


<b>Course Name</b>	<b>PCNSE - Palo Alto Networks Certified Network Security Engineer</b>	
<b>About the Course</b>	Design, deploy, configure, maintain, and troubleshoot Palo Alto Networks next-generation firewalls to protect networks from cutting edge cyber threats. The Palo Alto Networks Certified Network Security Engineer (PCNSE) recognizes individuals with in-depth knowledge and abilities to design, install, configure, maintain and troubleshoot the vast majority of implementations based on the Palo Alto Networks platform	
<b>Key Skills You Will Learn</b>	The Palo Alto Networks Certified Network Security Engineer (PCNSE) certification teaches skills related to designing, deploying, managing, and troubleshooting Palo Alto Networks firewalls. Some of the key skills you learn include: Firewall management, Security policies, Network traffic management, Threat prevention, VPN configuration, High availability, Security data interpretation, Firewall software maintenance, Traffic and routing optimization	
<b>Course Pre-Requisite</b>	There are no formal prerequisites for the Palo Alto Networks Certified Network Security Engineer (PCNSE) certification exam, but Palo Alto Networks recommends having the following knowledge and experience: A strong understanding of networking and cybersecurity, Extensive experience with Palo Alto security products, including PAN-OS, Panorama, and GlobalProtect , The ability to design, deploy, configure, maintain, and troubleshoot Palo Alto Networks Operating Platform implementations , A minimum of six months of hands-on experience with Palo Alto firewalls	
<b>Target Audience</b>	The PCNSE exam should be taken by anyone who wishes to demonstrate a deep understanding of Palo Alto Networks technologies, including customers who use Palo Alto Networks products, value-added resellers, pre-sales system engineers, system integrators, and support staff.	
<b>Job prospects with this role</b>	Cybersecurity / IT security. Security Engineer or Analyst, Security Architect, IT architecture and Design, Network Architect, Enterprise Architect. Cloud Architect, Infrastructure, Networking and Telecommunication. Network Engineer / Analyst / Technician	
<b>Course Duration</b>	~ 15 Hrs	
<b>Course Customisation</b>	Not applicable	
<b>Certification</b>	READYBELL PCNSE - Palo Alto Networks Security Engineer Certificate	
<b>Mode of Training</b>	Instructor-led 100% Online or 100% Classroom (Salt Lake, Kolkata - India) or hybrid mode (Online + Classroom) as suitable for the learner	
<b>Course Fees</b>	Please contact us	
<b>Refund Policy</b>	Get a 3-hours free trial during which you can cancel at no penalty. After that, we don't give refunds	
<b>Job Assistance</b>	Will assist candidate in securing a suitable job	
<b>Contact</b>	<b>READYBELL SOFTWARE SERVICES PVT. LIMITED</b> <b>AH 12, SALT LAKE SECTOR 2, KOLKATA (INDIA) - 700 091</b> <b>E-MAIL: <a href="mailto:contact@readybellsoftware.com">contact@readybellsoftware.com</a></b> <b>PH: +91 - 9147708045/9674552097, +91 - 33-79642872</b>	 Software Services Pvt. Ltd.

CURRICULUM		
Topic	Sub-Topic	Duration (Hrs)
<b>PCNSE - Palo Alto Networks Certified Network Security Engineer</b>	Module 1: Building a Palo Alto PCNSE Lab	15 Hrs
	Module 2: Configuring PA FW High Availability	
	Module 3: Using Template Stacks with Panorama	
	Module 4: Managing FWs with Panorama	
	Module 5: Managing PA FW Digital Certificates	
	Module 6: Enforcing Palo Alto FW User-ID	
	Module 7: Configure PA FW Admin Authentication	
	Module 8: Implement Routing on PA FWs	
	Module 9: Configure PA FW QoS	
	Module 10: Implementing PA FW L2 Interfaces	
	Module 11: Using PA FW Zone, Vulnerability, & DoS Protection	
	Module 12: Implementing PA FW Virtual Wires	
	Module 13: Configuring GlobalProtect Remote Access VPNs	
	Module 14: Implementing Palo Alto FW App-ID	
	Module 15: Configure PA FW Source and Destination NAT	
	Module 16: Configure PA FW VLAN, TAP, and Aggregate Interfaces	
	Module 17: Configuring PA FW Decryption Services	
	Module 18: Configure Static PA FW S2S VPNs	
	Module 19: Using PA FW S2S VPNs with Certificates	
	Module 20: Configure an IPsec VPN: PA FW to Cisco	
	Module 21: Using LSVPNs with GlobalProtect	
	Module 22: Using PA FW AV & WildFire	
	Module 23: Using Palo Alto ZTP	
	Module 24: Troubleshooting PA FW Routing	
	Module 25: Using PA FW Dynamic Groups	
	Module 26: Troubleshooting PA FW NAT	
	Module 27: Troubleshooting PA FW IPsec VPNs	
	Module 28: Troubleshooting PA FW Decryption	
	Module 29: Using PA FW Anti-Spyware	
	Module 30: Using IPv6 with PA FWs	
	Module 31: Using Palo Alto FW Authentication Portal	

**To register for this course please e-mail/call us**