SUPREME COURT OF INDIA
ADMN. MATERIAL (P&S)

F. No.: Data Center/2019
Dated: 15th February, 2020

Last date for Submission of Tender: 6th March, 2020 up to 03:00 p.m.

NOTICE INVITING TENDER FOR SUPPLY & INSTALLATION OF MODULAR RACK, RACK SERVERS WITH VMWare, Windows 2012 Server R2 Std, DDOS,

Next Generation Firewall, Anti APT Appliance, Server Load Balancer, Web Application Firewall, SAN Switch, etc.)

Sealed tenders are invited for supply of MODULAR RACK, RACK SERVERS WITH VMWare, Windows 2012 Server R2 Std, DDOC in HA, Firewall in HA, Anti APT Appliance (Single), Server Load Balancer in HA, WAF in HA, SAN Switch etc. as per Proformas enclosed herewith at **Annexure-'A' and 'D'**. Tenderers are advised to **visit the Registry on 24th February, 2020 at 11:00 a.m. for Pre Bid Meeting** being convened to clarify doubts and queries regarding the use of aforesaid items, before finally submitting their bids on or before the last date mentioned in this document.

Interested parties, if so desire, may contact Ms. Padma Sundar, Branch Officer, Admn. Material (P&S) telephonically or personally visit at Reception Counter No.42 for any clarification on any working day between 10.30 A.M. and 4.00 P.M. (except Saturdays & holidays) on Telephone Nos. 23111483 and 23112235.

A. TENDER

1. The tender should be sent in Three Sealed Envelopes superscribed with (a) “Earnest Money for Data Center Hardware”, (b) “Technical Bid for Data Center Hardware” and (c) “Financial Bid for Data Center Hardware” by post sufficiently early so as to reach the Registry within date and time or may be delivered to the undersigned. If tender is sent through Special Messenger, an authority

letter from the tenderer with proof of identity may also be given to the Messenger so that he/she could show the same along with his/her own identity proof to the Reception Officer at Reception Counter No.42 for issuance of entry pass.

2. The tenderers are expected to examine all the instructions, Proformas, terms

   & conditions and specifications in the tender documents. Failing to furnish all information required by the tender document in any respect will be at the tenderer's risk and may result in the rejection of the tender.

3. The tender must be received not later than the date & time specified for submitting the same. In case, the date of submitting the tender will be declared as holiday by the Govt. of India then next working day of the Registry will be treated as due date of Tender.

B. TERMS AND CONDITIONS OF TENDER & QUALIFICATION CRITERIA FOR BIDDERS

1. The bidders are required to quote their lowest rate per unit for supply of Data Center Hardware in **Annexure-'D'** along with Four resident engineers, technology specific(certified-mentioned below) for one year to manage the hardware with required configuration changes time to time. Enclosed herewith and the rates should be valid for a period of 60 days from the date of opening of Tenders. The bidders shall not be entitled during the said period of 60 days to revoke or cancel its tender or to vary the tender or any terms thereof.

2. The bidders are required to send their tender along with Demand Draft drawn in favour of ''The Registrar (Admn), Supreme Court of India "towards **Earnest Money Deposit of Rs. 20,000/-** for supply of Data Center Hardware (Name of the firm, telephone number and name of the item may be written on the reverse side of the Demand Draft). No interest will be payable on EMD. If EMD is exempted, Certificate has to be submitted along with the tender documents.

3. Earnest Money Deposit of bidders would be returned by way of RTGS/NEFT or cheque after the contract has been finally awarded to the successful bidder. A copy of cancelled cheque is required to facilitate refund of EMD amount.

4. Hypothetical or conditional Tender shall not be entertained. Tender once submitted shall not be allowed to be withdrawn or altered. If the tender is withdrawn or altered by the concerned party at any time after it is submitted, EMD submitted by tenderer may be confiscated and in future the tenderer may be debarred to participate in the tender process of the Supreme Court.

5. The Registry will deal with the bidders directly and no middlemen/commission agents etc. should be asked by the bidders to represent the cause and they will not be entertained by the Registry.

6. Over-writing/over-typing or erasing of the figures which render the tender doubtful or ambiguous are not allowed and shall render the tender invalid.

7. The Registry, in its discretion, reserves the right to reject or accept any or all bidders, partly or completely, at any time without assigning any reason thereof.

