Relesae
June 6, 2016

PCNSE7
Palo Alto Networks Network Security Engineer on PAN OS7

Education Services
E-Mail: mtuite@paloaltonetworks.com

Overview

The Palo Alto Networks Certified Network Security Engineer (PCNSE) is a formal, third-party proctored certification that indicates those who have passed it possess the in-depth knowledge to design, install, configure, maintain and troubleshoot the vast majority of implementations based on the Palo Alto Networks platform. The PCNSE exam should be taken by anyone who wishes to demonstrate a deep understanding of Palo Alto Networks technologies, including customers who use Palo Alto Networks products, value-added resellers, pre-sales system engineers, system integrators, and support staff.

Exam Details

- **Certification Name**: Palo Alto Networks Certified Network Security Engineer on PAN OS7
- **Delivered through Pearson VUE**: www.pearsonvue.com/paloaltonetworks
- **Exam Series**: PCNSE7
- **Seat Time:** 90 minutes/120 minutes ESL
- **# of items**: 60
- **Format**: Multiple Choice, Scenarios with Graphics, and Matching
- **Language**: English

Intended Audience

This exam will certify that the successful candidate has the knowledge and skills necessary to implement Palo Alto Networks security platform V7 in any environment and understands the next generation security platform. This exam will **NOT** cover Aperture, Traps and AutoFocus

Qualifications

Experience:

Three to five years working in the Networking or Security industries.
The equivalence of 6 months' experience working full-time with Palo Alto Networks security platform.

Skills Required

- Candidate can plan, deploy, configure and troubleshoot Palo Alto Networks Security platform components
- Candidate has product expertise and understands the unique aspects of the next generation security platform and how to deploy one appropriately.
- Candidate understands Palo Alto networking and security policies

Recommended Training

Palo Alto Networks strongly recommends, you attending our Firewall: Install Configure and Manage (201), Firewall: Configure Extended Features (205), and Panorama: Manage Multiple Firewalls (221), Firewall: Manage Cyber threats (231) and Firewall: Debug and Troubleshoot (311) classes. Courses do not cover everything that a PCNSE7 needs to know, but they're the most efficient way to start learning. When you have the basics mastered, you should spend time on our platform practicing using the information in the 7.0 versions of the Administrator's Guides.

Blueprint Objectives:

Objectives summarize what the test is designed to measure. Objectives are developed by Exam Developers and Subject Matter Experts based on identified tasks that relate that the successful candidate has the knowledge and skills necessary to implement Palo Alto Networks Next Generation Firewall platform in any environment and understands the next generation security platform. Once the initial development process is complete, these objectives are verified using an external group of individuals in the actual job role. The external survey determines the number of questions for each objective, which relates directly to the criticality of the task in the job role.

Prior to taking this exam, candidates should understand each of the following objectives. Each objective is listed below; along with related tools the candidate should have experience with, and related documentation that contains information relevant to the objective. All objectives may also be referenced in other product documentation not specifically highlighted below. The candidate should be familiar with all relevant product documentation or have an equivalent skillset.

Architecture and Design

- Identify how Palo Alto Networks products work together to detect and prevent threats.
- Given a scenario, architect a solution to meet the business requirements leveraging the security platform.
- Evaluate high availability (HA) designs and configurations for various deployments.
- Identify the appropriate interface type and configuration for a specified network deployment.
- Identify strategies for retaining logs using Distributed Log Collection.
- Identify how to design a scalable solution for administering Palo Alto Devices using Panorama.
- Identify deployment strategies for virtualized environments.

