Indian Financial Technology & Allied Services		
Job Description		
	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:		
() 6 (1.00)	Additional Information	
(a) Responsibilities:	*Bonfiguration, 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. 	
	*nesponsible for leading any planned scheduled maintenance activities.	
	*Ribe to lead any incident calls with OEM technical support and provide any inputs required for restoration.	
	• Key Spot 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.	
II .	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	
(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.	
(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)Trouble-brooting experience on IPS and IDS.	
(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	
(b) Experience:	Clandidate should have strong 4 + years of overall experience as a Network/Security Engineer either in Service Provider Environment or diverse enterprise network. Clandidate should experience on IPS and IDS. Clandidate should be should	
(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)Trouble-shooting experience on IPS and IDS. 3)Implementation & Trouble-shooting experience on industry standard protocols/Technology including IPSEC VPN, SSL, Clientless VPN, Clustering, URL Filtering. 4)Implementation and Trouble-shooting experience on Next generation firewalls specifically Check point, Palo alto, FortiGate.	
(b) Experience:	Clandidate should have strong 4 + years of overall experience as a Network/Security Engineer either in Service Provider Environment or diverse enterprise network. Clandidate Shoulding experience on IPS and IDS. Clandidate Shoulding experience on IPS and IDS. Clandidate Shoulding experience on IPS and IDS. Clandidate Shoulding Experience on Industry standard protocols/Technology including IPSEC VPN, SSL, Clientless VPN, Clustering, URL Filtering. Climplementation and Troubleshooting experience on Next generation firewalls specifically Check point, Palo alto, FortiGate. Simplementation and Troubleshooting experience on IPS and IDS.	
(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)Trouble-shooting experience on IPS and IDS. 3)Implementation & Trouble-shooting experience on industry standard protocols/Technology including IPSEC VPN, SSL, Clientless VPN, Clustering, URL Filtering. 4)Implementation and Trouble-shooting experience on Next generation firewalls specifically Check point, Palo alto, FortiGate. 5)Implementation and Trouble-shooting experience on IPS and IDS. 6)Trouble-shooting experience on industry standard protocols/Technology including	
(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)IPN state, ACL, Packet capture.	
(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)Trouble-shooting experience on IPS and IDS. 3)Implementation & Trouble-shooting experience on industry standard protocols/Technology including IPSEC VPN, SSL, Clientless VPN, Clustering, URL filtering. 4)Implementation and Trouble-shooting experience on Next generation firewalls specifically Check point, Palo alto, FortiGate. 5)Implementation and Trouble-shooting experience on IPS and IDS. 6)Trouble-shooting 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	
(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)Trouble-shooting experience on IPS and IDS. 3)Implementation & Trouble-shooting experience on industry standard protocols/Technology including IPSEC VPN, SSL, Clientless VPN , Clustering, URL Filtering. 4)Implementation and Trouble-shooting experience on Next generation firewalls specifically Check point, Palo alto, FortiGate. 5)Implementation and Trouble-shooting experience on IPS and IDS. 6)Trouble-shooting experience on industry standard protocols/Echnology including 7)IP Nat, ACL, Packet capture. 8)Network setting: 2 cone, Security policy, NAT polices, tunnel Interface, virtual Routers 9)IPSEC VPN, ICIENTIES VPN, Site to Site, Client based, etc.	
	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)Ingle Neuralbility: Custering, Actor (Actor) Ac	
(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)Trouble-shooting experience on IPS and IDS. 3)Implementation & Trouble-shooting experience on industry standard protocols/Technology including IPSEC VPN, SSL, Clientless VPN , Clustering, URL Filtering. 4)Implementation and Trouble-shooting experience on Next generation firewalls specifically Check point, Palo alto, FortiGate. 5)Implementation and Trouble-shooting experience on IPS and IDS. 6) Trouble-shooting experience on industry standard protocols/Technology including 7)IP Nat, ACL, Packet capture. 8)Network setting: - Zone, Security policy, NAT polices, turnuel interface, virtual Routers 9)IPSEC VPN. I Clientless VPN. Nite to Site, client based, etc. 10)Injel Availability: Clustering, Active /Active/Standby. 1) Check Point Certified Security Administrator (CCSA) 2) Any Firewall	
(c) Certifications:	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)IPN sta. ACL, Packet capture. 8)Network setting: -Zone, Security policy, NAT polices, tunnel interface, virtual Routers 9)IPSEC VEN, Clientless VPN, Site to Site, Client based, etc. 10)Vegih Availability: Clistering, Active /Active, Active/Standby. 1) Check Point Certified Security Administrator (CCSA) 2) Any Firewall certification will be added advantage Preferrable	
