



PCNSE

Palo Alto Networks Certified Network Security Engineer

NWExam.com

SUCCESS GUIDE TO PALO ALTO CERTIFICATION
Exam Summary – Syllabus – Questions

Table of Contents

Introduction to PCNSE Exam on Palo Alto Networks Certified Network Security Engineer	2
 Palo Alto PCNSE Certification Details:.....	2
 Palo Alto PCNSE Exam Syllabus:.....	3
 PCNSE Sample Questions:	5
 Answers to PCNSEExam Questions:.....	7

Introduction to PCNSE Exam on Palo Alto Networks Certified Network Security Engineer

A great way to start the Palo Alto Networks Certified Network Security Engineer (PCNSE PAN-OS 8) preparation is to begin by properly appreciating the role that syllabus and study guide play in the Palo Alto PCNSE certification exam. This study guide is an instrument to get you on the same page with Palo Alto and understand the nature of the Palo Alto PCNSE exam.

Our team of experts has composed this Palo Alto PCNSE exam preparation guide to provide the overview about Palo Alto Network Security Engineer exam, study material, sample questions, practice exam and ways to interpret the exam objectives to help you assess your readiness for the Palo Alto PCNSE PAN-OS 8 exam by identifying prerequisite areas of knowledge. We recommend you to refer the simulation questions and practice test listed in this guide to determine what type of questions will be asked and the level of difficulty that could be tested in the Palo Alto PCNSE certification exam.

Palo Alto PCNSE Certification Details:

Exam Name	Network Security Engineer
Exam Number	PCNSE PCNSE PAN-OS 8
Exam Price	\$160 USD
Duration	90 minutes
Number of Questions	75
Passing Score	70%
Recommended Training	Firewall Essentials 8.0: Configuration and Management (EDU-210) Panorama 8.0: Manage Multiple Firewalls (EDU-221) Firewall 8.0: Debug and Troubleshoot (EDU-311)
Exam Registration	PEARSON VUE
Sample Questions	Palo Alto PCNSE Sample Questions
Practice Exam	Palo Alto Networks Certified Network Security Engineer Practice Test

Palo Alto PCNSE Exam Syllabus:

Section	Weight	Objectives
Plan	16%	<ul style="list-style-type: none"> - 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 leveraging the Palo Alto Networks Security Platform. - Given a scenario, identify how to design an implementation of firewalls in High Availability to meet business requirements leveraging the Palo Alto Networks Security Platform - Identify the appropriate interface type and configuration for a specified network deployment - 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 options to deploy Palo Alto Networks firewalls in a private cloud (VM-Series). - Identify methods for authorization, authentication, and device administration. - 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.

Section	Weight	Objectives
Deploy and Configure	23%	<ul style="list-style-type: none"> - Identify the application meanings in the Traffic log (incomplete, insufficient data, non-syn TCP, not applicable, unknown TCP, unknown UDP, and unknown P2P). - Given a scenario, identify the set of Security Profiles that should be used. - Identify the relationship between URL filtering and credential theft prevention. - Identify differences between services and applications. - Identify how to create security rules to implement App-ID without relying on port-based rules. - Identify the required settings and steps necessary to provision and deploy a next-generation firewall. - Identify various methods for Authentication, Authorization, and Device Administration within a firewall. - Identify how to configure and maintain certificates to support firewall features. - Identify how to configure a virtual router. - Identify the configuration settings for site-to-site VPN. - Identify the configuration settings for GlobalProtect. - Identify how to configure items pertaining to denial-of-service protection and zone protection. - Identify how to configure features of the NAT rulebase. - 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.
Operate	20%	<ul style="list-style-type: none"> - 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, and HA3 functionality; HA backup links; and differences between A/A and A/P). - Identify the sources of information pertaining to HA functionality.

Section	Weight	Objectives
		<ul style="list-style-type: none"> - 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 it pertains to dynamic updates versions and policy implementation and/or HA peers.
Configuration Troubleshooting	18%	<ul style="list-style-type: none"> - Identify system and traffic issues using WebUI 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 certificate chain of trust issues. - Given a scenario, identify how to troubleshoot traffic routing issues.
Core Concepts	23%	<ul style="list-style-type: none"> - Identify the correct order of the policy evaluation based on the packet flow architecture. - Given an attack scenario, identify the Palo Alto Networks appropriate threat prevention component to prevent/mitigate the attack. - Identify methods for identifying users. - Identify the fundamental functions residing on the management and dataplanes 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 traffi. - Given a scenario, identify how to configure policies and related objects. - Identify the methods for automating the configuration of a firewall.

PCNSE Sample Questions:

01. The Management network port on a firewall can be configured as which type of interface?

- a) Layer 2
- b) Layer 3
- c) Virtual wire
- d) Serial

02. Which two Palo Alto Networks firewall models support active/active High Availability?

(Choose two.)

- a) PA-200
- b) VM-300
- c) PA-7050
- d) PA-3020
- e) VM-200

03. Which three statements are true about Palo Alto Networks Next-Generation Firewalls?

(Choose three.)

- a) The Single Pass Architecture design includes an industry-leading content scanning engine available as a software or hardware option.
- b) Palo Alto Networks firewalls are part of a Security Platform that includes integration with a Threat Intelligence Cloud.
- c) The App-ID next-generation feature of the firewall will accurately identify the responsible application generating all traffic passing through the firewall.
- d) Palo Alto Networks firewalls natively support encrypted connections with IPSec and SSL encryption technologies.

04. Complete the following statement: Packet captures can be performed by:

(choose three)

- a) Security profiles
- b) manual configuration by an administrator in the WebUI
- c) manual configuration on the CLI
- d) specified trigger events from the WebUI

05. What are three advantages of the Palo Alto Networks Next-Generation Firewall?

(Choose three.)

- a) Application-based rather than port-based traffic recognition for better rules and granularity
- b) Ports can now be safely ignored because they are no longer a factor
- c) Uses a stream-based, single-pass parallel processing engine for fast performance
- d) Application signatures are distributed regularly from Palo Alto Networks, although custom signatures cannot be created
- e) Provides full Unified Threat Management on a single platform with one policy and log database

06. In a new firewall, which port provides WebUI access by default?

- a) Traffic port #1
- b) Any Traffic port
- c) Management port
- d) Console port
- e) Maintenance port

07. Which statement is not true about User-ID?

- a) User-ID is collected by an endpoint agent.
- b) User-ID monitors Domain Controllers for authentication.

- c) User-ID tasks can be shared among multiple firewalls.
- d) User-ID collects LDAP group membership data for users.

08. Firewall configuration files can :

(choose two)

- a) Be captured at any time and stored on the firewall
- b) Restored to the running configuration
- c) Transferred out of the firewall
- d) Shared between firewalls

09. Which two types of encryptions can a Palo Alto Networks firewall decrypt through decryption policies?

(Choose two.)

- a) SSL
- b) Blowfish
- c) AES
- d) SSH
- e) 3DES

10. The configuration of a DoS Protection profile can defend nodes from which attacks?

- a) Floods
- b) TCP port scans
- c) IP address spoofing
- d) ICMP large packets

Answers to PCNSE Exam Questions:

Question: 01	Question: 02	Question: 03	Question: 04	Question: 05
Answer: b	Answer: c, d	Answer: b, c, d	Answer: a, b, c	Answer: a, c, e
Question: 06	Question: 07	Question: 08	Question: 09	Question: 10
Answer: c	Answer: a	Answer: a, c	Answer: a, b	Answer: a

Note: If you find any typo or data entry error in these sample questions, we request you to update us by commenting on this page or write an email on feedback@nwexam.com