

PALO ALTO

Palo Alto Networks Certified Network Security (PCNSE) Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

ADVANCED

40 HOURS

5 DAYS

NETWORK SECURITY

At a glance

COURSE	Palo Alto Networks Certified Network Security (PCNSE)
TRACK	Palo Alto
DOMAIN	Cyber Security
LEVEL	Advanced
DURATION	40 hours (about 5 days)
DELIVERY	Classroom · Online live · On-site at your office
LANGUAGE	English
CLASS SIZE	Small cohorts — everyone gets lab time

WHAT IS INCLUDED

- ✓ Instructor-led delivery by practitioners who also work our SOC
- ✓ Hands-on lab access for the duration of the course
- ✓ Course materials and lab guides
- ✓ Hacky Security certificate of completion
- ✓ Post-course support by email

Who this is for

This is an advanced course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

The PCNSE is retired. Palo Alto Networks withdrew the Certified Network Security Engineer exam on 31 July 2025 as part of a move from product-based certifications to role-based ones, and there is no direct successor exam. Existing PCNSE certificates remain valid for two years from the date they were awarded, but the exam can no longer be booked. The nearest current credential for the same job is the Palo Alto Networks Certified Next-Generation Firewall Engineer, whose blueprint is built on three areas rather than six: PAN-OS Networking Configuration at 40%, PAN-OS Device Setting Configuration at 40%, and Integration and Automation at 20%. If you want the certification rather than the syllabus, tell us at enrolment and we will place you on the NGFW Engineer map instead.

We keep this map because the PCNSE blueprint is still the best public description of what a Palo Alto firewall engineer is expected to know, and because a large number of estates are staffed by people who were trained against it. The six domains below are Palo Alto's own, in their published order, with their published weightings. Palo Alto's companion study guide was written against PAN-OS 11.0; the material below is taught on a current PAN-OS build, and we call out where behaviour has moved.

This is an engineering syllabus, not an introduction. Nearly a fifth of the blueprint is troubleshooting, and troubleshooting is the one thing that cannot be taught from slides. Every domain has lab time attached, on firewalls and a Panorama instance you are free to misconfigure.

Domain 01 — Core Concepts

The design decisions that everything later in the blueprint assumes you have already made correctly. 12% of the exam.

- How the Palo Alto product set fits together, and what each component contributes to PAN-OS services
- Interface and zone types — Layer 3, Layer 2, virtual wire, tap, aggregate, subinterface — and choosing the right one for a given insertion point
- Decryption deployment strategies, and the traffic, legal and performance reasons to exclude some of it
- Enforcing User-ID: where identity comes from, how it maps to an IP, and how long that mapping should be trusted
- Authentication policy, and the difference between authenticating a session and identifying a user
- Management plane against data plane, and which functions live on each
- Multiple virtual systems, and when a multi-vsys design beats separate firewalls
- Reading a design and predicting which of these choices will cause the first outage

Domain 02 — Deploy and Configure Core Components

The largest domain: the base build that a working firewall depends on. 20% of the exam.

- Management profiles, and restricting what each interface will answer
- Security profiles and profile groups: antivirus, anti-spyware, vulnerability protection, URL filtering, file blocking, WildFire analysis
- Zone protection, packet buffer protection and DoS protection, and the flood and reconnaissance cases each one covers
- Designing a deployment configuration for a given topology, including the interface and zone layout that follows from it

- Authentication, authorisation and device access for administrators, including role-based access and external authentication
- Certificate management: generating, importing, chaining, and the certificates decryption and portals depend on
- Routing configuration, including virtual routers, static routes and dynamic routing protocols
- NAT: source and destination, static and dynamic, and the relationship between the NAT rule and the security rule
- Site-to-site tunnels: IKE and IPSec profiles, tunnel interfaces, and proxy IDs
- Service routes, so management traffic leaves by the interface you intend
- Application-based quality of service, and marking traffic the network will honour

Domain 03 — Deploy and Configure Features and Subscriptions

The subscription layer that turns a firewall into a next-generation firewall. 17% of the exam.

- App-ID: application signatures, dependencies, application filters and groups, and building a rulebase around applications rather than ports
- Application shifts and the dependency chain that silently breaks a rule you thought was complete
- GlobalProtect: portal and gateway configuration, agent settings, and the authentication chain behind them
- Decryption configuration: forward proxy, inbound inspection, and the exclusions that keep pinned applications working
- User-ID configuration: agents, agentless collection, group mapping, and the redistribution of mappings between firewalls
- WildFire: submission policy, analysis profiles, verdict handling, and signature turnaround
- Web Proxy configuration, and the deployment it suits
- Verifying that each subscription is licensed, updating, and actually inspecting what you believe it is inspecting

Domain 04 — Deploy and Configure Firewalls Using Panorama

Managing an estate rather than a device. 17% of the exam.

