ANNEXURE – A - Technical Bid

S. No.	Firewall Appliances specifications	Compliance (YES/NO)	**Reference** (URL Address with page no. / data sheet with page no.)
1. VENDOR ELIGIBLITY CRITERIA:			
1	The Vendor should have office at Chennai with experts / specialists to handle Installation, Configuration and solving all types of issues in time.**[Self Declaration]**		
2	MAF - Manufacturer Authorization Form to be attached for the quoted specification**[MAF to be attached for Firewall and Tranceiver modules]**		
2. TECHNICAL REQUIREMENT:			
	Specify the proposed solution Brand name, Model no., Supporting software packages details		
1	The Proposed solution should be leaders in the latest (2018) gartnermagic quadrant for enterprise firewall. **[Gartner Certificate to be attached]**		
2	Should be recommended in NSS Labs, NGFW 2017 / 2018 **[NSS Certificate to be attached]**		
3	Should have exploit block rate of above 95% in NSS Labs NGFW 2018 **[NSS Certificate to be attached]**		
4	Should be passed in NSS labs ngfw 2017/2018 evasion testing and it Should be blocked all 190 out of 190 evasions **[NSS Certificate to be attached]**		

5	The appliance-based security platform should be capable of providing firewall, application visibility, IPS, Antivirus / Zero-day protection, Antibot, Antispam, Web filtering, DLP (Data Leak Protection), IPSEC VPN and SSL VPN.		
6	The appliance should have dual power supply unit for redundancy		
7	Appliance should have minimum power Consumption and power consumption value should be mentioned in the data sheet.		
8	Appliance should support UTP, SFP, SFP+, QSFP28		
9	The appliance should have at least 4 x 1G UTP, 6 x 10G Fiber port compatible to 10 G SFP+, 4 x 40G QSFP28 Interfaces.		
10	The appliance should support 15,000 users and 35,000 devices		
11	Proposed platform should have future scalability and capability to deliver minimum of 100 Gbps Threat Protection throughput.		
12	The Appliance should support firewall throughput (FW+AVC+AV / Zero-day protection +IPS) of 50 Gbps or more. (or)The Appliance should support SSL Inspection Throughput (IPS, HTTP) : 90 Gbps or moreThe Appliance should support Application control throughput (HTTP 64K) : 150 Gbps or moreThe Appliance should support NGFW throughput : 90 Gbps or more The Appliance should support Threat		

	Protection throughput : 50 Gbps or more The Appliance should support IPS throughput of 110 Gbps		
13	The Appliance should support Concurrent sessions (TCP) : 30 millions or more		
14	The Appliance should support New sessions per sec (TCP) : 300 K or more		
15	The Appliance should support IPSEC VPN throughput : 15 Gbps or more		
16	Device should support at least 1000 VLANs		
17	Appliance should support 20,000 or more concurrent ssl VPN users		
18	Appliance should support 15,000 client to site and site to site VPN		
19	Appliance should have 1 TB or more internal storage		
20	The appliance should have network cards and processing cards for better availability and performance		
21	Device should support creating access rules with IPv4 & IPv6 objects simultaneously from day 1		
22	Should support Static, RIP, OSPF, OSPFv3 and BGP		
23	Appliance should support manual NAT		
24	The appliance should support DHCPv6		
25	The appliance should support Multicast protocols like IGMP, PIM, etc.		
26	The system should supports SNMP Versions 1, 2c and 3		

27	The appliance should support security policies based on group names in source or destination fields or both		
28	The appliance should support capability to limit bandwidth on basis of apps/groups, Networks / Geo, Ports, etc.		
29	The appliance should support Stateful firewall inspection		
30	Appliance should support Active/Standby and Active/Active fail over		
31	Appliance should support FQDN policy based routing		
32	The appliance should be capable of tuning IDS/IPS, AV, URL Filtering (ex., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.		
33	The appliance Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.		
34	The appliance should be able to link Active Directory and LDAP user names to IP addresses related to suspected security events.		
35	The appliance should have inbuilt anti virus detection and should be able to quarantine the IP for a defined duration and should be able to restrict access of infected host . The Solution should prevent malware based threats.		

