Networking & Infrastructure

Program Brochure · 2026

PALO ALTO PCNSE PREP

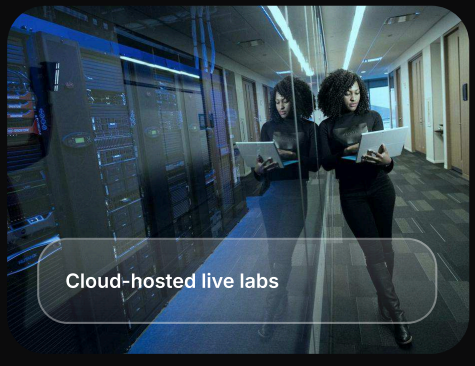
Next-generation firewalls, mastered.

Advanced ↗ 72 Hours ↗ PCNSE ↗

Networking & Infrastructure

Connect. Secure. Scale.

10 programs in this track



8

modules · hands-on labs · capstone project

Inside this brochure

Contents

Program overview 03
Who it's for 04
Learning outcomes 05
Program runway 06
Detailed curriculum 07
Tools & frameworks 10
Projects & capstone 11
Certification & method 12
Learning path 13
FAQs 14



AT A GLANCE

Level	**Advanced**
Duration	**72 Hours**
Modules	**8**
Certificate	**PCNSE**

Program overview

Next-generation firewalls, mastered.

Configure and manage Palo Alto next-generation firewalls, policies and threat prevention.

Next-generation firewalls sit at the centre of modern network defence, and Palo Alto Networks platforms are widely deployed across enterprises. This advanced program prepares engineers for the PCNSE exam, covering PAN-OS deployment, App-ID, User-ID and Content-ID, decryption, GlobalProtect, Panorama management and troubleshooting through extensive hands-on firewall labs. Scenarios mirror real enterprise firewall operations.

DELIVERY

ILT · VILT · Lab-intensive



WHAT YOU'LL PRACTISE

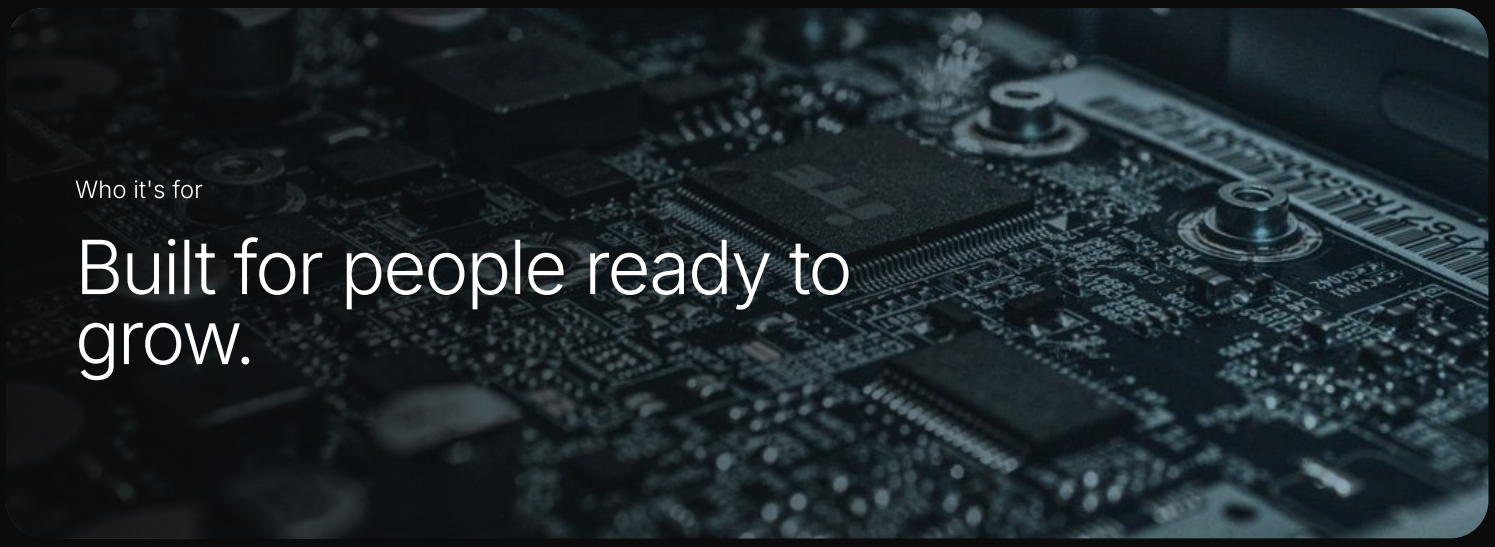
- Configure NGFW policies
- Use App-ID and User-ID
- Set up threat prevention
- Prepare for the PCNSE exam