	Special State Special Stat	
(c) Certifications:	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)Trouble-shooting experience on IPS and IDS. 3)Implementation & Trouble-shooting experience on industry standard protocols/Technology including IPSEC VPN, SSL, Clientless VPN , Clustering, URL Filtering. 4)Implementation and Trouble-shooting experience on Next generation firewalls specifically Check point, Palo alto, FortiGate. 5)Implementation and Trouble-shooting experience on IPS and IDS. 6)Trouble-shooting experience on industry standard protocols/Technology including 7)IPN standard, Packet capture. 8)Metwork setting: -Zone, Security policy, NAT polices, tunnel interface, virtual Routers 9)Mescry CNF. Clientess VPN, Site to Site, client based, etc. 10)High Availability: Clustering, Active /Active Active/Standby. 1) Check Point Certified Security Administrator (CCSA) 2) Any Firewall certification will be added advantage Preferrable 1) Expert knowledge in Network & Security. 2) In-depth understanding and experience (Firewall/IPS/IDS/VPN)	
(c) Certifications:	3)Candidate should have strong 4 + years of overall experience as a Network/Security Engineer either in Service Provider Environment or diverse enterprise network. 2)Trouble-shooting experience on IPS and IDS. 3)Implementation & Trouble-shooting experience on industry standard protocols/Technology including IPSEC VPN, SSL, Clientiess VPN, Clustering, URL Filtering. 4)Implementation and Trouble-shooting experience on Next generation firewalls specifically Check point, Palo alto, FortiGate. 5)Implementation and Trouble-shooting experience on IPS and IDS. 6)Introuble-shooting experience on industry standard protocols/Technology including 7)IP Nat, ACL, Packet capture. 8)Network setting - Zone, Security policy, NATs polices, tunnel interface, virtual Routers 9)PSEC VPN : Cientless VPN, Jist to Sitz, client based, etc. 10)Ingly Availability: Custering, Active /Active, Active/Standby. 1) Check Point Certified Security, Administrator (CCGA) 2) Any Firewall certification will be added advantage Preferable 1) Expert Knowledge in Network & Security, 2) In-depth understanding and experience (Firewal)(IPS/IDS/VPN) 4)Knowledge of Analysis of IPSe-VPN implementation and Manage and Monitor all VPN connectivity.	
(c) Certifications:	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)Trouble-shooting experience on IPS and IDS. 3)Implementation & Trouble-shooting experience on industry standard protocols/Technology including IPSEC VPN, SSL, Clientless VPN , Clustering, URL Filtering. 4)Implementation and Trouble-shooting experience on Next generation firewalls specifically Check point, Palo alto, FortiGate. 5)Implementation and Trouble-shooting experience on IPS and IDS. 6)Trouble-shooting experience on industry standard protocols/Technology including 7)IPN standard, Packet capture. 8)Metwork setting: -Zone, Security policy, NAT polices, tunnel interface, virtual Routers 9)Mescry CNF. Clientess VPN, Site to Site, client based, etc. 10)High Availability: Clustering, Active /Active Active/Standby. 1) Check Point Certified Security Administrator (CCSA) 2) Any Firewall certification will be added advantage Preferrable 1) Expert knowledge in Network & Security. 2) In-depth understanding and experience (Firewall/IPS/IDS/VPN)	
(c) Certifications:	3)Candidate should have strong 4 + years of overall experience as a Network/Security Engineer either in Service Provider Environment or diverse enterprise network. 2)Trouble-shooting experience on IPS and IDS. 3)Implementation & Trouble-shooting experience on industry standard protocols/Technology including IPSEC VPN, SSL, Clientiess VPN, Clustering, URL Filtering. 4)Implementation and Trouble-shooting experience on Next generation firewalls specifically Check point, Palo alto, FortiGate. 5)Implementation and Trouble-shooting experience on IPS and IDS. 6)Introuble-shooting experience on industry standard protocols/Technology including 7)IP Nat, ACL, Packet capture. 8)Network setting - Zone, Security policy, NATs polices, tunnel interface, virtual Routers 9)PSEC VPN : Cientless VPN, Jist to Sitz, client based, etc. 10)Ingly Availability: Custering, Active /Active, Active/Standby. 1) Check Point Certified Security, Administrator (CCGA) 2) Any Firewall certification will be added advantage Preferable 1) Expert Knowledge in Network & Security, 2) In-depth understanding and experience (Firewal)(IPS/IDS/VPN) 4)Knowledge of Analysis of IPSe-VPN implementation and Manage and Monitor all VPN connectivity.	
(c) Certifications: (d) Knowledge:	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)Trouble-shooting 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 Ns. Act, CL, Packet capture. 8)Network setting: - Zone, Security policy,NAT polices, tunnel Interface, virtual Routers 9)IPSEC VPN. 1; Clientless VPN, Site to Site, client based, etc. 10)Ingip Availability: Clustering, Active /Active /Active/Standby, 1) Check Point Certified Security Administrator (CCSA) 2) Any Firewall 1) Expert knowledge in Network & Security. 2) In-deepth understanding and experience (Firewall/IPS/IDS/VPN) 4)Knowledge of Analysis, troubleshoot, and investigates Frewall related issues.	
(c) Certifications: (d) Knowledge:	Special State Special Stat	