Firewall 11.1 Essentials: Configuration and Management

Course code: EDU-210

Successful completion of this five-day, instructor-led course should enhance the student's understanding of how to configure and manage Palo Alto Networks Next-Generation Firewalls. The course includes hands-on experience configuring, managing, and monitoring a firewall in a lab environment.

Affiliate	Duration	Course price	ITB
Praha	5	59 000 Kč	0
Bratislava	5	2 400 €	0

The prices are without VAT.

Course terms

Date	Duration	Course price	Type	Course language	Location
19.01.2026	5	59 000 Kč	Presence	CZ/SK	TD SYNNEX Czech
19.01.2026	5	59 000 Kč	Online	CZ/SK	TD SYNNEX Czech - Online
23.02.2026	5	59 000 Kč	Online	EN	TD SYNNEX Czech - Online
16.03.2026	5	59 000 Kč	Online	CZ/SK	TD SYNNEX Czech - Online
16.03.2026	5	59 000 Kč	Presence	CZ/SK	TD SYNNEX Czech
11.05.2026	5	59 000 Kč	Online	EN	TD SYNNEX Czech - Online
08.06.2026	5	59 000 Kč	Presence	CZ/SK	TD SYNNEX Czech
08.06.2026	5	59 000 Kč	Online	CZ/SK	TD SYNNEX Czech - Online
22.06.2026	5	59 000 Kč	Online	EN	TD SYNNEX Czech - Online
07.09.2026	5	59 000 Kč	Online	EN	TD SYNNEX Czech - Online
05.10.2026	5	59 000 Kč	Presence	CZ/SK	TD SYNNEX Czech
05.10.2026	5	59 000 Kč	Online	CZ/SK	TD SYNNEX Czech - Online
02.11.2026	5	59 000 Kč	Online	EN	TD SYNNEX Czech - Online

The prices are without VAT.

What we teach you

The Palo Alto Networks Firewall Essentials: Configuration and Management (EDU-210) course is five days of instructor-led training that will help you to:

- Configure and manage the essential features of Palo Alto Networks next-generation firewalls
- Configure and manage Security and NAT policies to enable approved traffic to and from zones
- Configure and manage Threat Prevention strategies to block traffic from known and unknown IP addresses, domains, and URLs
- Monitor network traffic using the interactive web interface and firewall reports

Who is the course for

Security Engineers, Security Administrators, Security Operations Specialists, Security Analysts, and Support Staff

Required skills

Students must have a basic familiarity with networking concepts including routing, switching, and IP addressing.

Students also should be familiar with basic security concepts. Experience with other security technologies (IPS, proxy, and content filtering) is a plus.

GOPAS®

Course outline

- Palo Alto Networks Portfolio and Architecture
- Configuring Initial Firewall Settings
- Managing Firewall Configurations
- Managing Firewall Administrator Accounts
- Connecting the Firewall to Production Networks with Security Zones
- Creating and Managing Security Policy Rules
- Creating and Managing NAT Policy Rules
- Controlling Application Usage with App-ID
- Blocking Known Threats Using Security Profiles
- Blocking Inappropriate Web Traffic with URL Filtering
- Blocking Unknown Threats with Wildfire
- Controlling Access to Network Resources with User-ID
- Using Decryption to Block Threats in Encrypted Traffic
- Locating Valuable Information Using Logs and Reports
- What's Next in Your Training and Certification Journey
- Securing Endpoints with GlobalProtect
- Providing Firewall Redundancy with High Availability
- Connecting Remotes Sites using VPNs
- Blocking Common Attacks Using Zone Protection