LEVEL
Advanced

DURATION
72 Hours

CERTIFICATION
PCNSE

TRACK
Networking & Infrastructure



Who it's for

Built for people ready to grow.

01

Beginners

Network+ and CCNA foundations

02

Network engineers

CCNP Enterprise, SD-WAN, automation

03

Security engineers

Palo Alto, Fortinet, network security

04

Architects

CCIE prep, Zero Trust, SASE / SSE

PREREQUISITES

Solid TCP/IP and routing knowledge	01
Experience with firewall or security concepts	02
Basic familiarity with VPNs and NAT	03

ROLES THIS PREPARES YOU FOR

- Firewall Engineer ↗
- Network Security Engineer ↗
- Security Administrator ↗
- Security Implementation Consultant ↗
- Network Security Architect ↗

Learning outcomes

What you'll be able to do.



01 Deploy and configure PAN-OS firewalls in common modes

02 Build security and NAT policies using App-ID and zones

03 Integrate User-ID for identity-based access control

04 Configure threat prevention, URL filtering and WildFire profiles

05 Implement SSL decryption and GlobalProtect remote access

06 Manage multiple firewalls centrally using Panorama

Program runway

Module by module.

8
modules · 72 hours

01	**PAN-OS Architecture and Deployment** Single-pass parallel processing architecture, Interface types and deployment modes, Initial configuration and licensing	8 hrs
02	**Security and NAT Policy** Zone-based security policy, Policy rule ordering and best practices, Source and destination NAT	10 hrs
03	**App-ID and Content-ID** App-ID identification process, Application dependencies and overrides, Antivirus and anti-spyware profiles	10 hrs
04	**User-ID and Identity** User-ID agents and mapping methods, Group mapping with LDAP, Authentication policy and MFA	8 hrs
05	**URL Filtering, WildFire and DNS Security** Advanced URL Filtering categories, WildFire analysis and verdicts, DNS Security and sinkholing	8 hrs
06	**Decryption and GlobalProtect** SSL forward proxy decryption, Inbound inspection and exclusions, GlobalProtect portal and gateway	10 hrs
07	**Panorama and Operations** Panorama device groups and templates, Commit and push workflows, Logging, reporting and log forwarding	10 hrs
08	**Troubleshooting and Exam Readiness** CLI troubleshooting commands, Packet captures and flow basics, Session and traffic log analysis	8 hrs
★	**Capstone · Enterprise NGFW Deployment Project** Assessment, capstone review and certification	

The syllabus.

Modules 01–03

Module 01

PAN-OS Architecture and Deployment

8 hours

Hands-on lab
Perform initial setup of a VM-Series firewall with interfaces and zones.

TOPICS COVERED

- Single-pass parallel processing architecture
- Interface types and deployment modes
- Initial configuration and licensing
- Virtual routers and logical routers
- High availability concepts

Module 02

Security and NAT Policy

10 hours

Hands-on lab
Build security and NAT rules publishing an internal web server.

