Indian Financial Technology & Allied Services Job Description			
I		Role Summary	Remarks
	(a) Title:	Sr. Security Analyst -Firewall Operations	L2
	(b) Business/Function:	Cyber Security	
	(c) Band / Designation:	Security Analyst	
	(d) Location:	Mumbai/Hyderabad	
	(e) Reports to:		
	(f) Team:	Cyber Security	
	(g) Summary:	1) The candidate will be supporting the Firewall,security solutions & reporting. 2) The Candidate will be managing the FW operations & day-to-day activity.	
	(h) Position Code:		
II		Additional Information	
	(a) Responsibilities:	•Configuration, Management & troubleshooting of Firewalls, IPS. •Expert to administer the day-to-day checkpoint firewall & IPS operational issues. •Involve in change management process for HW replacement/ Config change/ SW upgrade/ FW Rules management etc. •Troubleshoot and resolve any hardware, software or configuration related incidents. •Responsible for preparing Method of Procedure for any configuration changes and executing any configuration changes as per approval. •Responsible for leading any planned scheduled maintenance activities. •Able to lead any incident calls with OEM technical support and provide any inputs required for restoration. •Key Spoc for Incident & Change Management •Effective Ticket handling, Monitor the queue and maintain regular updates on the Tickets as per agreed timeline, providing the detailed closure summary on the tickets. •Co-ordination with teams and providing timely updates whenever required.	
III		Requirements	Classification
	(a) Education:	BSC / Diploma in computer science with relevant experience in Information Security or Network Security. or BE/B tech/Computer Science.	
	(b) Experience:	1)Candidate should have strong 4 + years of overall experience as a Network/Security Engineer either in Service Provider Environment or diverse enterprise network. 2)Troubleshooting experience on IPS and IDS. 3)Implementation & Troubleshooting experience on industry standard protocols/Technology including IPSEC VPN, SSL, Clientless VPN , Clustering, URL Filtering. 4)Implementation and Troubleshooting experience on Next generation firewalls specifically Check point, Palo alto, FortiGate. 5)Implementation and Troubleshooting experience on IPS and IDS. 6)Troubleshooting experience on industry standard protocols/Technology including 7)IP Nat, ACL, Packet capture. 8)Network setting :- Zone,Security policy,NAT polices, tunnel interface, virtual Routers 9)IPSEC VPN : Clientless VPN , Site to Site, client based, etc. 10)High Availability: Clustering, Active /Active, Active/Standby.	
	(c) Certifications:	1) Check Point Certified Security Administrator (CCSA) 2) Any Firewall certification will be added advantage. - Preferrable	
	(d) Knowledge:	1) Expert knowledge in Network & Security. 2) In-depth understanding and experience (Firewall/IPS/IDS/VPN) 4)Knowledge of Analysis of IPSec VPNs implementation and Manage and Monitor all VPN connectivity. 5)Knowledge of Analyse, troubleshoot, and investigate Firewall related issues.	
	(e)Technical Skills:	Primary Mandatory Skills: Experience in Firewall,IPS,IDS,VPN,Routing Switching Secondary Desirable Skills: Understanding of Proxy, LB, AV, VA & other security solutions.	