- A. Zone Protection Policy with UDP Flood Protection
- B. QoS Policy to throttle traffic below maximum limit
- C. Security Policy rule to deny traffic to the IP address and port that is under attack
- D. Classified DoS Protection Policy using destination IP only with a Protect action

Correct Answer: D

---

#### QUESTION 5

Based on the image, what caused the commit warning?

The screenshot shows a network management interface with a 'Device' tab selected. Under 'Device Certificates', there is a sub-tab for 'Default Trusted Certificate Authorities'. A table lists two certificates:

Name	Subject	Issuer	CA	Key	Expires	Status	AI...	Usage
FWDtrust	CN=FWDtrust	DC = local, DC = lab, CN = lab-SRV2016-LABCA-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29 02:02:05 2020 GMT	valid	RSA	Forward Trust Certificate
FWD-UnTrust	CN = FWD-UnTrust	CN = FWD-UnTrust	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29 02:06:36 2019 GMT	valid	RSA	Forward Trust Certificate

Below the table, a 'Commit Status' dialog box is open, showing the following information:

```

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully
Warnings Warning: cannot find complete certificate chain for certificate FWDtrust (Module: device)
    
```

The dialog box has 'Cancel' and 'Close' buttons at the bottom.

- A. The CA certificate for FWDtrust has not been imported into the firewall.
- B. The FWDtrust certificate has not been flagged as Trusted Root CA.
- C. SSL Forward Proxy requires a public certificate to be imported into the firewall.
- D. The FWDtrust certificate does not have a certificate chain.

Correct Answer: D

[Latest PCNSE8 Dumps](#)

[PCNSE8 Study Guide](#)

[PCNSE8 Exam Questions](#)