8. Each bidder has to certify that all the terms and conditions are acceptable to him.

9. **The bidders are advised to visit the Registry on 24th February, 2020 at 11:00 a.m. for a Pre Bid Meeting to be convened by Sr. Director(CERT-IN), Sr. Technical Director(NIC), Member(eCommittee), Addl. Registrar(Computer Cell) and IT Consultant(Computer Cell) before finally submitting their bids on or before the last date mentioned in this document.**

10. Bidders are required to fill the Technical Specifications Compliance Sheet as at **Annexure- 'C'**. Financial Bids of only the technically-qualified tenderers shall be opened.

11. Notwithstanding the scope of work, engineering, supply and services stated in bid document, any equipment or material, engineering or technical services which might not be even specifically mentioned under the scope of supply of the bidder and which are not expressly excluded there from but which – in view of the bidder - are necessary for the performance of the equipment in accordance with the specifications are treated to be included in the bid and has to be performed by bidder. The items which are over & above the scope of supply specified in the Schedule of Requirements may be marked as "Optional Items".

12. The Bidder shall submit all necessary documentary evidence to establish that the Bidder meets the above qualifying requirements.

13. Bidder last three-year turnover average must be 250cr or more, ending 31st March 2019.

14. One similar completed work costing not less than ₹ 10 Cr.
OR two similar completed works each costing not less than ₹ 6 Cr.
OR 3 similar completed works each costing not less than ₹ 5 Cr.

Note: Executed amount of completed work orders (single/two/ three) as mentioned above is exclusive of service tax and according executed value of the job excluding service tax shall be considered for evaluation of QC.

15. The hardware shall be delivered, installed and commissioned in full at the site within Weeks (8) weeks from the date of PO/LOI. Thereafter the hardware shall be handed over to the owner as per the relevant clauses above. Partial delivery and installation, if necessary, shall be allowed only with prior approval of the owner

16. The bidders should be an Authorized Dealer/Distributor of the OEM of offered product. (Please submit manufacturer's authorization letter, in original, on the OEM's letter head duly signed by authorized signatory).

17. Certificates from the end user/ Owner/ Consultant of the owner stating that they have been allowed/ permitted as a sub- contractor.

18. The software licenses, if any, shall be required in the name of Registrar, Supreme Court of India. The licenses shall contain paper licenses and at least one set of media (CDs), wherever applicable.

19. SCI, Registry reserves the right to levy penalty @ of 0.5 % of value of the unexecuted portion of the order, per week of delay beyond the time schedule stipulated in the order, subject to maximum of 10 % of the value of unexecuted portion of order. SCI, Registry reserves the right to cancel the order in case the delay is more than 5 weeks.

The delay in delivery and/or installation not attributed to supplier viz. delay in site preparation, delay in submission of required documents (by SCI, Registry) etc. and the conditions arising out of Force Majeure will not be considered for the purpose of calculating penalties.

20. The Bidder is required to quote for the complete BOQ. Partial quote is liable to be rejected.

21. The Bidder should be a public/private limited company registered under Companies Act, 1956 for a minimum period of five years in India.

22. The Bidder should be a profit-making company in at least three of the last five financial years 2014-15, 2015-16, 2016-17, 2017-18, 2018-19.

23. The Bidder should have a valid Registration/VAT/Service tax Certificate, PAN Card and should be registered with the appropriate authorities for all applicable statutory taxes/duties in India.

24. The Bidder should have at least one certified on direct payroll expert of these each certification: Certified Information Security Manager (CISM), Cisco Certified Internetwork Expert (CCIE), PRINCE2 Practitioner & VMware Certified Professional with a valid certificate till the last date of bid submission.

25. Vendor shall provide comprehensive on-site warranty for trouble free operation of hardware for a minimum period of five years after commissioning and successful testing and taking over. During this period, it will be the responsibility of the vendor to maintain and support the hardware fully and ensure availability of the same. The Vendor shall be responsible for providing, free of cost, all supplies, spares and services necessary for maintenance during warranty.

26. The vendor shall procure all the equipment's from genius sources as approved by the company and as per company specification

27. The vendor shall arrange for standby equipment, if the faulty equipment is not rectified within two working days or machines/accessories are taken out of customer premises for servicing/ repair.

28. The Vendor shall provide periodic preventive maintenance during the warranty including cleaning or periodic inspection. The detailed scope of services/preventive maintenance schedule recommended shall be furnished by the vendor and shall be finalized in consultation with SCI Computer cell.

29. The vendor has to provide detailed project reports with all document including warranty cards, licenses hardcopies, etc. The vendor

30. The vendor will provide single point of contact detail with escalation metric & SLA's agreed by the SC registry with all penalty clauses.

