

➤ **Vendor: Palo Alto Networks**

➤ **Exam Code: PCNSE**

➤ **Exam Name: Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 10.0**

➤ **New Updated Questions from [Braindump2go](#)**

➤ **(Updated in [November/2022](#))**

[Visit Braindump2go and Download Full Version PCNSE Exam Dumps](#)

QUESTION 580

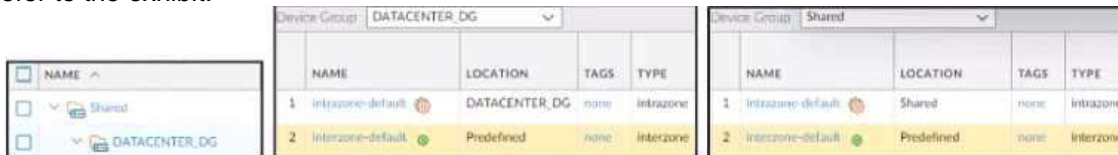
An engineer needs to configure SSL Forward Proxy to decrypt traffic on a PA-5260. The engineer uses a forward trust certificate from the enterprise PKI that expires December 31, 2025. The validity date on the PA-generated certificate is taken from what?

- A. The trusted certificate
- B. The server certificate
- C. The untrusted certificate
- D. The root CA

Answer: B

QUESTION 581

Refer to the exhibit.



Device Group: DATACENTER_DG				
NAME	LOCATION	TAGS	TYPE	
1 Intrazone-default	DATACENTER_DG	none	Intrazone	
2 Interzone-default	Predefined	none	Interzone	

Device Group: Shared				
NAME	LOCATION	TAGS	TYPE	
1 Intrazone-default	Shared	none	Intrazone	
2 Interzone-default	Predefined	none	Interzone	

Based on the screenshots above, what is the correct order in which the various rules are deployed to firewalls inside the DATACENTER_DG device group?

- A. shared pre-rules
 DATACENTER DG pre rules
 rules configured locally on the firewall
 shared post-rules
 DATACENTER_DG post-rules
 DATACENTER.DG default rules
- B. shared pre-rules
 DATACENTER_DG pre-rules
 rules configured locally on the firewall
 shared post-rules
 DATACENTER.DG post-rules
 shared default rules
- C. shared pre-rules
 DATACENTER_DG pre-rules
 rules configured locally on the firewall

- DATACENTER_DG post-rules
- shared post-rules
- shared default rules
- D. shared pre-rules
 - DATACENTER_DG pre-rules
 - rules configured locally on the firewall
 - DATACENTER_DG post-rules
 - shared post-rules
 - DATACENTER_DG default rules

Answer: A

QUESTION 582

How can Panorama help with troubleshooting problems such as high CPU or resource exhaustion on a managed firewall?

- A. Firewalls send SNMP traps to Panorama when resource exhaustion is detected Panorama generates a system log and can send email alerts
- B. Panorama provides visibility into all the system and traffic logs received from firewalls it does not offer any ability to see or monitor resource utilization on managed firewalls
- C. Panorama monitors all firewalls using SNMP It generates a system log and can send email alerts when resource exhaustion is detected on a managed firewall
- D. Panorama provides information about system resources of the managed devices in the Managed Devices > Health menu

Answer: A

QUESTION 583

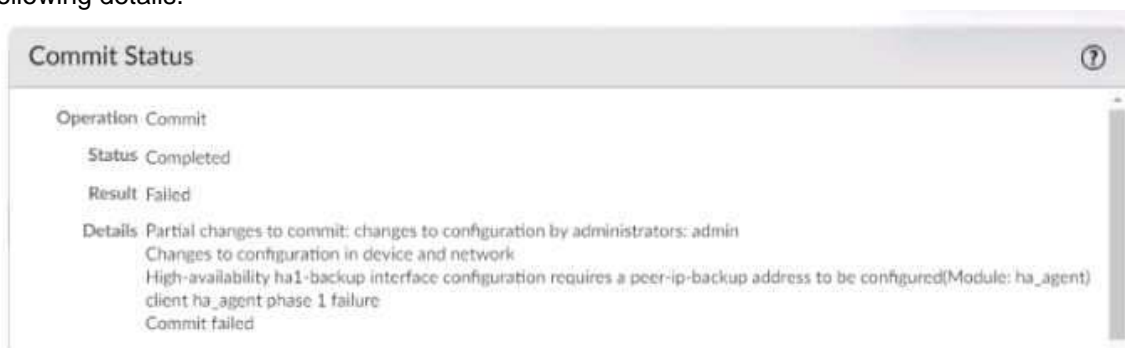
Four configuration choices are listed, and each could be used to block access to a specific URL. If you configured each choice to block the same URL, then which choice would be evaluated last in the processing order to block access to the URL1?