TOPICS COVERED

- Zone-based security policy
- Policy rule ordering and best practices
- Source and destination NAT
- Policy Optimizer
- Security policy troubleshooting

Module 03

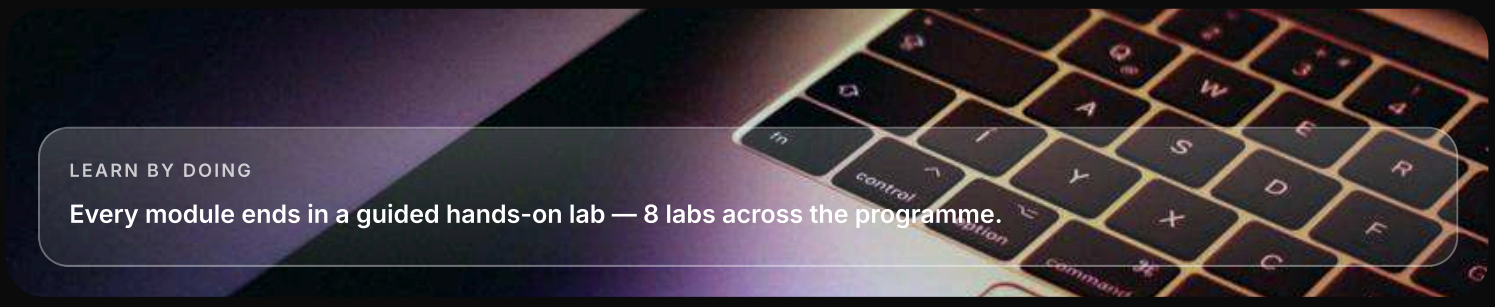
App-ID and Content-ID

10 hours

Hands-on lab
Migrate port-based rules to App-ID rules with threat profiles attached.

TOPICS COVERED

- App-ID identification process
- Application dependencies and overrides
- Antivirus and anti-spyware profiles
- Vulnerability protection profiles
- File blocking and data filtering



LEARN BY DOING

Every module ends in a guided hands-on lab — 8 labs across the programme.

Syllabus, continued.

Modules 04–06

Module 04

User-ID and Identity

8 hours

Hands-on lab
Configure User-ID with group-based policy for two departments.

TOPICS COVERED

- User-ID agents and mapping methods
- Group mapping with LDAP
- Authentication policy and MFA
- Captive portal configuration
- Cloud Identity Engine overview

Module 05

URL Filtering, WildFire and DNS Security

8 hours

Hands-on lab
Enforce URL filtering and verify a DNS sinkhole action in logs.

TOPICS COVERED

- Advanced URL Filtering categories
- WildFire analysis and verdicts
- DNS Security and sinkholing
- Credential phishing prevention
- Custom URL categories and exceptions

Module 06

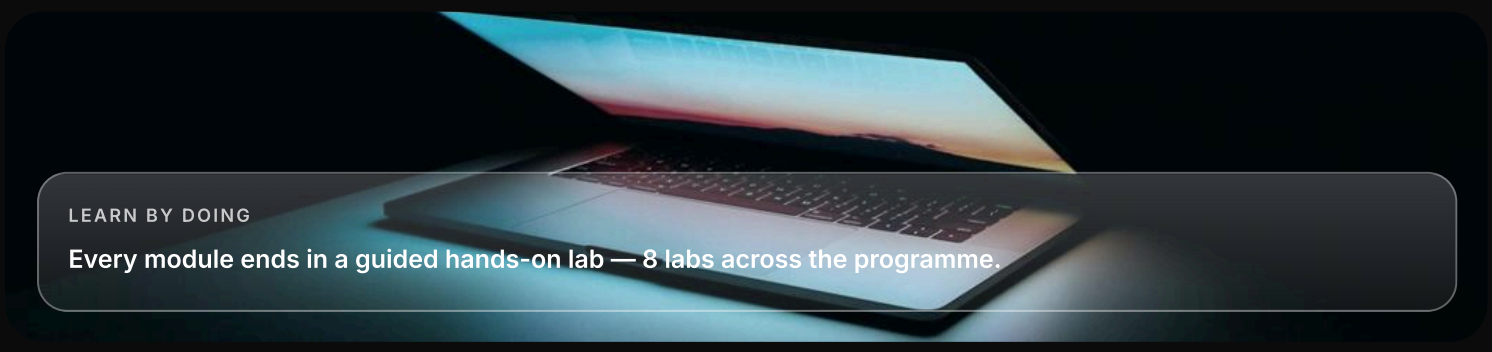
Decryption and GlobalProtect

10 hours

Hands-on lab
Configure SSL forward proxy decryption and GlobalProtect client access.

