Course Name	**Cisco Certified Network Professional (CCNP) Security**
About the Course	CCNP Security also known as professional level certification in Network Security discipline. This certification is basically meant for aspirants seeking career in the field of network security by using vendor specific devices like ASA firewalls, Switches and IPS Systems. This certification basically deals in making individuals well equipped with skillset required while handling complex security issues incurring in enterprise networks
Key Skills You Will Learn	The Cisco Certified Network Professional (CCNP) Security certification validates your skills and knowledge in securing Cisco networks. Some of the key skills you learn in CCNP Security include: Network security concepts, Secure network access, Endpoint security, Web and email security, Security incident response, Security policy and management, VPN technologies, Firewalls and IPS/IDS, Secure routing and switching, Network infrastructure security
Course Pre-Requisite	To become a Cisco Certified Network Professional (CCNP) Security expert, you should have the following skills and knowledge: Network security, Cisco Identity Services Engine, Extensible Authentication Protocols (EAP), Cisco clientless SSL VPNs, Cisco AnyConnect SSL, and IPsec VPNs, Ethernet and TCP/IP networking, Windows operating system, Cisco IOS networking and concepts, Security technologies, Security incidents, Network architectures
Target Audience	Cisco Network Security Engineer, Network Engineers, Network Administrators, IT professionals who wish to improve their knowledge and proficiency in securing Cisco networks
Job prospects with this role	Network security architect, Network security engineer, Network engineer, Network administrator, Network consultant, IT manager, Security specialist, Senior network engineer, Senior network architect
Course Duration	~ 60 Hrs
Course Customisation	Not applicable
Certification	READYBELL CCNP Security Certificate
Mode of Training	Instructor-led 100% Online or 100% Classroom (Salt Lake, Kolkata - India) or hybrid mode (Online + Classroom) as suitable for the learner
Course Fees	Please contact us
Refund Policy	Get a 3-hours free trial during which you can cancel at no penalty. After that, we don’t give refunds
Job Assistance	Will assist candidate in securing a suitable job
Contact	**READYBELL SOFTWARE SERVICES PVT. LIMITED** **AH 12, SALT LAKE SECTOR 2, KOLKATA (INDIA) - 700 091** **E-MAIL: contact@readybellsoftware.com** **PH: +91 - 9147708045/9674552097, +91 - 33-79642872** ReadyBell Software Services Pvt. Ltd.

CURRICULUM		
Topic	**Sub-Topic**	**Duration (Hrs)**
Cisco Certified Network Professional (CCNP) Security	**Cisco CCNP Security Core (350-701 SCOR)**	60 Hrs
	Module 1: Explain Common Threats Against On-premises and Cloud Environments	
	Module 2: Compare Common Security Vulnerabilities	
	Module 3: Components of Cryptography	
	Module 4: IPsec Fundamentals	
	Module 5: Cisco Router Site-To-Site VPNs	
	Module 6: Cisco Point-To-Point GRE over IPsec VPNs	
	Module 7: Cisco DMVPN	
	Module 8: Cisco GET VPN	
	Module 9: Cisco FlexVPN	
	Module 10: Cisco Remote Access VPNs	
	Module 11: 802.1X Fundamentals	
	Module 12: Debugging for IPsec Tunnels	
	Module 13: Configure ISE for 802.1X	
	Module 14: Security Intelligence	
	Module 15: Configure a Switch for 802.1X	
	Module 16: Explain APIs in the SDN Architecture	
	Module 17: DNA Center Foundations	
	Module 18: Configure Cisco TrustSec	
	Module 19: Interpret Basic Python Scripts used with Cisco Security	
	Module 20: Troubleshoot NetFlow	
	Module 21: The Components of Network Security Design	
	Module 22: Configure and Verify Cisco Port Security	
	Module 23: Configure and Verify Cisco DHCP Snooping	
	Module 24: Configure and Verify Cisco Dynamic ARP Inspection	
	Module 25: Private VLANS	
	Module 26: VRF-lite	
	Module 27: Network Infrastructure Device Hardening	
	Module 28: Additional Layer 2 Security	
	Module 29: EIGRP Neighbor Relationships and Authentication	
	Module 30: Troubleshoot OSPF Authentication for IPv4	
	Module 31: Troubleshoot OSPF Authentication for IPv6	
	Module 32: Firepower Access Control Policies	
	Module 33: Management Options to Improve Security	
	Module 34: Troubleshoot SNMP	
	Module 35: Troubleshoot Network Problems using Logging	

	Module 36: Capture and Redirection Methods	
	Module 37: Cisco Web Security	
	Module 38: Cisco Email Security	
	Module 39: Cisco Umbrella	
	Module 40: Understand and Configure AMP for Endpoints	
	Module 41: Explain Various Types of Endpoint Defenses	
	Module 42: Endpoint Security	
	Module 43: Describe Controls for End Users' Network Access	
	Module 44: Explain Exfiltration Techniques	
	Module 45: Explaining the Benefits of Streaming Telemetry	
	Module 46: Describing the Features of Various Cisco Security Offerings	
	Module 47: Planning for and Securing Cloud Platform	
	Module 48: Software Development Methodologies	
	Module 49: Securing Cloud Software-as-a-Service	
	Module 50: Securing Cloud Infrastructure-as-a-Service	
	Module 51: Securing Cloud Platform-as-a-Service	
	Cisco CCNP Securing Networks with Cisco Firepower (300-710 SNCF)	
	Module 52: Build a Cisco Firepower Lab in ESXi	
	Module 53: Build a Cisco Firepower Lab in VMware Workstation	
	Module 54: Build a Cisco Firepower Lab in EVE-NG	
	Module 55: Getting Started with Cisco Firepower	
	Module 56: Cisco Firepower Access Control Policy Fundamentals	
	Module 57: Cisco Firepower IPS/IDS	
	Module 58: Cisco Firepower SSL Decryption	
	Module 59: Cisco Firepower Malware and File Policies	
	Module 60: Cisco Firepower Security Intelligence	
	Module 61: Cisco Firepower High Availability	
	Module 62: Leveraging Identity in Cisco Firepower	
	Module 63: Upgrading Firepower	
	Module 64: Cisco Firepower VPNs	
	Module 65: Cisco Firepower Device and Platform Settings	
	Module 66: Cisco Firepower Integration	
	Module 67: Cisco Firepower Correlation Policies	
	Module 68: Firepower Troubleshooting	
	Module 69: Firepower Dashboards and Scheduling	
	Module 70: Firepower Audit Logging and Reporting	
To register for this course please e-mail/call us		