- A. PAN-DB URL category in URL Filtering profile
- B. Custom URL category in Security policy rule
- C. Custom URL category in URL Filtering profile
- D. EDL in URL Filtering profile

Answer: D

QUESTION 584

After configuring HA in Active/Passive mode on a pair of firewalls the administrator gets a failed commit with the following details.



What are two s for this type of issue? (Choose two)

- A. The peer IP is not included in the permit list on Management Interface Settings

- B. The Backup Peer HA1 IP Address was not configured when the commit was issued
- C. Either management or a data-plane interface is used as HA1-backup
- D. One of the firewalls has gone into the suspended state

Answer: BC

QUESTION 585

A company with already deployed Palo Alto firewalls has purchased their first Panorama server. The security team has already configured all firewalls with the Panorama IP address and added all the firewall serial numbers in Panorama. What are the next steps to migrate configuration from the firewalls to Panorama?

- A. Use API calls to retrieve the configuration directly from the managed devices
- B. Export Named Configuration Snapshot on each firewall followed by Import Named Configuration Snapshot in Panorama
- C. import Device Configuration to Panorama followed by Export or Push Device Config Bundle
- D. Use the Firewall Migration plugin to retrieve the configuration directly from the managed devices

Answer: C

QUESTION 586

Which log type would provide information about traffic blocked by a Zone Protection profile?

- A. Data Filtering
- B. IP-Tag
- C. Traffic
- D. Threat

Answer: C

QUESTION 587

An engineer is creating a template and wants to use variables to standardize the configuration across a large number of devices. Which two variable types can be defined? (Choose two.)

- A. Path group
- B. Zone
- C. IP netmask
- D. FQDN

Answer: CD

QUESTION 588

An engineer is bootstrapping a VM-Series Firewall Other than the /config folder, which three directories are mandatory as part of the bootstrap package directory structure? (Choose three.)

- A. /software
- B. /opt
- C. /license
- D. /content
- E. /plugins

Answer: AD

QUESTION 589

Review the screenshot of the Certificates page.



Issued To	Issued By	Expiration Date	Issued On
C:\Users\Administrator\My Computer	C:\Users\Administrator\My Computer	12/31/2022	12/31/2022
C:\Users\Administrator\My Computer	C:\Users\Administrator\My Computer	12/31/2022	12/31/2022
C:\Users\Administrator\My Computer	C:\Users\Administrator\My Computer	12/31/2022	12/31/2022

An administrator for a small LLC has created a series of certificates as shown, to use for a planned Decryption roll out. The administrator has also installed the self-signed root certificate on all client systems. When testing, they noticed that every time a user visited an SSL site they received unsecured website warnings. What is the cause of the unsecured website warnings.

- A. The forward trust certificate has not been signed by the self-signed root CA certificate
- B. The self-signed CA certificate has the same CN as the forward trust and untrust certificates
- C. The forward untrust certificate has not been signed by the self-signed root CA certificate
- D. The forward trust certificate has not been installed in client systems

Answer: C

QUESTION 590

Which statement about High Availability timer settings is true?

- A. Use the Moderate timer for typical failover timer settings.
- B. Use the Critical timer for faster failover timer settings.
- C. Use the Recommended timer for faster failover timer settings.
- D. Use the Aggressive timer for faster failover timer settings

Answer: C

QUESTION 591

What are two best practices for incorporating new and modified App-IDs? (Choose two)

- A. Configure a security policy rule to allow new App-IDs that might have network-wide impact
- B. Study the release notes and install new App-IDs if they are determined to have low impact
- C. Perform a Best Practice Assessment to evaluate the impact of the new or modified App-IDs
- D. Run the latest PAN-OS version in a supported release tree to have the best performance for the new App-IDs

Answer: AB