


Course Name	Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW) v1.0	
About the Course	This course helps you prepare to take the exam, Securing Networks with Cisco Firepower (300-710 SNCF), which leads to CCNP Security and Cisco Certified Specialist – Network Security Firepower certifications. The 300-710 SNCF exam has a second preparation course as well, Securing Networks with Cisco Firepower Next-Generation Intrusion Prevention System (SSFIPS)	
Key Skills You Will Learn	You will learn how to implement advanced Next-Generation Firewall (NGFW) and Next-Generation Intrusion Prevention System (NGIPS) features, including network intelligence, file type detection, network-based malware detection, and deep packet inspection. You will also learn how to configure site-to-site VPN, remote-access VPN, and SSL decryption before moving on to detailed analysis, system administration, and troubleshooting	
Course Pre-Requisite	Cisco recommends that you have the following knowledge and skills before taking this course: Technical understanding of TCP/IP networking and network architecture, Basic familiarity with firewall and IPS concepts	
Target Audience	The primary audience for this course is technical professionals who need to know how to deploy and manage a Cisco Firepower Threat Defense NGFW in their network environments. This class would be suitable for anyone who is replacing Cisco ASA devices with Cisco Firepower Threat Defense	
Job prospects with this role	Firewall engineers, senior security and network engineers, information technology managers, and network managers	
Course Duration	~ 40 Hrs	
Course Customisation	Not applicable	
Certification	READYBELL Cisco Firepower Next Generation Firewall (SSNGFW) v1.0 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	 Software Services Pvt. Ltd.

CURRICULUM		
Topic	Sub-Topic	Duration (Hrs)
Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW) v1.0	Module 1: Cisco Firepower Threat Defense Review	40 Hrs
	Research and comparison of NGFW and NGIPS technologies	
	Cisco Firepower Features and Components	
	Comparison of Cisco Firepower Platforms	
	Steps to Implement Cisco Firepower on a Network	
	Module 2: Configuring Cisco Firepower NGFW	
	Registering a Cisco Firepower Device	
	FXOS and Firepower Device Manager	
	Primary settings	
	NGFW Device Management	
	Policy research	
	Working with objects	
	System settings and monitoring of device health indicators	
	Device management	
	Resiliency Research	
	Migration from Cisco ASA to Firepower	
	Migration from Cisco ASA to Cisco Firepower Threat Defense	
	Module 3: Traffic control in Cisco Firepower NGFW	
	Package Processing	
	Implementation of QoS	
	Transmitting traffic without checking	
	Module 4: Address translation in Cisco Firepower NGFW	
	What is NAT	
	Implementation of NAT	
	Examples of NAT rules	
	Module 5: Exploring the Key Features of Cisco Firepower	
	Network analysis	
	Setting up a network analysis policy	
	Implementing Access Control Policies	
	Default action	
Connection events		
Advanced access control policy settings		
Module 6: Security Intelligence		
Security Intelligence Objects		
Implementation of Security Intelligence and log analysis		

Module 7: File control and advanced malware protection	
Malware detection and file policy	
Advanced Malware Protection	
Module 8: Intrusion Prevention Systems	
Snort Rules	
Variables and lists of variables	
Intrusion policy	
Module 9: Site-to-Site VPN	
IPsec Overview	
Setting up Site-to-Site VPN	
Troubleshooting Site-to-Site VPN	
Implementation of Site-to-Site VPN	
Module 10: Remote-Access VPN	
Research of Remote-Access VPN mechanisms	
Certificates and Public Key Infrastructure	
Certificate signing process	
Remote-Access VPN Settings	
Implementing Remote-Access VPN	
Module 11: Decryption of SSL traffic	
Opportunity Research	
Setting up an SSL policy	
Best practices and recommendations	
Monitoring	
Module 12: Data Analysis	
Event Analysis	
Event Types	
Contextual information	
Event Analysis Tools	
Threat Analysis	
Module 13: System administration	
Software update management	
Account Management	
System administration	
Module 14: Troubleshooting Cisco Firepower	
Common settings mistakes	
Troubleshooting Commands	
System troubleshooting process	
To register for this course please e-mail/call us	