

Firewall 8.x: Troubleshooting (EDU-330)

Überblick

Der Kurs Palo Alto Networks Firewall 8.x Troubleshooting (EDU-330) ist ein dreitägiges Training, welches Ihnen dabei hilft:

- Netzwerkprobleme mithilfe von Firewall-Tools einschließlich der CLI zu untersuchen
- Bewährte Methoden zur Fehlerbehebung für einzelne Funktionen anzuwenden
- Reale Szenarien auf Grundlage von advanced Logs zu analysieren

Palo Alto Networks Ausbildung

Trainings von Palo Alto Networks und Palo Alto Networks Authorized Trainings Centern vermitteln das Know-how und die Expertise, die Lebensweise in Zeiten des digitalen Wandels zu schützen. Mit den anerkannten Security-Zertifizierungen erhalten Teilnehmer das nötige Wissen rund um die Next Generation Security-Plattformen, um Cyber-Attacken erfolgreich abzuwehren und Applikationen sicher bereit zu stellen.

Kursziele

Nach dem erfolgreichen Abschluss des dreitägigen Trainings haben Teilnehmer ein tiefes Verständnis bezüglich des Troubleshooting der Palo Alto Networks Next Generation Firewalls. Sie erhalten die Möglichkeit, anhand von praktischen Übungen, häufig auftretende Probleme hinsichtlich der Konfiguration der Sicherheitsfunktionen des PAN-OS Betriebssystems zu beheben. Zusätzlich erlangen Sie fundierte Kenntnisse über das allgemeine Troubleshooting und die Kontrolle von Apps, Usern und Content.

Umfang

Level: Fortgeschrittene

Dauer: 3 Tage

Format: Vorträge mit Hands-on Labs

Plattformen: Alle Palo Alto Networks Next-Generation Firewall Modelle, die unter PAN-OS laufen

Zielgruppe

Security Engineers, Security Administratoren, Security Operations Spezialisten, Security Analysten, Network Engineers und IT-Support

Voraussetzungen

Für diesen Kurs werden die Inhalte des Palo Alto Networks Firewall 8.x Essentials: Konfiguration und Management (EDU-210) vorausgesetzt. Zusätzlich sollten Sie fundierte, praktische Erfahrungen mit Netzwerksicherheitskonzepten sowie Routing, Switching und der IP Adressierung aufweisen. Darüber hinaus werden mindestens 9 Monate On-the-Job Erfahrung mit Palo Alto Networks Firewalls empfohlen.

Inhalte

Module 1: Tools and Resources

Module 2: CLI Primer

Module 3: Flow Logic

Module 4: Packet Captures

Module 5: Packet-Diagnostics Logs

Module 6: Host-Inbound Traffic

Module 7: Transit Traffic

Module 8: System Services

Module 9: SSL Decryption

Module 10: User-ID

Module 11: GlobalProtect

Module 12: Escalation and RMAs