31. The vendor shall be responsible for all risk to the works to be performed under its obligation under the Contract and for trespassers, and shall make good at his own expenses all losses and damages whether to the works, themselves, or to any other property of the company or the lives, persons or property of other forms, whatsoever cause, in connection with the works, although all reasonable and proper precautions may have been taken by the contractor, and in case registry is called upon to make good any such costs, loss or damages or to pay compensation to any person(s) sustaining damages by reason of any act, or any negligence or omission on the part of the vendor, the amount of any costs or charges (including costs and charges towards legal proceedings) which the Company may incur in reference thereto,

shall be charged to the vendor. The vendor shall reimburse such costs immediately to the registry.

32. All materials received at site shall be accompanied by the Test certificate of the manufacturer. The Officer-In-Charge reserves the right to instruct any material to be further tested in an approved laboratory for which the Contractor shall make no additional claims. Where ever test requirements are not specified in the specifications relevant IS code of practice shall govern.

33. Vendor will ensure that the Environment, Health & Safety (EHS) requirements are clearly understood and faithfully implemented at all levels at site as per instruction of Company. Contractors must comply with these requirements:

a) Comply with all of the elements of the EHS Plan and any regulations applicable to the work.

b) Comply with the procedures provided in the interests of Environment, Health and Safety.

c) Ensure that all of their employees designated to work are properly trained and competent.

d) Ensure that all plant and equipment they bring on to site has been inspected and serviced in accordance with legal requirement and manufacturer's or suppliers' instructions.

e) Make arrangements to ensure that all employees designated to work on or visit the site present themselves for site induction prior to commencement of work.

f) Provide details of any hazardous substances to be brought onsite.

g) Ensure that a responsible person accompanies any of their visitors to site.

All Contractor/workers are accountable for the following:

1. Use the correct tools and equipment for the job and use safety equipment and Protective clothing supplied, e.g. helmets, goggles, ear protection, etc. as instructed.

2. Keep tools in good condition.

3. Report to the Supervisor any unsafe or unhealthy condition or any defects in plant or equipment.

4. Develop a concern for safety for themselves and for others.

5. Not to operate any item of plant unless they have been specifically trained and are authorized to do so.

34. The bidder shall provide training for installation and maintenance to staff of the purchaser free of cost where required. The bidder shall specify in his bid the number of trainees, quantum of proposed training, pre-training qualifications required of the trainees and duration of the proposed training. The bidder shall provide all training material and documents. Conduct of training of the purchaser's personnel shall be at the on-site in assembly start-up operation, maintenance and/or repair of the supplied goods.

35. If the vendor needs to carry out any work or rework due to change in drawings or structural consultants' instructions, the vendor shall take the prior permission of the registry before commencing such works.

36. The vendor at its own cost shall also arrange, secure and maintain the insurance covers of hardware & manpower provided.

37. Vendor design the guidelines shared here with end-to-end tight integration of all data center devices. Supply and installation of all the hardware items as per the scope detailed.

38. Vendor shall furnish the Part no./ Product identification number for all products as provided by the original manufacturer.

39. The disputes, legal matters, court matters, if any shall be subject to Delhi jurisdiction only.

40. SCI, Registry reserves the right to increase or decrease up to 25% of the quantity of goods and services specified in the schedule of requirements as per NIT, without any change in the unit price or other terms and conditions at the time of award of contract.

a SCI, Registry also reserves the right for placement of additional order or up to 50% of the additional quantities of goods and services contained in this running tender/contract within a period of twelve months from the date of acceptance of first PO in the tender at the same rate or a rate negotiated (downwardly) with the existing vendors considering the reasonability of rates based on prevailing market conditions and the impact of reduction in duties and taxes etc. and supplies to be obtained within delivery period scheduled a fresh.

b In exceptional situation where the requirement is of an emergent nature and it is necessary to ensure continued supplies from the existing vendors, the purchaser reserves the right to place repeat order up to 100% of the quantities of goods and services contained in the running tender/contract within a period of twelve months from the date of acceptance of first PO in the tender at the same rate or a rate negotiated (downwardly) with the existing vendors considering the reasonability of rates based on prevailing market conditions and the impact of reduction in duties and taxes etc. Exceptional situation and emergent nature should be spelt out clearly detailing the justification as well as benefits accrued out of it and loss incurred in case this provision is not invoked and approved by the authority competent to accord administrative and financial approval for the procurement calculated on the basis of total procurement i.e. initial and proposed add on quantity.

c The Purchaser reserves the right to place one or more Purchase order(s) on the successful in phases bidders(s) up to one year from the date of issue of PO. SCI, Registry will have discretion to extend the validity of rate contract for additional one year on the same terms and conditions mutually agreed by both.

