

Palo Alto Networks Network Security Professional

Datasheet

AUGUST 2025

The Palo Alto Networks Certified Network Security Professional certification is designed to validate a candidate's understanding of all products and services included in the Palo Alto Networks network security solution, their use cases, and how they are applicable to an organization. The Network Security Professional exam also validates a candidate's ability to use, maintain, and configure network security products at an entry level, and to perform basic network security product installation and deployment.

The purpose of this document is to help you prepare for the exam and attain the certification. Please note that this document is intended to help identify the topics covered and to provide resources and references for understanding those topics. It is not intended to be used as the sole document to prepare for the Network Security Professional exam.

Exam Details:

- Duration: 90 minutes
- Format: Multiple-choice questions
- Language: English
- Cost: \$200 USD*
- Delivered by Pearson Vue

** Price may vary by country*

Audience and Qualifications

Target Audience

This exam is designed for individuals with the following job roles:

- Networking and Security professionals responsible for installing / deploying, operating, or administering the Palo Alto Networks suite of:
 - Next-generation firewall (NGFW) products
 - Cloud-Delivered Security Services (CDSS) subscriptions
 - Secure Access Service Edge (SASE) products, including Prisma Access, Enterprise Browser, and Prisma SD-WAN
 - Management products, including Strata Cloud Manager (SCM)
- Individuals responsible for establishing and maintaining the connectivity and security of:
 - Data centers (i.e., on-premises, public cloud, private cloud)
 - Branches and campuses
 - Remote users (i.e., client-based, proxy-based, Enterprise Browser, RBI)
 - Internet-connected devices (i.e., internet of things (IoT), internet of medical things (IoMT), operational technology)
 - Data handling (i.e., SaaS applications, data loss prevention (DLP), cloud access)

Skills Required

The successful candidate can demonstrate understanding of NetSec processes and procedures

- Basic knowledge of securing networks of all sizes
- Configuration of Palo Alto Networks Strata and Prisma SASE products for security outcomes
- Basic knowledge of options for managing Palo Alto Networks solutions (e.g., Panorama, SCM)
- Basic knowledge of configuring relevant Palo Alto Networks products (e.g., hardware, VM-Series firewalls, CN-Series firewalls, Cloud NGFWs, Prisma Access, Prisma SD-WAN, CDSS)
- Basic knowledge of best practices for Strata and SASE products

Blueprint

The blueprint table lists the domains covered and includes domain weighting. The percentage weights represent the portion of the exam score that is attributed to each domain. Many candidates find the table provides focus for studies during exam preparation. Also included in the blueprint table are the more specific tasks associated with each domain. Pay particular attention to these tasks, as they provide more targeted areas of study within the domains.

1. Network Security Fundamentals 16%

1.1 Explain Application Layer inspection for Strata and SASE products

1.2 Differentiate between slow path and fast path for packet inspection

1.3 Explain the use of decryption on Strata and SASE products

- 1.3.1 SSL Forward Proxy
- 1.3.2 SSL Inbound Inspection
- 1.3.3 SSH Proxy
- 1.3.4 No decrypt

1.4 Apply network hardening methods for enhanced security on Strata and SASE products

- 1.4.1 Content-ID
- 1.4.2 Zero Trust
- 1.4.3 User-ID (including Cloud Identity Engine) and Device-ID
- 1.4.4 Zones

2. NGFW and SASE Solution Functionality 18%

2.1 Explain the function of Cloud NGFWs, PA-Series, CN-Series, and VM-Series firewalls

- 2.1.1 Perimeter and core security
- 2.1.2 Zone security and segmentation
- 2.1.3 High availability (HA)
- 2.1.4 Security and NAT policy implementation
- 2.1.5 Monitoring and logging

2.2 Explain the function of Prisma SD-WAN

- 2.2.1 WAN optimization
- 2.2.2 Path and NAT policies
- 2.2.3 Zone-based firewall
- 2.2.4 Monitoring and logging

2.3 Explain the function of Prisma Access

- 2.3.1 Remote user configuration
- 2.3.2 Remote network configuration
- 2.3.3 Public and private application access
- 2.3.4 Security and NAT policy implementation
- 2.3.5 Monitoring and logging (Strata Logging Service)

