PCNSE Q&As

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.leads4pass.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

Which Panorama feature protects logs against data loss if a Panorama server fails?

A. Panorama HA automatically ensures that no logs are lost if a server fails inside the HA Cluster.

B. Panorama Collector Group with Log Redundancy ensures that no logs are lost if a server fails inside the Collector Group.

C. Panorama HA with Log Redundancy ensures that no logs are lost if a server fails inside the HA Cluster.

D. Panorama Collector Group automatically ensures that no logs are lost if a server fails inside the Collector Group

Correct Answer: B

"Log redundancy is available only if each Log Collector has the same number of logging disks." (Recommended) Enable log redundancy across collectors if you are adding multiple Log Collectors to a single Collector group. Redundancy ensures that no logs are lost if any one Log Collector becomes unavailable. Each log will have two copies and each copy will reside on a different Log Collector. For example, if you have two Log Collectors in the collector group the log is written to both Log Collectors. Enabling redundancy creates more logs and therefore requires more storage capacity, reducing storage capability in half. When a Collector Group runs out of space, it deletes older logs. Redundancy also doubles the log processing traffic in a Collector Group, which reduces its maximum logging rate by half, as each Log Collector must distribute a copy of each log it receives.

https://docs.paloaltonetworks.com/panorama/11-0/panorama-admin/manage-log-collection/manage-collector-groups/configure-a-collector-group

---

QUESTION 2

Which log file can be used to identify SSL decryption failures?

A. Configuration

B. Threats

C. ACC

D. Traffic

Correct Answer: D

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClboCAC

QUESTION 3

An engineer needs to redistribute User-ID mappings from multiple data centers. Which data flow best describes redistribution of user mappings?

A. Domain Controller to User-ID agent

B. User-ID agent to Panorama

C. User-ID agent to firewall

D. firewall to firewall

Correct Answer: D

QUESTION 4

When setting up a security profile which three items can you use? (Choose three)

A. Wildfire analysis

B. anti-ransom ware

C. antivirus

D. URL filtering

E. decryption profile

Correct Answer: ACD

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security- profiles

QUESTION 5

An administrator connected a new fiber cable and transceiver to interface Ethernetl/l on a Palo Alto Networks firewall. However, the link does not seem to be coming up.

If an administrator were to troubleshoot, how would they confirm the transceiver type, tx-power, rx-power, vendor name, and part number via the CLI?

A. show system state filter sw.dev.interface.config

B. show chassis status slot s1

C. show system state filter-pretty sys.s1.*

D. show system state filter ethernet1/1

Correct Answer: C

The correct syntax should be show system state filter-pretty sys.s1.p1.phy, where s is slot 1, p is port one = ethernet1/1

QUESTION 6

An organization conducts research on the benefits of leveraging the Web Proxy feature of PAN-OS 11.0.

What are two benefits of using an explicit proxy method versus a transparent proxy method? (Choose two.)

A. No client configuration is required for explicit proxy, which simplifies the deployment complexity.

B. Explicit proxy allows for easier troubleshooting, since the client browser is aware of the existence of the proxy.

C. Explicit proxy supports interception of traffic using non-standard HTTPS ports.

D. It supports the X-Authenticated-User (XAU) header, which contains the authenticated username in the outgoing request

Correct Answer: BD

QUESTION 7

What happens, by default, when the GlobalProtect app fails to establish an IPSec tunnel to the GlobalProtect gateway?

A. It keeps trying to establish an IPSec tunnel to the GlobalProtect gateway

B. It stops the tunnel-establishment processing to the GlobalProtect gateway immediately

C. It tries to establish a tunnel to the GlobalProtect gateway using SSL/TLS

D. It tries to establish a tunnel to the GlobalProtect portal using SSL/TLS

Correct Answer: C

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface- help/globalprotect/network-globalprotect-portals/globalprotect-portals-agent-configuration- tab/globalprotect-portals-agent-app-tab.html

QUESTION 8

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 9

What best describes the HA Promotion Hold Time?

A. the time that is recommended to avoid an HA failover due to the occasional flapping of neighboring devices

B. the time that is recommended to avoid a failover when both firewalls experience the same link/path monitor failure simultaneously

C. the time that the passive firewall will wait before taking over as the active firewall after communications with the HA peer have been lost

D. the time that a passive firewall with a low device priority will wait before taking over as the active firewall if the firewall is operational again

Correct Answer: C

QUESTION 10

An organization wants to begin decrypting guest and BYOD traffic.

Which NGFW feature can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted?

A. Authentication Portal

B. SSL Decryption profile

C. SSL decryption policy

D. comfort pages

Correct Answer: D

https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-web-interface-help/device/device-response-pages

QUESTION 11

Which of the following commands would you use to check the total number of the sessions that are currently going through SSL Decryption processing?

A. show session all ssl-decrypt yes count yes

B. show session filter ssl-decryption yes total-count yes

C. show session all filter ssl-decrypt yes count yes

D. show session all filter ssl-decryption yes total-count yes

Correct Answer: C

QUESTION 12

If a template stack is assigned to a device and the stack includes three templates with overlapping settings, which settings are published to the device when the template stack is pushed?

A. The settings assigned to the template that is on top of the stack.

B. The administrator will be promoted to choose the settings for that chosen firewall.

C. All the settings configured in all templates.

D. Depending on the firewall location, Panorama decides with settings to send.

Correct Answer: A

Reference:

https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/ma nage-firewalls/manage-templates-and-template-stacks/configure-a-template-stack

QUESTION 13

Which two benefits come from assigning a Decryption Profile to a Decryption policy rule with a "No Decrypt" action? (Choose two.)

A. Block sessions with expired certificates

B. Block sessions with client authentication

C. Block sessions with unsupported cipher suites

D. Block sessions with untrusted issuers

E. Block credential phishing

Correct Answer: AD

https://www.paloaltonetworks.com/documentation/71/pan-os/pan- os/decryption/configure-decryption-exceptions Block sessions based on certificate status, including blocking sessions with expired certificates, untrusted issuers, unknown certificate status, certificate status check timeouts, and certificate extensions. Block sessions with unsupported versions and cipher suites, and that require using client authentication.