C. TERMS & CONDITIONS OF THE SUCCESSFUL TENDERER

1. The successful tenderer shall have to deposit **Performance Security @ 5% of the total amount of the Purchase Order** by way of Bank Guarantee drawn in favour of ''The Registrar (Admn), Supreme Court of India, New Delhi.“ The Performance Security amount will be released after two months from the date of final bill payment and after satisfactory supply of the material, whichever is later.

2. The supply of the material as per the required specifications shall be required to be made within 30 days in the Registry (F.O.R. Destination) on receipt of the Purchase Order; in case supply is not made within the stipulated time and the Registry is forced to make short purchase to meet the emergent demand, the tenderer will be liable to make good the loss due to difference which the Registry may directly deduct from

Bill/Security Deposit. Non-availability of raw material/items shall not be accepted as a ground for delay in supply and shall equally be penalised.

3. Supply of Data Center Hardware is to be made on bill basis. The payment is normally made after full supply is received and accepted as per specifications/requirement.

4. Even after awarding the Supply Order, the Registry reserves the right to terminate the same at any time, if the services of the tenderer are not found satisfactory.

5. The tenderer shall give an undertaking **(as per Annexure 'B')** that the firm/ Partners/
   Director/ Proprietor has not been blacklisted and its business dealings with Central/State Government/Public Sector units/ Autonomous bodies have not been banned/ terminated on account of poor performance.

6. The successful tenderer will have to abide by the terms and conditions as may be fixed from time to time by the Registry.

7. The materials supplied will be inspected by an Inspection Committee of Senior Officers of the Registry and in case the supply is not found in conformity with the approved samples and any complaint is received about its quality and performance during the course of their use/utilization, the entire supply will have to be replaced with the good quality exactly commensurate with approved specifications at the cost of the tenderer. The decision of the Committee in this regard shall be final.

8. Registry has asked for the five-years warranty & support for 24*7 in 4 hours resolution category. The warranty & support should be back to back buy the OEM.

9. The payment will be made only after full supply is received and accepted as preapproved samples against single supply order.

10. If either Party is unable to carry out his obligations under this Contract due to an Act of God, war, riot, blockade, strike (i.e. national/ state or city), lockout, flood or earthquake or Government orders/ restrictions not within the control of the parties hereto which results in an inability, in spite of due diligence of either party in performing its obligation in time, this Contract shall remain effective, but the obligation which the affected party is unable to carry out shall be suspended for a period equal to the duration of the relevant circumstances provided that :

a) The non-performing party shall give the other Party prior written notice describing particulars of the inability including but not limited to the nature of occurrence with its expected duration and the steps which the non-forming parties is taking to fulfill its obligation.

b) Upon receipt of such notice the other party shall discuss the matter with the non- performing party with a view to helping the non-performing party to fulfill its obligations. This clause does not envisage financial assistance.

c) If in any event the Force Majeure situation continues for a period of three weeks both the parties shall meet again and discuss whether the Contract can be amended to overcome the Force Majeure situation so the Project can proceed further. Notwithstanding anything contained to the contrary it is clarified that economic hardship, non-availability of material, labour and transport shall not constitute Force Majeure. The overall responsibilities and obligations of the parties shall not be excused by reasons of Force Majeure situation. Not with standing the above if the Force Majeure continues for a period of three months or more in that event without prejudice to the rights of the parties, the Company shall have the right thereafter to terminate this contract.

D. PENALTIES

1. If delivery is not made in given time and the Registry is required to make purchase from outside at higher rates, the loss, if any, sustained by the Registry would be recovered from the tenderer.

2. Irrespective of the fact as to whether or not the Registry makes purchases from outside, the Registry may impose penalty up to **1% per week subject to maximum of 10%** of total cost of delayed articles, or of forfeiting the performance security if the delay is due to wilful latches or negligence on the part of the tenderer irrespective of inconvenience caused to the Registry.

3. The Security Deposit shall stand forfeited in case of breach of any of the conditions mentioned herein or if the supply of the items is found unsatisfactory/not as per specifications.

E. INVITATION OF TENDER

Interested parties may send their Tenders in Three sealed envelopes superscribing (a) "Earnest Money for Supply of Data Center Hardware", (b) "Technical Bid for Supply of Data Center Hardware" and (c) "Financial Bid for Supply of Data Center Hardware" addressed by name to the undersigned so as to reach on or before 6th March 2020 up to 3:00 P.M. which will be opened on the same day at 3:30 P.M. in the Registry by a Committee of Officers in the presence of the tenderers or their authorized representatives who may wish to remain present there at that time. The tenders received after due date and/or time or without Earnest Money Deposit will not be entertained. In the first instance, envelopes containing Earnest Money may be opened and thereafter the envelopes containing Technical Bids **(Annexure-'C')** will be opened. The envelopes containing Financial Bids **(Annexure-'D')** will be opened at a later date and time to be communicated only to the tenderers who are found technically-qualified.