TOPICS COVERED

- SSL forward proxy decryption
- Inbound inspection and exclusions
- GlobalProtect portal and gateway
- Site-to-site IPsec VPN
- HIP checks



LEARN BY DOING

Every module ends in a guided hands-on lab — 8 labs across the programme.

Syllabus, continued.

Modules 07–08

Module 07

Panorama and Operations

10 hours

Hands-on lab
Manage two firewalls through Panorama templates and device groups.

TOPICS COVERED

- Panorama device groups and templates
- Commit and push workflows
- Logging, reporting and log forwarding
- HA active/passive configuration
- Upgrades and maintenance

Module 08

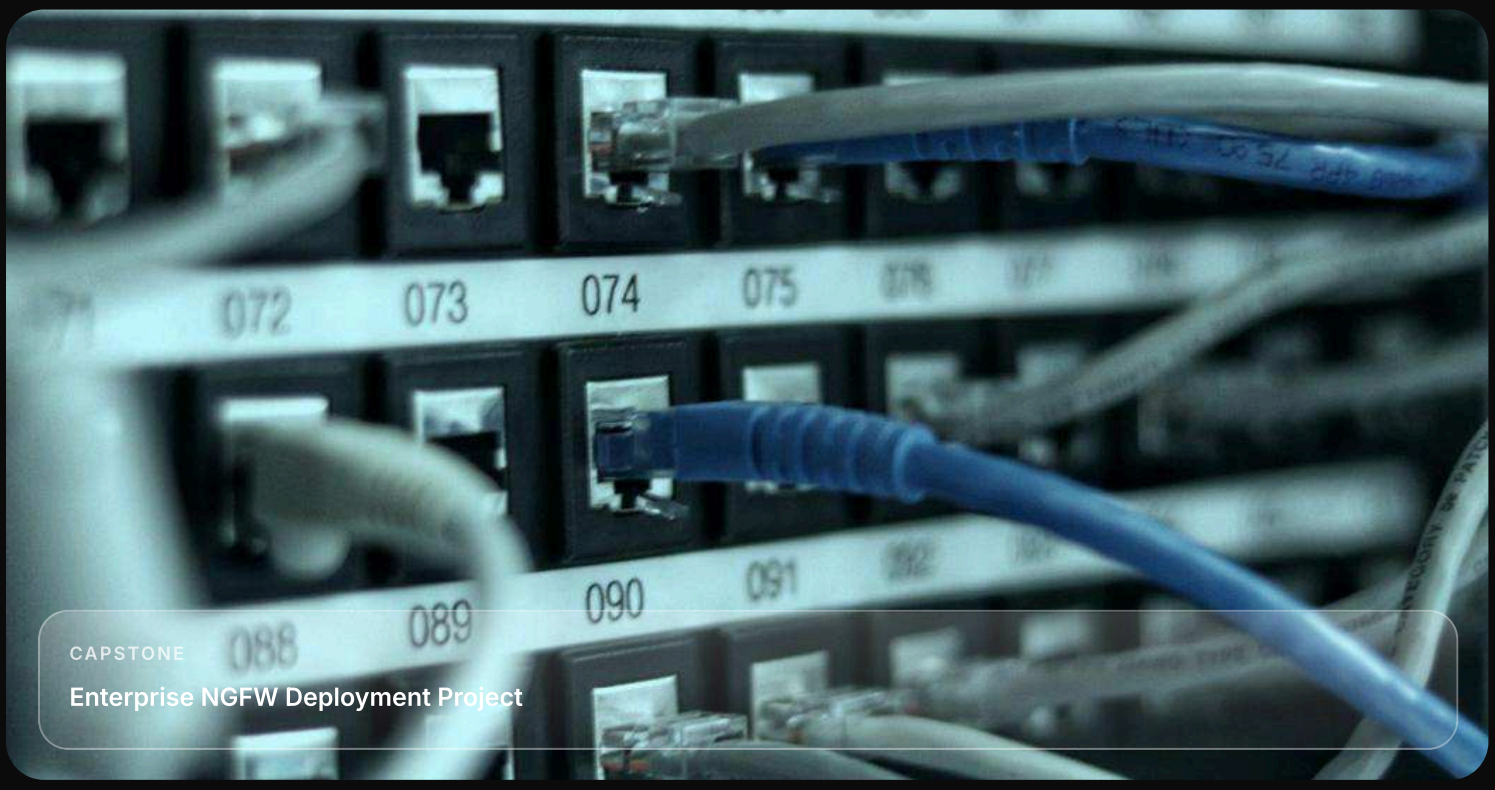
Troubleshooting and Exam Readiness

8 hours

Hands-on lab
Troubleshoot broken policy, NAT and VPN scenarios using CLI tools.

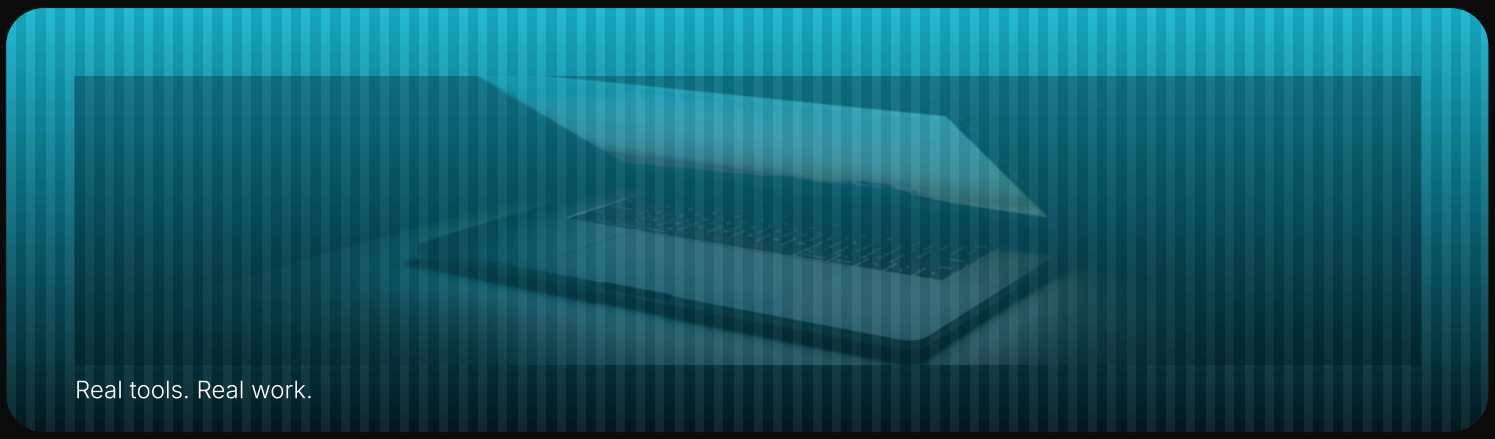
TOPICS COVERED

- CLI troubleshooting commands
- Packet captures and flow basics
- Session and traffic log analysis
- PCNSE domain review
- Timed practice questions