- Templates and template stacks, and the network and device settings that belong in each
- Stack ordering, and which template wins when two of them set the same value
- Device groups, the hierarchy above them, and inheritance down the tree
- Pre-rules and post-rules, and where a local rule sits between them
- Managing firewall configurations from Panorama: commit, push, and the difference between them
- Partial commits, commit scope, and pushing to a subset of devices
- Config audit and revision comparison before a push rather than after it
- Recovering a device group or template change that went out wrong
- What stays local on the firewall, and the settings Panorama will not manage for you

Domain 05 — Manage and Operate

The lifecycle work that keeps the estate current and observable. 16% of the exam.

- Log forwarding configuration: profiles, match lists and forwarding destinations
- Choosing what to log and at what verbosity, and the storage and performance that follows
- Forwarding to Panorama, to a log collector, and to an external SIEM or syslog target
- Planning a PAN-OS upgrade: version paths, content versions, and the order in which devices are upgraded

- Executing an upgrade on standalone firewalls, on an HA pair, and through Panorama
- High availability functions: active-passive and active-active, link and path monitoring, and preemption
- HA session and configuration synchronisation, and what does not synchronise
- Testing failover deliberately, and confirming the passive member is genuinely ready

Domain 06 — Troubleshooting

The second-largest domain, and the one that decides whether the certificate means anything. 18% of the exam.

- Site-to-site tunnels: isolating a phase 1 failure from a phase 2 failure, and proxy ID mismatches
- Interfaces: link state, negotiation, counters, and the physical fault the configuration cannot fix
- Decryption failures: certificate trust, unsupported ciphers, pinned applications, and reading the decryption log
- Routing: route selection, next hop reachability, asymmetric paths, and virtual router leakage
- General troubleshooting method — session browser, packet capture, global counters, and the flow logic in the right order
- Resource protections: identifying which protection dropped the traffic and whether the threshold was wrong
- GlobalProtect: portal against gateway failures, agent logs, and authentication versus tunnel establishment
- Policies: the rule that matched instead of the one you expected, shadowed rules, and the test security-policy-match command
- High availability: split brain, failed synchronisation, and a pair that failed over for a reason nobody recorded
- Building a fault hypothesis and testing it, rather than changing configuration until the symptom moves

Who should take this

Engineers who already deploy and operate Palo Alto firewalls. Palo Alto's own guidance for this exam was three to five years in networking or security, plus six to twelve months actually deploying and configuring next-generation firewalls, and that is the right bar for this course too.

You should arrive able to build a Layer 3 interface, write a security rule and configure NAT without help. The course spends its time on the things that are hard — decryption, Panorama hierarchy, HA behaviour and troubleshooting method — and does not re-teach the basics. If firewall administration is new to you, take the foundational course first.

It suits network security engineers, firewall specialists, and consultants who inherit unfamiliar Palo Alto estates and have to make sense of them quickly.

The exam

The PCNSE is set and awarded by Palo Alto Networks and was delivered at Pearson VUE test centres and online.

- Exam code PCNSE
- 70 questions, 80 minutes
- Multiple choice, scenario questions with graphics, and matching items
- Available in English and Japanese
- Delivered through Pearson VUE
- Retired on 31 July 2025 and no longer bookable

Palo Alto Networks does not publish a passing score for this exam, so we do not quote one. The blueprint the domains above are taken from is dated February 2023 and the companion study guide January 2023, written against PAN-OS 11.0.

If you need a current certification, the Palo Alto Networks Certified Next-Generation Firewall Engineer is the closest equivalent and is the one we will book for you. Its blueprint is published on Palo Alto's own site; we will send it with your joining instructions so you can see the mapping between it and the material below.

How we deliver it

Five days, classroom or online live, or at your office for a private group. Every delegate gets their own firewalls and a shared Panorama, because template stacks and device group hierarchy cannot be understood from a diagram and HA cannot be tested on one box.

The final two days are troubleshooting-weighted to match the blueprint. You are handed estates that are already broken — a tunnel that will not come up, a decryption policy that breaks one application, an HA pair that failed over overnight — and asked to diagnose them against the clock and explain your reasoning afterwards.

Mapped to the Palo Alto Networks PCNSE exam blueprint. Taught from Hacky Security's own curriculum and lab estate by instructors who design and run Palo Alto deployments in production. These are our own preparation courses; they are not official Palo Alto Networks courseware and we are not an Authorised Training Partner.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

FROM

₹110,500

per person

INR ₹110,500 per person

USD \$1,319 per person

GBP £1,039 per person

AED AED 4,899 per person

Group, corporate and repeat-cohort pricing on request. Prices are reviewed quarterly and exclude the exam voucher.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 • info@hackysecurity.com

<https://hackysecurity.com/courses/hacky-palo-alto-networks-training/>

CHANDIGARH • SHIMLA • DELHI • DUBAI • LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 12 September 2026.