Additional Registrar (AM)
(B.L.N. Achary)

ANNEXURE-‘A’

Supreme Court of India
Admn. Material (P & S)

F. No.: Data Center/2019
Dated : 15th February, 2020

Last date for Submission of Tender: 06th March, 2020 up to 03:00 p.m.

NOTICE INVITING TENDER FOR SUPPLY OF Data Center Hardware

(Proforma to be filled by the Tenderer)

1. Name of the Tenderer :
 ____
 with Delhi Address

2. Name of the Contact Person with Telephone/Mobile No./
 Fax No./E-Mail ID : ____

3 PAN No. : ___________________________________(Attach Proof)

3A. GST Registration No. : ___________________________________(Attach Proof)

4. Whether all the terms & conditions of NIT are acceptable : Yes/No
 : ____________________________________

5. Whether rates are inclusive/exclusive of GST.

Please mention it clearly : ________________________________

6. Discount, if any : ________________________________

7. FOR: Supreme Court Registry : ________________________________

8. Whether Undertaking of Non-blacklisting attached: __________________

9. Whether empanelled with the Registry enclose proof with tender document: _____________________________ 10. Delivery Schedule : ________________________________

11. Name & address of the Govt. Offices etc. of which the tenderer is having the contract (For Data Center Hardware) with name of contact person and his telephone/mobile number: __________________________________

12. Details of previous experience in the field & infrastructure of the Company: _______________________

13. Whether EMD is submitted or Certificate for its exemption is enclosed: __________________________

Dated: Signature

(Name of firm with stamp)

ANNEXURE-'B'

UNDERTAKING

I/We undertake that (name of the company) has not been blacklisted/banned by any Government Department/Public Sector undertaking/Autonomous Body.

Signature of the authorised signatory of the firm/company/
organisation/Official Stamp/Seal. Date:

Place:

ANNEXURE-'C'
TECHNICAL BID

SPECIFICATION COMPLIANCE SHEET			
Sl. No.	Technical Specification	Description	Compliance (Yes/ No)
1	Modular Rack's	Supply, Installation & Support	
2	Rack Servers With Windows 2012 Server R2 Std & VM Ware	Supply, Installation & Support	
3	DDoS's	Supply, Installation & Support	
4	Next Generation Firewalls	Supply, Installation & Support	
5	Anti APT Appliance (On Premise)	Supply, Installation & Support	
6	Server Load Balancer's	Supply, Installation & Support	
7	Web Application Firewall's (WAF)	Supply, Installation & Support	
8	Storage Area Network (SAN) Switch's	Supply, Installation & Support	
9	Centralised 104 TB Storage	Supply, Installation & Support	
10	5070" Monitor/screen LED displays	Supply, Installation & Support	
11	NMS/ EMS, Gate pass, Ticket login system Software	Supply, Installation & Support	
12	Centralised Backup Software (Storage capacity based license for 10TB)	Supply, Installation & Support	
13	Wifi Controller & Access Points	Supply, Installation & Support	
14	Anti-Virus Endpoint protection	Supply, Installation & Support	
15	Blank IBM Blade Chassis	Supply, Installation & Support	
15	Four resident engineers for one year	Depute & Support	
16	All Documentation & Training to the SC-CC Staff	Service	

Dated: Signature

(Name of firm with stamp)

Technical Specifications.

Modular Racks Total 5 Racks (Qty2 , (Combo of -2 racks) & (Qty1 , (Standalone rack)Specification's:

General Requirements:

- Racks should be self-contained.
- Proper Air circulation with in Row Cooling solution should be provided
- Rack should have 100% assured compatibility with all equipment's conforming to **DIN**

41494(General Industrial Standard for equipment's) or Equivalent **EIA /ISO / EN** Standard

- The Racks should be not more than 2200mm in height with 800X1450 for Network application.

Physical Specifications:

- The Rack unit supported by Plinth should support a static load of at least 1,500 kg, total installed equipment weight.
- The OEM should have Front Glass door and Back Metal door
- The Rack should have two side panels, top Cover, four vertical frame posts, four adjustable19" verticals and grounding and bonding accessories preinstalled by the manufacturer.