36	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor		
37	The appliance must support URL and DNS threat feeds to protect against threats		
38	The appliance should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 65 categories from day one		
39	The appliance should support more than 2500 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.		
40	The Appliance OEM must have its own threat intelligence analysis centre and should use the global footprint of security deployments for more comprehensive network protection.		
41	The detection engine should have the capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).		
42	The appliance should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location		

43	The proposed solution should support AAA solution for user authentication		
44	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques. Support to Identify and explain each type of detection mechanism.		
45	The device should have inbuilt antibot and should prevent clients from contacting C&C		
46	The appliance should not allow clients contacting malware infected domains		
47	Appliance should be able to share threat intelligence with other security components in the network natively		
48	Solution should have inbuilt application control		
49	Solution should support policy based routing to provide better user experience		
50	Solution should support scanning the files for threats with file size starting from KB to 500 MB.		
51	The appliance should support interface based polices and should have policy for multiple interfaces bundled together		
52	Should have inbuilt DNS filter to provide DNS based security		
53	Should have integration for Domain and IP Reputation based protection		

54	Solution should be able to exchange threat intelligence with other components like WAF/NAC/SIEM etc		
55	Solution should support device based / IP based restriction		
56	Proposed solution should have SSL/SSH inspection		
57	Should be able to download and update firmware from the firewall		
58	The management must be accessible via web-based interface without any additional client software		
59	The management solution must be capable of role-based administration		
60	The proposed solution should have dedicated management and reporting solution / Analyzer for accessing up to 10 TB or more of syslog files		
61	The analyzer / reporting solution must provide multiple report output types or formats, such as PDF, HTML, and CSV.		
62	The analyzer / reporting solution must have reporting function to perform a detailed search on User Account with Downloadable format in PDF, HTML, CSV. It should support search options (User name, IP Address, Time zone)		
63	The solution must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).		

64	The solution must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.		
65	The solution must provide risk reports like advanced malware attacks		
66	Appliance Should support REST/API to support API integration		
67	Appliance should have inbuilt web management for configuring polices, objects etc		
68	The solution should support COA (Change of Authorization) functionality to integrate with AAA to restrict users based on data used (User based quota management).		
69	The Proposed solution should have bandwidth restriction in web filtering to allocate certain bandwidth per user per day		
70	Message should be displayed to the blocked user that he exceeded his daily quota of data assigned		
71	The proposed solution should have AAA solution		

72	All performance numbers mentioned in the data sheet should be arrived by: 1) Enabling scan of all packets by IPS & Anti-Virus/zero-day protection 2) IPS to scan all parts of session in both direction 3) AV to scan the complete payload 4) Complete Threat Prevention signatures to be enabled.		
73	Data sheet should be submitted as proof for all specifications		
74	Lab. Test report of Firewall throughput should be submitted after enabling(i) SSL Inspection Throughput (IPS, AV, HTTP) : 90 Gbps(ii) Application Control Throughput (HTTP 64K) : 150 Gbps(iii) Threat Prevention Throughput : 50 Gbps**[Lab Test Report to be attached]**		
75	Product supplied should be directly installed by OEM professionals / OEM Certified professionals.		
76	Supplied products and licenses should be supported for 5 years warranty from the date of Installation completion by OEM		
	Authentication, Authorization, and Accounting (AAA) Specification		
1	Proposed AAA solution should be an Appliance/VM based solution. OEM should include the required software and license to install on VM. The no. of cores, Memory and storage space required should be specified.		

2	Proposed solution should include AAA Solution and provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization and accounting (AAA) and profiling.		
3	The proposed solution should have Built-in user database with per device/user credential management and should also provide Seamless back end integration with Active Directory, LDAP(open LDAP). Should have capability to authenticate with open LDAP using captive portal.		
4	The appliance should support user to remove his authenticated devices / IP's.		
5	The AAA solution should have SSO integration with the NGFW		
6	The system should show the user statistics in dashboard to display the latest data on the number of different users with different statuses(Authenticated, connected, Active, Pending Approval, Rejected, suspended, Expired users)		

7	System should provide a way to give levels of time access to different User accounts and also a level of Data Usage • Data Upload - Apply a Data Usage upload restriction to user, and the usage should be determine in KB, MB or GB. • Data Download - Apply a Data Usage download restriction to user and the usage should be determine in KB, MB or GB. • Total Upload & Download - Apply a Total Data Usage restriction to user and the usage should be determine in KB, MB or GB.		
8	The appliance should able to run a report on successful or failed LDAP Authentications		

SIGNATURE OF TENDERER
ALONG WITHSEAL OF
THE COMPANY WITH DATE