Resources:

- *Firewall: Install, Configure and Manage (201) Course* for PAN OS7 https://www.paloaltonetworks.com/services/education
- *Firewall: Configure, Extended Features (205)* for PAN OS7 https://www.paloaltonetworks.com/services/education
- Global Protect Admin Guide (query on objectives above)
- https://live.paloaltonetworks.com/docs/ as examples the following are relevant
    - Doc 2541, 1517, 2561 and others

Core Concepts

- Identify the key features of a next generation Layer 7 firewall and its advantages over a traditional firewall.
- 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.
- Identify methods for mapping users to IP addresses and troubleshoot related issues.
- Identify the fundamental functions residing on the management and data planes of a Palo Alto Networks firewall.
- Given a scenario, determine how to control bandwidth utilization on a per application basis.
- Identify the fundamental functions and concepts of WildFire.

Resources:

- *Firewall: Install, Configure and Manage(201) Course* for PAN OS7 https://www.paloaltonetworks.com/services/education
- *Firewall: Configure, Extended Features (205)* for PAN OS7 https://www.paloaltonetworks.com/services/education
- Global Protect Admin Guide (query on objectives above)
- PAN OS 6.0 Admin Guide
- PAN OS 7.0 Admin Guide

Logs and Stats

- Identify considerations for configuring external log forwarding.
- Interpret log files, reports, and graphs to determine traffic and threat trends.
- Identify system and traffic issues utilizing Web UI and CLI tools.
- Given a session output, identify the configuration requirements used to perform a packet capture.
- Given a scenario including an Application Command Center (ACC) output, identify trends and troubleshoot issues
- Identify configurations for distributed log collections and verify functionality.

Resources:

- PAN OS 6.0 Admin Guide
- PAN OS 7.0 Admin Guide
- PAN-OS Command line reference guide
- New Features Guide, PAN-OS 6.1
- Panorama Admin Guide 7.0

Management

- Identify the required settings and steps necessary to provision and deploy a Next-Generation Firewall.
- Determine how to leverage Panorama to centrally manage device configurations and logs.
- Given a scenario, explain the process to update a Palo Alto Networks system to the latest version of code or content.
- Identify how configuration management operations are used to ensure desired operational state of stability and continuity.
- Identify methods for Authorization, Authentication, and Device Administration.
- Identify the proper use of Public Key Infrastructure components.

Resources:

- Getting Started Guide 6.0
- Firewall Inline Guide
- https://www.paloaltonetworks.com/documentation/70/pan-os/newfeaturesguide/management-features/review-new-app-ids.html
- Palo Alto Networks Quick Start Guide v6.0
- GlobalProtect Admin Guide 6.0

Networking

- Given a scenario, determine how to configure and troubleshoot interface components.
- Identify the configurations settings that are required to enable IPv6 features.
- Given a scenario, configure and troubleshoot Routing.
- Identify the configuration settings for site-to-site VPN.
- Identify the configuration settings for SSL/remote access VPN.
- Identify ways to mitigate resource exhaustion (due to denial of service) in application servers.

Resources:

- Firewall InLine Help
- Global Protect Admin Guide 6.0
- Palo Alto Whitepapers/Tech Notes

Policies and Procedures

- Identify the deployment, configuration, and management features of the security rule-base.
- Identify the deployment, configuration and management of security profiles and options.
- Identify the deployment, configuration, and management features of the NAT rule-base.
- Identify decryption deployment strategies.
- Given a scenario, identify application override configuration and use.

Resources:

- *Firewall: Install, Configure and Manage(201) Course* for PAN OS7 https://www.paloaltonetworks.com/services/education
- *Firewall: Configure, Extended Features (205)* for PAN OS7 https://www.paloaltonetworks.com/services/education
- *Panorama: Manage Multiple Firewalls (221) Course*
- https://www.paloaltonetworks.com/services/education
- PAN-OS 6.0 and 7.0 Admin Guide
- Firewall InLine Help
- Panorama Admin Guide 7.0

[1]

Disclaimer:
This blueprint is intended to provide information about the objectives covered by this exam, related resources, and recommended courses. The material contained within this blueprint is not intended to guarantee that a passing score will be achieved on the exam. Palo Alto Networks recommends that a candidate thoroughly understands the objectives indicated in this guide and utilizes the resources and courses recommended in this guide where needed to gain that understanding.