Equipment Access & Installation:

- The Rack should have 35U usable Space
- The Rack should have 4No's adjustable, 19" verticals with punched 10mm square hole and Universal 12.7mm15.875mm15.875mm alternating hole pattern offers greater mounting flexibility with Numbered U positions
- The OEM should include Mounting hardware for equipment fixing.
- The front and rear doors should be easily detachable
- The front and rear doors should be openable to allow easy access
- The doors of the rack should be reversible such that it can be mounted on either side.
- The racks should have side panels which can be removed without using tools, using easy finger latches for fast access to cabling and equipment.
- Side panels should flush with the frame so the overall width of the unit does not change with the side panels installed.
- The Vertical cable managers and the PDU has to flushed inside the rack frame there by leading better hot air management at the Rear.

Material Requirements:

- All weight bearing components should be made from steel with a thickness not less than

2.0mm, 19" equipment mounting angle should be 2.5MM and other parts not less than 1mm.

- All sheet metal parts should be Pre-treated and powder coated meeting ASTM Standard.

Grounding Requirements:

- All enclosure components i.e. frame and door should be bonded together and to rack ground point
- OEM to provide rack ground point, Provision to further ground to Telecom Ground bus bar System
- Grounding and bonding as per UL Standards
- Manufacture should provide Horizontal OR vertical Ground bus bar for equipment

Grounding as per Customer / Tender Requirement

Certifications, Environmental and Safety Requirements:

- Racks should be manufactured by ISO9001:20015, ISO14001:2004, ISO27001-2013 & OHSAS18001:2007Certified company and should have proper EHS Policy.
- Manufacturer must certify that the products are RoHS Compliance.
- Manufacturer must certify that the products are Comply DIN41494 and Equivalent EIA/ISO/EN /CEA Standard.
- The rack should comply minimum of IP 50 rating for protection against touch, ingress off origin bodies and ingress of water.
- The enclosure should both protect the user from mechanical hazards and generally meet the requirements for a mechanical enclosure (stability, mechanical strength, aperture sizes, etc.) as defined in IEC 60950 Third Edition.

Ventilation and Thermal Management:

- The Rack should have minimum ventilated with 5 fan which is placed inside the PAC unit
- No ventilation on front & rear doors to avoid cold air leakage.
- The Rack should provide the means to mount optional cooling accessories for high density.
- The manufacturer should provide blanking panel kit to prevent the Recirculation of hot exhaust air.
- The manufacturer should provide air seal kit to seal all gaps to prevent recirculation of hot air.
- The Manufacture should provide PG Gland entry and exit cut outs to avoid cold air leakage.

Rack Power Distribution Units

Type Of PDU	Intelligent (As per the specification)
Phase	1Phase
Rating	7.4
Current	32
Type Of Out Let	C13 & C19
No Of Out let	20 X C13 & 4 X C19
PDU Mounting	Vertical
Space Requirement	0
Measurement	PDU level

PDU Specifications

- Intelligent PDU should be single phase and shall have 32A IEC309 Industrial connector
- Intelligent PDU should have 24 Ports: IEC C13 X 20 and IEC C19 X 4 sockets3
- Intelligent PDU should offer real-time remote power monitoring of power at the inlet: RMS current per line, RMS voltage, Apparent and Active power (kVA, kW), Power Factor (PF) and Energy consumption (kWh)
- PDU should have 2 Network Ports One Gigabit and one 10/100 mbps ports either to access from two separate Networks or in failover mode
- PDU should have field replaceable controller to avoid downtime in case of maintenance
- PDU should support USB or Ethernet Cascading up to 16 PDU
- PDU should support both Port forwarding and Bridge Protocols for accessing the cascaded PDUs
- PDU should support connecting upto 32 Environmental Sensors using appropriate Hardware / Hubs
- PDU should provide power information from Line and CB
- PDU should have LCD Display for at the rack display of the power information from Line and CB
- PDU controller should share the Power with cascaded PDU controller so that in case if one power feed fails, both PDUs in the cabinet maintain network connectivity, and continue monitoring and alerting using the builtin power share capability
- Data provided by the PDUs should be of billing grade accuracy i.e. +/ 1%
- PDU should have USB Ports for serial access to PDU, connecting Wifi Dongles, Logitech Webcam, etc.
- PDU should support configuration of user defined thresholds and alerts
- PDU should have Circuit Breaker Trip Alarming feature
- PDU should support sending / recording alerts to users via SNMP, SMTP, GSM SMS, Syslog, etc.
- PDU should support variety of access protocols including HTTP, HTTPS, NTP, SMTP, SSH, Telnet, SSL, SNMP v1, v2 and v3, SNMP INFORMS and JSONRPC
- PDU should support both IPv4 and IPv6 network protocols
- PDU should support integration with LDAP/LDAPs and AD for secure authentication PDU should support setting Password Policies and Strong encryption.
- PDU should have current protection (OCP) via branch circuit breakers rated over 20A to protect the connected equipment’s
- PDU should provide for disaster recovery option in case of a catastrophic failure during firmware upgrade
- PDU should allow taking backup of the configured settings either for reconfiguring or using for bulk configuration of PDUs
- PDU should have the ability to display temperatures in Celsius or Fahrenheit, height in meters or feet, and pressure in Pascal or psi according to defined user credentials
- PDU should support integration with Power Management Software for providing periodical data of power consumption
- PDU should support multiple configuration options from USB flash drives to sophisticated network-based tools: TFTP, PXE over DHCP, JSONRPC, and others.
- PDU USB Ports should support Wi-Fi networking, PDU to PDU cascading up to 16 devices, bulk configuration, webcams, and mobile interface support on tablet or smartphone
- PDUs shall comply with regulatory CE and UL certifications PDU should be supplied with water leakage sensor

