PCNSA Q&As

Palo Alto Networks Certified Network Security Administrator

Pass Palo Alto Networks PCNSA Exam with 100% Guarantee

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

https://www.certbus.com/pcnsa.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 service protects cloud-based applications such as Dropbox and Salesforce by administering permissions and scanning files for sensitive information?

A. Aperture

B. AutoFocus

C. Parisma SaaS

D. GlobalProtect

Correct Answer: C

QUESTION 2

How would a Security policy need to be written to allow outbound traffic using Secure Shell (SSH) to destination ports tcp/22 and tcp/4422?

A. The admin creates a custom service object named "tcp-4422" with port tcp/4422. The admin then creates a Security policy allowing application "ssh" and service "tcp-4422".

B. The admin creates a custom service object named "tcp-4422" with port tcp/4422. The admin then creates a Security policy allowing application "ssh", service "tcp-4422", and service "application-default".

C. The admin creates a custom service object named "tcp-4422" with port tcp/4422. The admin also creates a custom service object named "tcp-22" with port tcp/22. The admin then creates a Security policy allowing application "ssh", service "tcp-4422", and service "tcp-22".

D. The admin creates a Security policy allowing application "ssh" and service "application-default".

Correct Answer: C

QUESTION 3

Your company requires positive username attribution of every IP address used by wireless devices to support a new compliance requirement. You must collect IP-to-user mappings as soon as possible with minimal downtime and minimal configuration changes to the wireless devices themselves. The wireless devices are from various manufactures.

Given the scenario, choose the option for sending IP-to-user mappings to the NGFW.

A. syslog

B. RADIUS

C. UID redistribution

D. XFF headers

Correct Answer: A

QUESTION 4

Selecting the option to revert firewall changes will replace what settings?

A. the running configuration with settings from the candidate configuration

B. the device state with settings from another configuration

C. the candidate configuration with settings from the running configuration

D. dynamic update scheduler settings

Correct Answer: C

QUESTION 5

An administrator is troubleshooting an issue with traffic that matches the intrazone-default rule, which is set to default configuration.

What should the administrator do?

A. change the logging action on the rule

B. review the System Log

C. refresh the Traffic Log

D. tune your Traffic Log filter to include the dates

Correct Answer: A

QUESTION 6

What is the purpose of the automated commit recovery feature?

A. It reverts the Panorama configuration.

B. It causes HA synchronization to occur automatically between the HA peers after a push from Panorama.

C. It reverts the firewall configuration if the firewall recognizes a loss of connectivity to Panorama after the change.

D. It generates a config log after the Panorama configuration successfully reverts to the last running configuration.

Correct Answer: C

Reference:https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/administer- panorama/enable-automated-commit-recovery.html

QUESTION 7

Which User-ID mapping method should be used for an environment with clients that do not authenticate to Windows Active Directory?

A. Windows session monitoring via a domain controller

B. passive server monitoring using the Windows-based agent

C. Captive Portal

D. passive server monitoring using a PAN-OS integrated User-ID agent

Correct Answer: C

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip- addresses-to-users/map-ip-addresses-to-usernames-using-captive-portal.html

QUESTION 8

The administrator profile "SYS01 Admin" is configured with authentication profile "Authentication Sequence SYS01," and the authentication sequence SYS01 has a profile list with four authentication profiles:

Auth Profile LDAP Auth Profile Radius Auth Profile Local Auth Profile TACACS

After a network outage, the LDAP server is no longer reachable. The RADIUS server is still reachable but has lost the "SYS01 Admin" username and password.

What is the "SYS01 Admin" login capability after the outage?

A. Auth KO because RADIUS server lost user and password for SYS01 Admin

B. Auth OK because of the Auth Profile TACACS

C. Auth OK because of the Auth Profile Local

D. Auth KO because LDAP server is not reachable

Correct Answer: C

Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMdXCAW

QUESTION 9

Which User Credential Detection method should be applied within a URL Filtering Security profile to check for the submission of a valid corporate username and the associated password?

A. Domain Credential

B. IP User

C. Group Mapping

D. Valid Username Detected Log Severity

Correct Answer: C

QUESTION 10

Which Security profile must be added to Security policies to enable DNS Signatures to be checked?

A. Anti-Spyware

B. Antivirus

C. Vulnerability Protection

D. URL Filtering

Correct Answer: A

"In addition, you can enable the DNS sinkholing action in Anti-Spyware profiles to enable the firewall to forge a response to a DNS query for a known malicious domain, causing the malicious domain name to resolve to an IP address that you define" https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/policy/security-profiles

QUESTION 11

During the packet flow process, which two processes are performed in application identification? (Choose two.)

A. pattern based application identification

B. application override policy match

C. session application identified

D. application changed from content inspection

Correct Answer: AB

Reference: http://live.paloaltonetworks.com//t5/image/serverpage/image- id/12862i950F549C7D4E6309

QUESTION 12

With the PAN-OS 11.0 release, which tab becomes newly available within the Vulnerability security profile?

A. Vulnerability Exceptions

B. Advanced Rules

C. Inline Cloud Analysis

D. WildFire Inline ML

Correct Answer: C

QUESTION 13

According to best practices, how frequently should WildFire updates he made to perimeter firewalls?

A. every 10 minutes

B. every minute

C. every 5 minutes

D. in real time

Correct Answer: D

https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-deployment-best-practices/wildfire-best-practicesIf you are running PAN-OS 10.0 or later, configure your firewall to retrieve WildFire signatures in real-time. This provides access to newly-discovered malware signatures as soon as the WildFire public cloud can generate them, thereby preventing successful attacks by minimizing your exposure time to malicious activity.

QUESTION 14

An administrator is reviewing the Security policy rules shown in the screenshot. Why are the two fields in the Security policy EDL-Deny highlighted in red?

A. Because antivirus inspection is enabled for this policy

B. Because the destination zone, address, and device are all "any"

C. Because the action is Deny

D. Because the Security-EDL tag has been assigned the red color

Correct Answer: D

QUESTION 15

Which path is used to save and load a configuration with a Palo Alto Networks firewall?

A. Device>Setup>Services

B. Device>Setup>Management

C. Device>Setup>Operations

D. Device>Setup>Interfaces

Correct Answer: C