PALO ALTO PCNSE

Palo Alto PCNSE PAN-OS 10 Certification Questions & Answers

Exam Summary – Syllabus – Questions

PCNSE

Palo Alto Networks Certified Network Security Engineer

75 Questions Exam – Variable (70-80 / 100 Approx.) Cut Score – Duration of 80 minutes

Table of Contents:

Know Your PCNSE Certification Well:

The PCNSE is best suitable for candidates who want to gain knowledge in the Palo Alto Network Security. Before you start your PCNSE preparation you may struggle to get all the crucial PCNSE PAN-OS 10 materials like PCNSE syllabus, sample questions, study guide.

But don't worry the PCNSE PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the PCNSE syllabus?
- How many questions are there in the PCNSE exam?
- Which Practice test would help me to pass the PCNSE exam at the first attempt?

Passing the PCNSE exam makes you Palo Alto Networks Certified Network Security Engineer. Having the PCNSE PAN-OS 10 certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Palo Alto PCNSE PAN-OS 10 Certification Details:

Exam Name	Network Security Engineer
Exam Code	PCNSE
Exam Price	$175 USD
Duration	80 minutes
Number of Questions	75
Passing Score	Variable (70-80 / 100 Approx.)
Recommended Training	**Firewall Essentials - Configuration and Management (EDU-210)** **Panorama - Managing Firewalls at Scale (EDU-220)** **Firewall - Troubleshooting (330)** **Firewall 10.0 - Optimizing Firewall Threat Prevention (EDU-214)**
Exam Registration	**PEARSON VUE**
Sample Questions	**Palo Alto PCNSE Sample Questions**
Practice Exam	**Palo Alto Networks Certified Network Security Engineer Practice Test**

PCNSE Syllabus:

Section	Weight	Objectives
Plan	16%	- Identify how the Palo Alto Networks products work together to detect and prevent threats - Given a scenario, identify how to design an implementation of the firewall to meet business requirements that leverage the Palo Alto Networks product portfolio - Given a scenario, identify how to design an implementation of firewalls in High Availability to meet business requirements that leverage the Palo Alto Networks product portfolio - Identify the appropriate interface type and configuration for a specified network deployment - Identify strategies for retaining logs using Distributed Log Collection - Given a scenario, identify the strategy that should be implemented for Distributed Log Collection - Identify how to use template stacks for administering Palo Alto Networks firewalls as a scalable solution using Panorama - Identify how to use device group hierarchy for administering Palo Alto Networks firewalls as a scalable solution using Panorama - Identify planning considerations unique to deploying Palo Alto Networks firewalls in a public cloud - Identify planning considerations unique to deploying Palo Alto Networks firewalls in a hybrid cloud - Identify planning considerations unique to deploying Palo Alto Networks firewalls in a private cloud - Identify methods for authorization, authentication, and device administration - Identify the methods of certificate creation on the firewall - Identify options available in the firewall to support dynamic routing - Given a scenario, identify ways to mitigate resource exhaustion (because of denial-of-service) in application servers - Identify decryption deployment strategies - Identify the impact of application override to the overall functionality of the firewall - Identify the methods of User-ID redistribution - Identify VM-Series bootstrap components and their function
Deploy and Configure	23%	- Identify the application meanings in the Traffic log (incomplete, insufficient data, non-syn TCP, not applicable, unknown TCP, unknown UDP, and unknown P2P)

Section	Weight	Objectives
		- Given a scenario, identify the set of Security Profiles that should be used - Identify the relationship between URL filtering and credential theft prevention - Implement and maintain the App-ID adoption - Identify how to create security rules to implement App-ID without relying on port-based rules - Identify configurations for distributed Log Collectors - Identify the required settings and steps necessary to provision and deploy a next-generation firewall - Identify which device of an HA pair is the active partner - Identify various methods for authentication, authorization, and device administration within PAN-OS software for connecting to the firewall - Identify how to configure and maintain certificates to support firewall features - Identify the features that support IPv6 - Identify how to configure a virtual router - Given a scenario, identify how to configure an interface as a DHCP relay agent - Identify the configuration settings for site-to-site VPN - Identify the configuration settings for GlobalProtect - Identify how to configure features of NAT policy rules - Given a configuration example including DNAT, identify how to configure security rules - Identify how to configure decryption - Given a scenario, identify an application override configuration and use case - Identify how to configure VM-Series firewalls for deployment - Identify how to configure firewalls to use tags and filtered log forwarding for integration with network automation
Operate	20%	- Identify considerations for configuring external log forwarding - Interpret log files, reports, and graphs to determine traffic and threat trends - Identify scenarios in which there is a benefit from using custom signatures - Given a scenario, identify the process to update a Palo Alto Networks system to the latest version of the software - Identify how configuration management operations are used to ensure desired operational state of stability and continuity - Identify the settings related to critical HA functions (link monitoring; path monitoring; HA1, HA2, HA3, and HA4 functionality; HA backup links; and differences between A/A