2.4 Identify options for managing Strata and SASE solutions

- 2.4.1 Panorama
- 2.4.2 Strata Cloud Manager (SCM)

3. Platform Solutions, Services, and Tools 18%

3.1 Describe Palo Alto Networks NGFW and Prisma SASE products for security efficacy

- 3.1.1 Security and NAT policy creation
- 3.1.2 Cloud-Delivered Security Services (CDSS) configuration (security profiles)
- 3.1.3 User-ID and App-ID configuration
- 3.1.4 Decryption
- 3.1.5 Monitoring and logging

3.2 Explain the application of CDSS

- 3.2.1 Internet of things (IoT) security
- 3.2.2 Enterprise Data Loss Prevention (DLP)
- 3.2.3 SaaS Security
- 3.2.4 PAN-OS SD-WAN
- 3.2.5 Premium GlobalProtect
- 3.2.6 Advanced WildFire
- 3.2.7 Advanced Threat Prevention
- 3.2.8 Advanced URL Filtering
- 3.2.9 Advanced DNS

3.3 Explain aligning AIOps to Palo Alto Networks best practices

- 3.3.1 Administration of AIOps
- 3.3.2 Dashboards
- 3.3.3 Best Practice Assessment (BPA)

4. NGFW and SASE Solution Maintenance and Configuration 19%

4.1 Maintain and configure Palo Alto Networks hardware firewalls, VM-Series firewalls, CN-Series firewalls, and Cloud NGFWs

- 4.1.1 Security policies
- 4.1.2 Profiles
- 4.1.3 Updates
- 4.1.4 Upgrades

4.2 Add, configure, and maintain Prisma SD-WAN

- 4.2.1 Initial ION setup
- 4.2.2 Pathing
- 4.2.3 Monitoring and logging

4.3 Maintain and configure Prisma Access

- 4.3.1 Security policies
- 4.3.2 Profiles
- 4.3.3 Updates
- 4.3.4 Upgrades
- 4.3.5 Monitoring and logging

5. Infrastructure Management and CDSS 15%

5.1 Maintain and configure CDSS

- 5.1.1 Security policies
- 5.1.2 Profiles
- 5.1.3 Updates

5.2 Maintain and configure IoT security

- 5.2.1 Security policies
- 5.2.2 Device-IDs
- 5.2.3 Monitoring and logging

5.3 Maintain and configure Enterprise DLP and Enterprise SaaS Security

- 5.3.1 Data encryption
- 5.3.2 Access control
- 5.3.3 Monitoring and logging

5.4 Maintain and configure Strata Cloud Manager (SCM) and Panorama in network security environments

- 5.4.1 Supported products
- 5.4.2 New device addition
- 5.4.3 Reporting
- 5.4.4 Configuration management

6. Connectivity and Security 14%

6.1 Maintain and configure network security of on-premises, cloud, and hybrid networks

- 6.1.1 Network segmentation
- 6.1.2 Policies (security and network)
- 6.1.3 Monitoring and logging
- 6.1.4 Certificates

6.2 Maintain connectivity and security of remote users

- 6.2.1 Remote access solutions
- 6.2.2 Network segmentation
- 6.2.3 Security policy tuning
- 6.2.4 Monitoring and logging
- 6.2.5 Certificates

English as a Second Language (ESL) Accommodation

All exams are delivered worldwide in English. A 30-minute time extension is provided by default to candidates testing in non-English speaking countries.

Learning Resources

Learning Path

The complete Palo Alto Networks recommended learning path can be found [here](#).

Recommended Preparation

Palo Alto Networks certification exam items are developed and approved by exam development experts in conjunction with subject matter experts (SMEs) who represent a broad spectrum of roles relevant to each certification. Each item is referenced to a publicly available technical or scholarly source.

This datasheet provides the full blueprint to which the exam items are written. A solid foundation of the knowledge, skills, and abilities required to pass this certification exam can be achieved by researching keywords from each topic area included in the blueprint—either through the use of an AI-powered browser or directly within Palo Alto Networks documentation—and completing relevant coursework found in the learning path.



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.