CAPSTONE

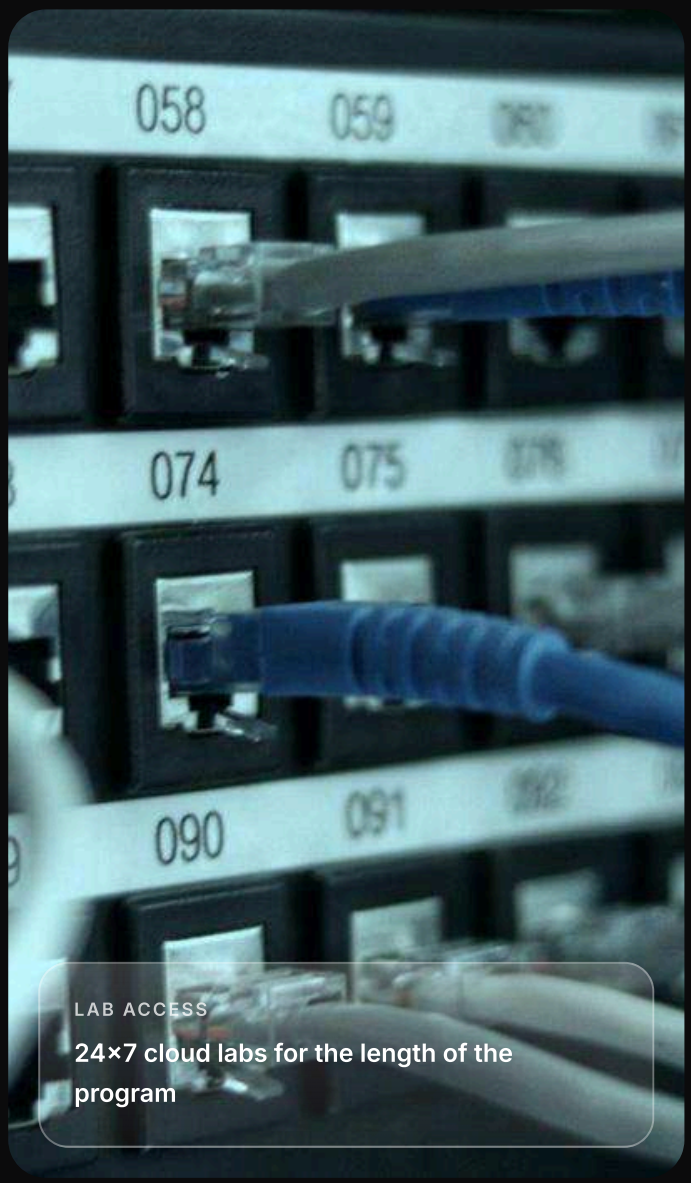
Enterprise NGFW Deployment Project



Palo Alto Networks
Next-gen firewalls

What you will build

Configure NGFW policies	01
Use App-ID and User-ID	02
Set up threat prevention	03
Prepare for the PCNSE exam	04



01

Data Centre Perimeter Policy

Design App-ID based security and NAT policies protecting a multi-tier application with full threat profiles.

02

Identity-Based Access Rollout

Integrate User-ID with LDAP groups and enforce department-based application access, backed by authentication policy and verified traffic logs.

03

Remote Access Deployment

Deploy GlobalProtect with HIP checks and SSL forward proxy decryption, documenting decryption exclusions, client experience and verification steps.



Capstone project

Enterprise NGFW Deployment Project

Design and deploy a Panorama-managed Palo Alto firewall pair with HA, App-ID and User-ID policies, threat prevention, decryption and GlobalProtect, then troubleshoot injected faults and present the design.

Real-world scenario ↗ Mentor review ↗ Portfolio ready ↗

Certification

PCNSE

Awarded on successful completion of the program assessments.

- MCQ assessments
- Practical lab evaluation
- Project & capstone review
- Final presentation



The SAM Learning Framework™

Scenario · Apply · Master · Mentor

Phase 01

Scenario

Real-world attack and use-case scenarios open every module.

Phase 02

Apply

Hands-on lab work, CTF challenges and live projects.

Phase 03

Master

Assessment, peer review and certification prep.

Phase 04

Mentor

Post-program career guidance and support.

DELIVERY MODELS

- Instructor-Led (ILT)
- Virtual Instructor-Led
- Self-Paced Online
- E-Learning Licensing
- Blended Learning
- Corporate Onsite
- Bootcamp Intensive

Learning path · Networking & Infrastructure

Where this program fits.