Cable Management:

42U 800 width Racks

- The manufacturer should supply 2 No Brushed cable management with detachable door for management of Horizontal Cables
- 2 No Closed Type Cable Organizer for management of Horizontal and power cables
- 2 No 100mm Universal Cable basket for management of Vertical Cables

Security:

Rack should be with Intelligent Locking solution which has provision to support IP based and solution should be with Biometric Reader.

Rack Lock (Biometric)

Lock system should be reliable easy to install with minimum support and can be Installed in new Racks and retrofitted on existing Racks.

Lock should have below features.

- 1U Rack mountable easy to install with excellent regional support, Value added customization support
- Reliable, robust and scalable solutions
- Industry specific value-added feature
- Solutions give a complete configurable facility to control front and back door of server rack
- Lock / unlock the access point depending upon the preconfigured access rules based on credentials and time
- Plug &amp; Play Mechatronic Locks and Readers with RJ45 Connectivity
- Onboard TCP/IP
- Easy Remote Online Firmware Upgradation, Device Has inbuilt capability for online firmware upgradation
- Transaction and user Capacity: It store up to 10000 User/Cards and up to 1,00,000
- Transaction/Events
- Dual Authentication Support (CARD + Biometric)
- Dual Door Controller
- Dual Door Single Reader Support
- Remote door opening
- Support for any Wiegand Reader
- TimeZone User based Access Control
- Real Time Alerts and Notifications via Email and SMS on critical events like Door Left Open, Door Abnormal, Door Opened Forcefully etc.
- Alarms for critical events like Door Left Open, Door Abnormal, Door Opened Forcefully etc.
- Ease of Integration with BMS/FMS
- Autonomous system (No dependency on PC based application software)
- Facility to activate/deactivate the user access based on requirement

Specification:

Maximum Readers	Up to 2 Readers (Wiegand and/or RS485)
Maximum Door	Two Doors
Mode of Use	Single Door Mode and Double Door Mode

Standalone Mode	With Built in Software in Multidoor site Controller-
Network Mode	With SERVER with or without Multidoor site Controller
READERS Power	12VDC at max. 150ma per Reader
Reader Types	2 Reader Port for any Wiegand or Matrix Reader
Interface	Wiegand and RS 485 (for Matrix Reader only)
INTERFACES Exit Switch	Yes
Door Status Sense	Programmable NO, NC, Supervised
Door Lock Relay	Form C, SPDT Relay (Max 2A@30 VDC)
Door Lock Power	Internal 12VDC @ 0.5A or External
AuxIN	Programmable NO, NC, Supervised
AuxOUT	Form C, SPDT Relay (Max 2A@30 VDC)
Reader Interface types	RS 232, and Wiegand IN/OUT
Reader Types	1 Port for Card Reader / Finger Reader / Card Finger Combo Reader / Third Party Wiegand reader
USB	1 USB Port (for Data Transfer and for 2G3G Dongle)

AUDIOVISUAL Buzzer
LED 2 LEDs (Device Status & Network Status)
ELECTRICAL Input Power PoE (IEEE802.3 af class 0; Max 12W) or External Power Adaptor (12VDC/2A)
Battery Backup Not Required
ENVIRONMENTAL Humidity 5% to 95% RH Noncondensing
Operating Temperature0°C to + 50°C (32°F to 122°F)
System Integration Software API for Software Integration
Certification CE and RoHS
Communication Interface Ethernet or RS485 (10/100 Mbps on Ethernet
USB 1 USB Port
Input Power External Power Adapter (12 VDC @ 2A) Battery Backup No

Features and Capabilities:

- The Block should be Self Cooled and contained.
- Each Racks Should have 30% 1U Screw Less Blank panels
- Rack Should Have Air Seal Kits to avoid Thermal Short circuit.
- Rack Should have Inspection Cover / Door for PAC units
- Rack Should have Racks Separators in front and back to ensure Multi user management.

