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.pass4itsure.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

QUESTION 1

An engineer is monitoring an active/active high availability (HA) firewall pair.

Which HA firewall state describes the firewall that is experiencing a failure of a monitored path?

A. Initial

B. Passive

C. Active-secondary

D. Tentative

Correct Answer: D

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/ha-firewall-states

QUESTION 2

Information Security is enforcing group-based policies by using security-event monitoring on Windows User-ID agents for IP-to-User mapping in the network. During the rollout, Information Security identified a gap for users authenticating to their VPN and wireless networks.

Root cause analysis showed that users were authenticating via RADIUS and that authentication events were not captured on the domain controllers that were being monitored Information Security found that authentication events existed on the Identity Management solution (IDM). There did not appear to be direct integration between PAN-OS and the IDM solution

How can Information Security extract and learn iP-to-user mapping information from authentication events for VPN and wireless users?

A. Add domain controllers that might be missing to perform security-event monitoring for VPN and wireless users.

B. Configure the integrated User-ID agent on PAN-OS to accept Syslog messages over TLS.

C. Configure the User-ID XML API on PAN-OS firewalls to pull the authentication events directly from the IDM solution

D. Configure the Windows User-ID agents to monitor the VPN concentrators and wireless controllers for IP-to-User mapping.

Correct Answer: B

QUESTION 3

A firewall engineer has determined that, in an application developed by the company\\'s internal team, sessions often remain idle for hours before the client and server exchange any data. The application is also currently identified as unknowntcp by the firewalls. It is determined that because of a high level of trust, the application does not require to be scanned for threats, but it needs to be properly identified in Traffic logs for reporting purposes.

Which solution will take the least time to implement and will ensure the App-ID engine is used to identify the application?

A. Create a custom application with specific timeouts and signatures based on patterns discovered in packet captures.

B. Access the Palo Alto Networks website and complete the online form to request that a new application be added to App-ID.

C. Create a custom application with specific timeouts, then create an application override rule and reference the custom application.

D. Access the Palo Alto Networks website and raise a support request through the Customer Support Portal.

Correct Answer: C

QUESTION 4

How can an administrator configure the NGFW to automatically quarantine a device using GlobalProtect?

A. by adding the device\\'s Host ID to a quarantine list and configure GlobalProtect to prevent users from connecting to the GlobalProtect gateway from a quarantined device

B. by using security policies, log forwarding profiles, and log settings.

C. by exporting the list of quarantined devices to a pdf or csv file by selecting PDF/CSV at the bottom of the Device Quarantine page and leveraging the approbate XSOAR playbook

D. There is no native auto-quarantine feature so a custom script would need to be leveraged.

Correct Answer: B

https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new- features/globalprotect-features/identification-and-quarantine-of-compromised-devices.html https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/hostinformation/quarantine-devices-using-host-information/automatically-quarantine-a-device.html#idb42b2b82-b253-4be7-9840-1efa49dba3da

QUESTION 5

Which three methods are supported for split tunneling in the GlobalProtect Gateway? (Choose three.)

A. Video Streaming Application

B. Destination Domain

C. Client Application Process

D. Source Domain

E. URL Category

Correct Answer: BCE

The GlobalProtect Gateway supports three methods for split tunneling23:

Access Route -- You can define a list of IP addresses or subnets that are accessible through the VPN tunnel. All other traffic goes directly to the internet. Domain and Application -- You can define a list of domains or applications that are

accessible through the VPN tunnel. All other traffic goes directly to the internet. You can also use this method to exclude specific domains or applications from the VPN tunnel. Video Traffic -- You can exclude video streaming traffic from the

VPN tunnel based on predefined categories or custom URLs. This method reduces latency and jitter for video streaming applications.