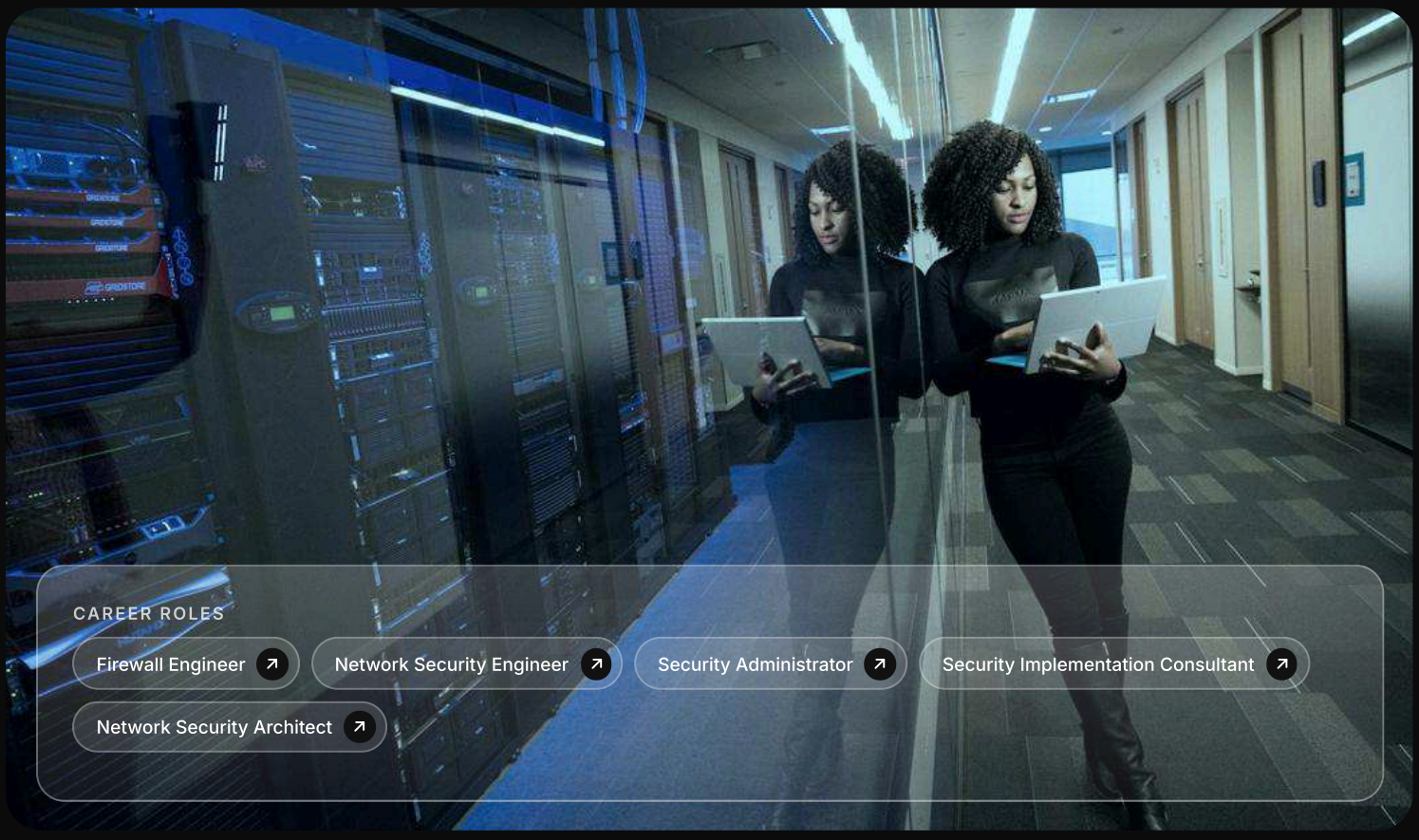
Beginner	Intermediate	Advanced	Expert
2 programs	3 programs	You are here	2 programs

Before this

Cisco CCNP Enterprise	120 Hours
Network Security Fundamentals	48 Hours
SD-WAN & Network Automation	56 Hours

Up next

Zero Trust Network Architecture	48 Hours
SASE & SSE Architecture	40 Hours



CAREER ROLES

- Firewall Engineer
- Network Security Engineer
- Security Administrator
- Security Implementation Consultant
- Network Security Architect

Questions, answered.

Q01

Do I need prior experience to join?

Yes. You should understand TCP/IP, routing, NAT and VPN concepts, and ideally have some firewall administration experience. Prior Palo Alto Networks experience is helpful but not mandatory, as PAN-OS fundamentals are reviewed early.

Q02

How is the program delivered and scheduled?

The 72 hours program is instructor-led and delivered live virtual or blended, combining concept sessions, demonstrations and guided hands-on work. Batch timings and session frequency are confirmed with the academy team at enrollment.

Q03

Will I get a certificate, and is the official exam included?

You receive a Samcommunity Academy certificate of completion after passing the program assessments. The PCNSE exam is booked and taken separately through Palo Alto Networks's official testing process; exam fees are included only if stated in your enrollment details.

Q04

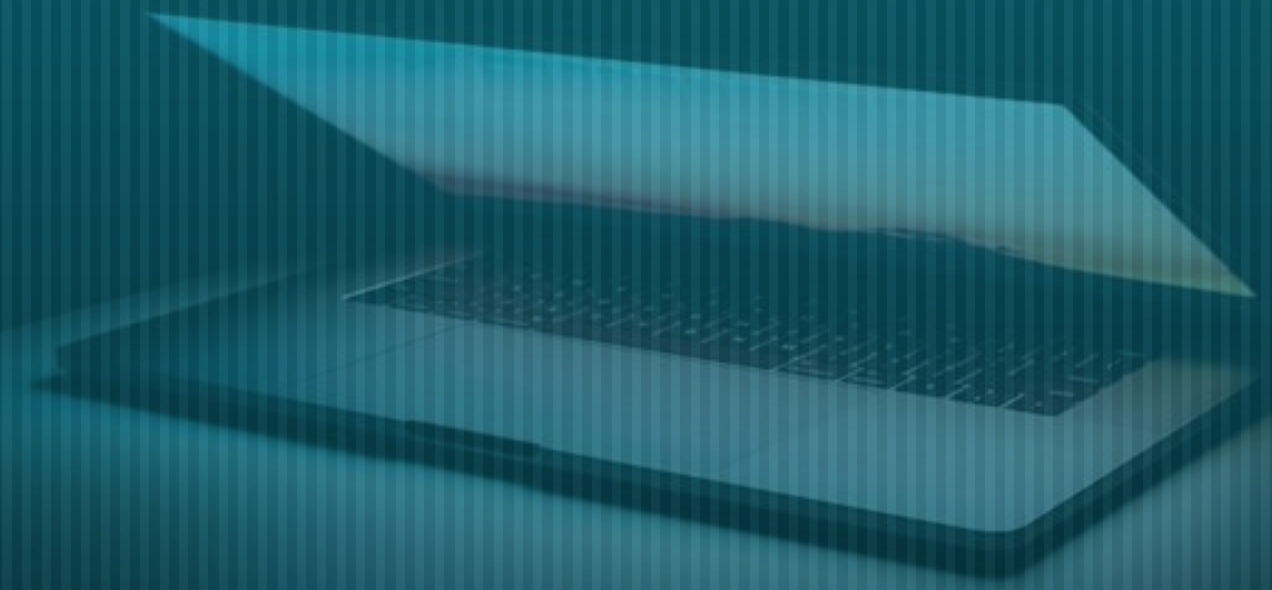
What labs and tools will I have access to?

Labs use Palo Alto Networks VM-Series firewalls and Panorama in virtual environments where licensing permits, along with Linux test hosts. Lab access arrangements and setup guidance are shared during onboarding.

Q05

Is career support provided?

Yes. You receive guidance on building a portfolio from your projects, presenting skills on your resume and preparing for interviews. Career support helps you present yourself well, but job placement, interviews and salaries are not guaranteed.



Let's talk

START PALO ALTO PCNSE PREP.

academy@samcommunity.in

corporate@samcommunity.in

samcommunity.in

@samcommunity_

Learn practical skills. Grow with mentors.

Xylyn Samcommunity Private Limited · DPIIT-recognized startup · Surat, Gujarat, India