

PALO ALTO NETWORKS FIREWALL ADMINISTRATION & SECURITY



GENTEX[®]
TRAINING CENTER



Introduction

Network perimeters now extend far beyond the office, and traditional port-based firewalls cannot follow that change. The Palo Alto Networks Firewall Administration & Security Training Course prepares security and network professionals to run next-generation firewalls that inspect traffic by application, user, and content. Participants learn to configure zones, security policies, NAT, and application identification on the PAN-OS platform. Furthermore, the course covers threat prevention, URL filtering, decryption, and the WildFire sandbox service. In addition, it addresses VPN configuration, high availability, and log-based investigation. As a result, teams gain stronger visibility, tighter control, and a firewall estate that supports compliance and incident response.

Palo Alto Networks Firewall Administration & Security Course Objectives

- Deploy and license Palo Alto Networks next-generation firewalls.
- Configure zones, interfaces, virtual routers, and network profiles.
- Build security policies using App-ID, User-ID, and Content-ID.
- Configure NAT, policy-based forwarding, and decryption profiles.
- Apply threat prevention, antivirus, and anti-spyware profiles.
- Configure URL filtering, DNS security, and WildFire sandboxing.
- Implement site-to-site and remote-access VPN using IPsec and GlobalProtect.
- Set up high availability, heartbeat, and link monitoring.
- Investigate incidents using logs, the ACC, and Panorama reporting.
- Manage configuration with Panorama templates and role-based admin access.

Course Methodology

- Instructor-led sessions combining firewall theory with hands-on practice.

LEARN BOLD. LEAD BEYOND

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com



- Guided configuration labs on PAN-OS firewalls and virtual instances.
- Simulated attack traffic to test App-ID and threat prevention rules.
- Scenario-based troubleshooting using real firewall logs.
- Group discussion and case studies on enterprise perimeter design.
- Continuous knowledge checks and a final practical configuration assessment.

Who Should Take This Course

- Network security engineers and firewall administrators.
- SOC analysts and incident response team members.
- Network engineers managing perimeter and data centre security.
- Security architects designing segmented network environments.
- IT infrastructure staff supporting enterprise firewalls.
- Consultants implementing next-generation firewall projects.

Palo Alto Networks Firewall Administration & Security Course Outlines

Day 1: Firewall Fundamentals and Initial Setup

- Next-generation firewall architecture and single-pass parallel processing.
- Hardware, VM-Series, and cloud form factors.
- Initial setup, licensing, and software updates.
- Administrative accounts, roles, and management access.
- Zones, interfaces, virtual routers, and security profiles.
- Understanding the traffic flow and session table.
- Lab: first deployment and administrative hardening.





Day 2: Security Policies and Traffic Control

- Security policy structure, order, and rule matching.
- App-ID application identification and policy creation.
- User-ID integration with Active Directory and LDAP.
- NAT configuration: source, destination, and static NAT.
- Policy-based forwarding and application override.
- Security profile groups and best practice rules.
- Lab: building a layered security policy for a branch.

Day 3: Threat Prevention and Content Inspection

- Antivirus, anti-spyware, and vulnerability protection profiles.
- Content-ID and file blocking rules.
- URL filtering, categories, and safe search enforcement.
- SSL decryption: forward proxy and inbound inspection.
- WildFire sandboxing and DNS security.
- Data filtering and pattern-based detection.
- Lab: blocking live threats with content inspection.

Day 4: VPNs, High Availability, and User Access

- IPsec site-to-site VPN configuration and troubleshooting.
- GlobalProtect remote access and host information profiles.
- Certificate management and VPN authentication.
- High availability active-passive and active-active modes.
- Link monitoring, path monitoring, and failover testing.

LEARN BOLD. LEAD BEYOND

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com



- Quality of service and bandwidth management.
- Lab: configuring a VPN and an HA pair.

Day 5: Monitoring, Automation, and Troubleshooting

- Log types, filtering, and the Application Command Center (ACC).
- Panorama management, templates, and device groups.
- REST API and CLI automation for routine tasks.
- Diagnosing policy, routing, and decryption failures.
- Reporting, compliance evidence, and audit support.
- Capacity planning and performance tuning.
- Lab: end-to-end investigation of a simulated incident.

Conclusion

By successfully completing the Palo Alto Networks Firewall Administration & Security Training Course, participants will have acquired the knowledge to deploy next-generation firewalls, build App-ID and User-ID based security policies, apply threat prevention and decryption, and configure VPNs and high availability. They will also gain the ability to investigate incidents through logs, the ACC, and Panorama. Furthermore, the course prepares teams to strengthen perimeter control and compliance. Gentex Training Center delivers this programme with a strong emphasis on practical, workplace-ready firewall administration.

FAQs for the Palo Alto Networks Firewall Administration & Security course





Q1 What is the "Palo Alto Networks Firewall Administration & Security" course about?

It is a hands-on programme on deploying and managing Palo Alto Networks next-generation firewalls. It covers PAN-OS configuration, zones and interfaces, App-ID and User-ID security policies, NAT, decryption, threat prevention, VPNs, high availability, and Panorama-based monitoring and reporting.

Q2 What are the key benefits of the "Palo Alto Networks Firewall Administration & Security" course?

Participants gain full visibility into application and user traffic, which allows precise control instead of broad port-based rules. The course strengthens protection against malware, exploits, and phishing through layered content inspection, improves VPN and perimeter reliability, and gives teams the investigative skills to reduce response time.

Q3 What skills will I gain from the "Palo Alto Networks Firewall Administration & Security" course?

Next-generation firewall deployment and configuration; security policy design with App-ID, User-ID and Content-ID; threat prevention, decryption and WildFire configuration; and log-based monitoring, Panorama management and troubleshooting.



Q4 What tools, methods, or standards are covered in the "Palo Alto Networks Firewall Administration & Security" course?

The course covers the PAN-OS platform, App-ID, User-ID, Content-ID, WildFire sandboxing, DNS Security, URL filtering, SSL decryption profiles, IPsec and GlobalProtect VPN, high availability modes, Panorama with templates and device groups, and the firewall REST API and CLI.

Q5 How is the "Palo Alto Networks Firewall Administration & Security" course applied in real-world practice?

Graduates apply it by placing next-generation firewalls at the perimeter and between internal segments, writing policies that allow only approved applications and users, and tuning threat prevention profiles to block malware and exploits. They also run decryption for inspection, manage VPN access, and investigate alerts in Panorama.