Section	Weight	Objectives
		and A/P HA pairs and HA clusters) - Identify the sources of information that pertain to HA functionality - Identify how to configure the firewall to integrate with AutoFocus and verify its functionality - Identify the impact of deploying dynamic updates - Identify the relationship between Panorama and devices as pertaining to dynamic updates versions and policy implementation and/or HA peers
Configuration Troubleshooting	18%	- Identify system and traffic issues using the web interface and CLI tools - Given a session output, identify the configuration requirements used to perform a packet capture - Given a scenario, identify how to troubleshoot and configure interface components - Identify how to troubleshoot SSL decryption failures - Identify issues with the certificate chain of trust - Given a scenario, identify how to troubleshoot traffic routing issues
Core Concepts	23%	- Identify the correct order of the policy evaluation based on the packet flow architecture - Given an attack scenario against firewall resources, identify the appropriate Palo Alto Networks threat prevention component to prevent or mitigate the attack - Given an attack scenario against resources behind the firewall, identify the appropriate Palo Alto Networks threat prevention component to prevent or mitigate the attack - Identify methods for identifying users - Identify the fundamental functions residing on the management plane and data plane of a Palo Alto Networks firewall - Given a scenario, determine how to control bandwidth use on a per-application basis - Identify the fundamental functions and concepts of WildFire - Identify the purpose of and use case for MFA and the Authentication policy - Identify the dependencies for implementing MFA - Given a scenario, identify how to forward traffic - Given a scenario, identify how to configure policies and related objects - Identify the methods for automating the configuration of a firewall

Palo Alto PCNSE Sample Questions:

Question: 1

The Palo Alto Networks Cortex Data Lake can accept logging data from which two products?

(Choose two.)

a) Cortex XDR
b) next-generation firewalls
c) Prisma SaaS
d) MineMeld
e) AutoFocus

Answer: a, b

Question: 2

Which profile do you use for DLP based on file content?

a) Antivirus
b) Anti-Spyware
c) Vulnerability Protection
d) URL Filtering
e) File Blocking
f) WildFire Analysis
g) Data Filtering

Answer: g

Question: 3

You are preparing a bootstrap template for use with a VM-Series firewall hosted in a public cloud. You don’t need to include the Content-ID files because the firewall will download the latest version when it is booted anyway.

How do you configure the bootstrap’s content directory?

a) leave it empty
b) delete it
c) rename it to content-null
d) add an empty file to it named no-download

Answer: a

Question: 4

How does the NGFW handle excess packets when there are QoS constraints?

a) It buffers them until there is bandwidth to send them.
b) It drops a percentage of them randomly.
c) It replaces them with packets that tell the computer on the other side to slow down.
d) It sends a portion instead of the whole packet.

Answer: b

Question: 5

In a Panorama managed environment, which two options show the correct order of policy evaluation?

(Choose two.)

a) device group pre-rules, shared pre-rules, local firewall rules, intrazone-default, interzone-default
b) device group pre-rules, local firewall rules, shared post-rules, device group post-rules, intrazone-default, interzone-default
c) device group pre-rules, local firewall rules, device group post-rules, shared post-rules, intrazone-default, interzone-default
d) device group pre-rules, local firewall rules, intrazone-default, interzone-default, device group post-rules, shared post-rules
e) shared pre-rules, device group pre-rules, local firewall rules, intrazone-default, interzone-default

Answer: c, e

Question: 6

Under which conditions can two Layer 3 interfaces have the same IP address?

a) They must be connected to a common VLAN object interface.
b) They must be connected to the same Ethernet network through a switch. This configuration can be used only for High Availability.
c) They must be connected to different virtual routers.
d) They must be subinterfaces of the same physical interface.
e) This feature is not supported.

Answer: e

Question: 7

On a PA-7000 Series firewall, which management function runs on a separate, dedicated card?

a) configuration management
b) logging
c) reporting
d) management web service

Answer: b

Question: 8

A Security policy accepts new FTP traffic sessions between 8:00 a.m. and 5:00 p.m. What happens to an already-accepted and running FTP session at 5:01 p.m.?

a) The session is re-evaluated to determine whether it is allowed under a different policy rule.
b) The session continues to run, because already accepted sessions are not re-evaluated.
c) The session is re-evaluated if the default configuration setting “Rematch all sessions on config policy change” is enabled.
d) The session is terminated, and the initiator must establish a new session.

Answer: b

Question: 9

Palo Alto Networks publishes new applications at which approximate interval?

a) every 30 minutes
b) hourly
c) daily
d) weekly

Answer: d

Question: 10

Which Captive Portal authentication method can be handled by the browser without affecting the user experience?

a) web-challenge
b) browser-challenge
c) web-form
d) browser-form

Answer: b

Study Guide to Crack Palo Alto PCNSE PAN-OS 10 PCNSE Exam:

- Getting details of the PCNSE syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the PCNSE exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Palo Alto provided training for PCNSE exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the PCNSE sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on PCNSE practice tests is must. Continuous practice will make you an expert in all syllabus areas.