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

An engineer is tasked with deploying SSL Forward Proxy decryption for their organization.

What should they review with their leadership before implementation?

A. Browser-supported cipher documentation

B. Cipher documentation supported by the endpoint operating system

C. URL risk-based category distinctions

D. Legal compliance regulations and acceptable usage policies

Correct Answer: D

The engineer should review the legal compliance regulations and acceptable usage policies with their leadership before implementing SSL Forward Proxy decryption for their organization. SSL Forward Proxy decryption allows the firewall to decrypt and inspect the traffic from internal users to external servers. This can raise privacy and legal concerns for the users and the organization. Therefore, the engineer should ensure that the leadership is aware of the implications and benefits of SSL Forward Proxy decryption and that they have a clear policy for informing and obtaining consent from the users. Option A is incorrect because browser-supported cipher documentation is not relevant for SSL Forward Proxy decryption. The firewall uses its own cipher suite to negotiate encryption with the external server, regardless of the browser settings. Option B is incorrect because cipher documentation supported by the endpoint operating system is not relevant for SSL Forward Proxy decryption. The firewall uses its own cipher suite to negotiate encryption with the external server, regardless of the endpoint operating system. Option C is incorrect because URL risk-based category distinctions are not relevant for SSL Forward Proxy decryption. The firewall can decrypt and inspect traffic based on any URL category, not just risk-based ones.

QUESTION 2

Which three authentication types can be used to authenticate users? (Choose three.)

A. Local database authentication

B. PingID

C. Kerberos single sign-on

D. GlobalProtect client

E. Cloud authentication service

Correct Answer: ACE

The three authentication types that can be used to authenticate users are:

A: Local database authentication. This is the authentication type that uses the local user database on the firewall or Panorama to store and verify user credentials1.

C: Cloud authentication service. This is the authentication type that uses a cloud- based identity provider, such as Okta, PingOne, or PingFederate, to authenticate users and provide SAML assertions to the firewall or Panorama2.

E: Kerberos single sign-on. This is the authentication type that uses the Kerberos protocol to authenticate users who are logged in to a Windows domain and provide them with seamless access to resources on the firewall or Panorama3.

QUESTION 3

In a security-first network, what is the recommended threshold value for apps and threats to be dynamically updated?

A. 1 to 4 hours

B. 6 to 12 hours

C. 24 hours

D. 36 hours

Correct Answer: B

Schedule content updates so that they download-and-install automatically. Then, set a Threshold that determines the amount of time the firewall waits before installing the latest content. In a security-first network, schedule a six to twelve hour threshold.

https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-upgrade/software-and-content-updates/best-practices-for-app-and-threat-content-updates/best-practices-security-first

QUESTION 4

An administrator device-group commit push is tailing due to a new URL category How should the administrator correct this issue?

A. verify that the URL seed Tile has been downloaded and activated on the firewall

B. change the new category action to alert" and push the configuration again

C. update the Firewall Apps and Threat version to match the version of Panorama

D. ensure that the firewall can communicate with the URL cloud

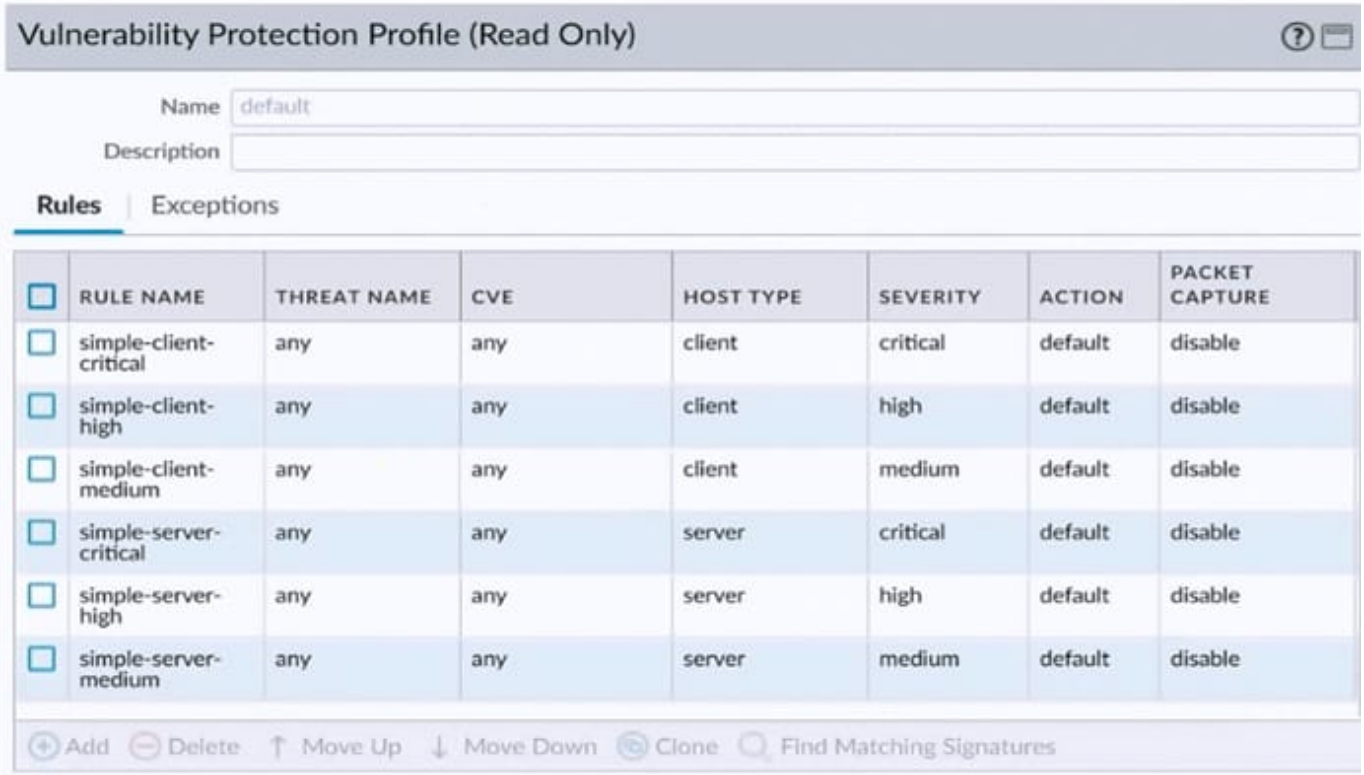
Correct Answer: C

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNqw

QUESTION 5

An administrator would like to determine which action the firewall will take for a specific CVE.

Given the screenshot below, where should the administrator navigate to view this information?


Vulnerability Protection Profile (Read Only)

Name default

Description

Rules | Exceptions

RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
simple-client-critical	any	any	client	critical	default	disable
simple-client-high	any	any	client	high	default	disable
simple-client-medium	any	any	client	medium	default	disable
simple-server-critical	any	any	server	critical	default	disable
simple-server-high	any	any	server	high	default	disable
simple-server-medium	any	any	server	medium	default	disable

Add Delete Move Up Move Down Clone Find Matching Signatures

A. The profile rule action

B. CVE column

C. Exceptions tab

D. The profile rule threat name

Correct Answer: C

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClMnCAK