DevOpsSchool

Course curriculum · November 2026

LEVEL 03 OF 04 · INTERMEDIATE

Palo Alto Networks Intermediate Training

Configure decryption, GlobalProtect and site-to-site VPNs and HA pairs, and troubleshoot traffic with CLI and packet captures.

LIVE ONLINE **Max 8-10 hours**	CORPORATE (DAY-WISE) **3 days · Days 1-3**	SELF-PACED VIDEO **1-year LMS access**
BATCH SIZE **Max 10 learners**	NEXT BATCHES **1st of every month · weekends: first Saturday**	CERTIFICATE **Verifiable certificate of completion**

Foundation	Essential	Intermediate	Advanced
1 day · Included	2 days · Included	3 days · This curriculum	5 days · Next step

INSIDE THIS CURRICULUM

What you will achieve	Outcomes and level focus
Who should attend	Audience and prerequisites
Agenda	35 topics · Foundation to Intermediate
Hands-on labs	3 labs
Formats and fees	Live, 1:1, self-paced, corporate
Trainer and reviews	Rajesh Kumar
Enrolment	Batches, payment, contacts

WHY DEVOPSSCHOOL

- Rated 4.6 on Google
- 1,500+ verifiable certificates issued in the public registry
- Trainer Rajesh Kumar: 20 years in industry
- Small batches: max 10 learners, every session recorded

Course page: www.devopsschool.com/courses/paloaltonetworks/palo-alto-networks-intermediate-training.html
Talk to us: WhatsApp +91 99057 40781 · +1 (469) 756-6329 · contact@DevOpsSchool.com · reply within 1 hour

OUTCOMES

What you will achieve

By the end of the Palo Alto Networks course path, you will be able to:

1

Configure Palo Alto firewalls

Set up interfaces, zones, NAT and application-based security policies on PAN-OS.

2

Prevent threats and secure access

Apply threat prevention, decryption, User-ID and VPNs to protect users and data.

3

Operate firewalls at scale

Manage, automate and troubleshoot firewall estates with Panorama and APIs.

WHAT THE INTERMEDIATE LEVEL ADDS

Decryption, VPNs, high availability and troubleshooting

Hands-on: Connect and protect remote users. Deploy an HA pair with decryption, a site-to-site IPsec VPN and GlobalProtect with SAML login, then trace a failing session with captures.

WHO SHOULD ATTEND

- Regular Palo Alto Networks users who want to automate, integrate and manage it at a deeper level.
- Specialists who support Palo Alto Networks for colleagues or customers.
- Leads preparing Palo Alto Networks for wider use across projects.

BEFORE YOU START

- The Essential level, or equivalent hands-on experience.
- You can already: Build application-based policies with threat prevention, URL filtering and User-ID, and monitor traffic with logs and the ACC.
- Basic computer skills and a laptop with a stable internet connection for the live sessions and labs.
- This curriculum includes every earlier level, so it is complete on its own.

AGENDA · FOUNDATION TO INTERMEDIATE

Palo Alto Networks Intermediate Training agenda

35 topics. Each level builds on the one before it, so this curriculum lists every earlier level in full. Days are for corporate (day-wise) delivery; live online batches cover the same agenda in max 8-10 hours.

DAY 1 — Foundation: NGFW concepts, initial setup and first policies

Included from Foundation

1. Next-generation firewall concepts: App-ID, User-ID, Content-ID and single-pass architecture
2. Palo Alto Networks portfolio: hardware NGFWs, VM-Series, CN-Series, Cloud NGFW, Panorama and Prisma Access
3. PAN-OS architecture: management plane versus data plane and the packet flow sequence
4. Initial configuration: management interface, admin accounts, DNS, NTP and licences
5. Web interface and CLI: navigation, configure mode and operational commands
6. Candidate and running configuration: commit, revert, configuration snapshots and backups
7. Security zones and interfaces: Layer 3, Layer 2, virtual wire and tap modes
8. Routing basics: virtual routers or logical routers, static routes and default gateways
9. Security policies: rule matching order, intrazone and interzone defaults and rule fields
10. Source NAT: dynamic IP and port for outbound internet access
11. Dynamic updates: applications and threats content, antivirus and WildFire update schedules

DAY 2 — Essential: App-ID policy, threat prevention and user identity

Included from Essential

12. App-ID in depth: application signatures, dependencies, application groups and filters
13. Policy Optimizer: moving from port-based rules to application-based rules
14. Destination NAT: publishing internal servers, U-turn NAT and NAT rule ordering
15. Security profiles: Antivirus, Anti-Spyware, Vulnerability Protection and File Blocking
16. URL Filtering: categories, custom URL categories, safe search and credential phishing prevention
17. WildFire: file submission, verdicts and updating protections
18. DNS Security: malicious domain blocking and sinkholing
19. User-ID: agent and agentless integration with Active Directory, group mapping and user-based rules
20. Monitoring: Traffic, Threat, URL and System logs and log filters
21. Application Command Center (ACC): widgets, drill-down and identifying risky applications
22. Reports: predefined, custom and scheduled reports
23. Change workflow: rule naming, tags, descriptions and peer-reviewed commits

DAY 3 — Intermediate: Decryption, VPNs, high availability and troubleshooting

New at this level

24. SSL/TLS decryption: forward proxy, inbound inspection, certificates and decryption exclusions
25. Decryption policy design: privacy categories, decryption profiles and troubleshooting broken sites
26. Site-to-site IPsec VPN: IKE gateways, IPsec tunnels, crypto profiles and proxy IDs
27. GlobalProtect: portal, gateway, agent configuration, authentication and split tunnelling
28. Authentication: authentication profiles with LDAP, RADIUS and SAML, MFA and admin roles
29. High availability: active/passive and active/active, HA links, path and link monitoring
30. Dynamic routing: OSPF and BGP on the firewall with route redistribution

31. Zone protection and DoS protection profiles: flood, reconnaissance and packet-based attack protection
32. Troubleshooting with the CLI: show session all, test security-policy-match and global counters
33. Packet captures: capture stages, filters and reading captures in Wireshark
34. Log forwarding: syslog, email and HTTP forwarding to a SIEM
35. Upgrades: PAN-OS upgrade paths, content compatibility and HA upgrade sequence

PRACTICE

Hands-on labs

You build these yourself during the course, guided by the trainer.

FOUNDATION

Set up a firewall from scratch

Configure a VM-Series firewall with management settings, zones, interfaces, a default route, outbound NAT and an internet access policy.

ESSENTIAL

Build application-aware threat prevention

Replace port-based rules with App-ID rules, apply security profile groups and URL filtering per AD group, and verify blocks in the logs and ACC.

INTERMEDIATE

Connect and protect remote users

Deploy an HA pair with decryption, a site-to-site IPsec VPN and GlobalProtect with SAML login, then trace a failing session with captures.

HOW YOU CAN LEARN

Formats and fees

The same agenda in four formats. Fees are in Indian rupees as of November 2026; the course page shows them in your currency.

FORMAT	DURATION	WHAT YOU GET	FEE
Live & interactive (online)	Max 8-10 hours	Instructor-led public batch of max 10 learners with demos, labs, Q&A and assignment review. Weekday batches start on the 1st of every month, weekend batches on the first Saturday of every month.	**INR 34,999**
1:1 live training (online)	Max 8-10 hours, one-to-one	The same agenda, taught one-to-one by the trainer. Starts immediately, without waiting for the next batch; sessions planned around your working hours, at your pace.	**INR 99,999**
Self-paced video	1-year LMS access	All four Palo Alto Networks levels, plus 20+ more courses and 50+ tools, at your own pace.	**INR 833/month** billed yearly at INR 9,996
Corporate (day-wise)	3 days for this level	A private batch for your team, on demand. Foundation 1 day, Essential 2, Intermediate 3, Advanced 5 (cumulative).	**Quote on request**

ASSESSMENT AND CERTIFICATE

Your progress is checked through hands-on labs and assignments at every level. On completion you receive a DevOpsSchool certificate of completion with a unique credential ID that anyone can verify at devopsschool.com/certificates.

INCLUDED WITH EVERY LIVE BATCH

- Every live session is recorded and stays in your LMS for a year.
- Can't attend your batch? Move to next month's batch.
- Free demo class before you pay.
- Free 10-15 minute call with an advisor or the trainer to check the course fits you.

YOUR TRAINER

Learn from Rajesh Kumar

Principal Architect, trainer and mentor in DevOps, SRE, DevSecOps and platform engineering, with 20 years across 8+ software MNCs, including Staff DevOps/SRE Engineer for a leading Japanese mobile-payment platform and Principal DevOps Architect and Manager in Europe.

Profile: www.rajeshkumar.xyz · Videos: youtube.com/@TheDevOpsSchool

20 years in industry	**200+** corporate trainings
10,000+ engineers mentored	**70+** organisations coached

REVIEWS

What learners say

Rated 4.6 on Google · more reviews at devopsschool.com/testimonials and in our video testimonials.

> “Rajesh is very good trainer. Rajesh was able to resolve our queries and question effectively. We really liked the hands-on examples covered during this training program.”
>
> Indrayani, India

> “The training was very useful and interactive. Rajesh helped develop the confidence of all.”
>
> Abhinav Gupta, Pune

START YOUR PALO ALTO NETWORKS TRAINING

Join the next batch

Weekday batches start on the 1st of every month and weekend batches on the first Saturday of every month, with max 10 learners each. 1:1 training can start immediately; corporate batches run on demand. We reply within 1 hour.

Pay by UPI, credit and debit cards, net banking or PayPal. Before you pay, read our refund policy. All levels of this course: www.devopsschool.com/courses/paloaltonetworks/

ENROL OR RESERVE A SEAT
Palo Alto Networks Intermediate Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com

Next step after this level: Palo Alto Networks Advanced Training - Manage firewalls centrally with Panorama or Strata Cloud Manager, automate configuration and design Zero Trust network security at scale.