- N+1 Cooling Redundancy
- Rack should include Novec 1230 suppression for 3.0m3 coverage The rack should be powered with Power Raceway.

Cooling:

- The solutions to DX type 21 KW cooling of 7 KW X 3 Units for N+1 cooling redundancy.
- The Dimension of the PAC should not be more than below dimension. 300mm wide,

1450mmDeep and 2100 Height (+/ 50MM)

- Balancing, Performance Testing & Handing Over of InRow DX Cooling Units with 300 mm width also called cabinet units as regards the indoor unit, with connected outdoor condensing unit, direct expansion version with DC inverter scroll compressor, R410A ecological refrigerant, aircooled by outdoor condensing unit

Casing:

- The Casing of the Unit shall be of frame and Panel type constructed out of 18 G corrosion resistant sheet steel and modular construction with aluminium based railings and hinged doors.
- The exterior panel shall have 80 Kg/m3 density foam insulation and the insulation shall comply with UL94HF1.
- The front & rear of the panel shall be 18 G perforated steel with 80% open free area with locking arrangement to provide a means of securing access to the internal component of the unit.
- The frame shall be made out of 16 G sheet steel and the unit shall have provision for maintenance from both front and the rear and suitable for installation within a row of IT racks.
- The exterior of the panel shall have powder coated texture finish. The unit shall be mounted on casters and levelling screws to allow ease of installation in row and provide a means to level the equipment with adjacent IT racks.

Cooling Coil:

- The evaporator coil shall be constructed of rifled bore copper tubes and louvered

aluminium fins, with the frame and drip tray fabricated from heavy gauge steel.

- The evaporator coil must be minimum 4 rows deep to handle high temperatures across the coil, further since the application are high sensible loads the evaporator must be designed accordingly.
- The coil with hydrophilic or varnish coating will be preferred to prevent any water carry if used without sensible loads only as a primary cooling solution.
- Drip trays are an option best recommended to be provided as standard option and must be double angled for condensate flow and easily removable for cleaning.
- The construction of the drip pan must be of stainless steel/aluminium or galvanized steel as per manufacturer’s recommendation.
- The coil shall be rated for a maximum pressure of 2070 kPa (300 psig).
- The coil is configured in a counter flow arrangement to enhance heat transfer efficiency.
- The cooling coil shall be suitable for chilled water application.
- The unit shall be supplied with inbuilt drain pump having head of up to 5 m for condensate removal.

Drain Pan:

The unit shall be provided with drain pan / drip trays, if required. The drain pans shall be made out of stainless steel / aluminum as per manufacturer's standard.

Temperature and Humidity Sensors:

Internal Sensors

- Internal Temperature Sensors: Thermistor temperature sensors shall be mounted behind the front and rear doors to provide control inputs based on supply and return air temperature. Sensor accuracy shall be within ±2°F accuracy.
- Internal Humidity Sensors: Humidity sensors shall be mounted behind The rear door.

Fan Motor Assembly:

- The air-conditioning unit will have fans with backward curved blades made from reinforced ultralight and highly resistant polymer material. The motors are coupled directly to the fans (plug fan), and are EC (Electronically Commuted) brushless motors: this technology allows continuous modulation of air flowrate by continuously controlling fan speed via a 010V signal. Fan rotation speed can also be controlled directly on the user terminal, so as to allow adjustment of the flowrate or external static pressure (ESP).
- The motor can be powered at either 50 or 60Hz, and will have IP54 ingress protection. All the fans are statically and dynamically balanced, have self-lubricating bearings and are mounted on vibration damping supports.
- The unit controller will be able to modulate fan speed at part loads, together with the compressor inverter. This further reduces power consumption during part load operation.
- The fans are designed to allow "hot replacement" in the event of faults, i.e. an individual faulty fan can be replaced without having to stop the entire unit, thus reducing system down time

Compressor:

- The unit will feature a cooling circuit with one compressor.
- The compressor will be a high efficiency scroll unit installed on the outdoor condensing unit so as to limit maintenance requirements inside the data center. This is equipped with an electronic controller for managing cooling capacity, using DC INVERTER Brushless technology. An electronic board fitted with microprocessor will control effective compressor capacity using a PID algorithm (proportional – integral – derivative) so as to ensure continuous and precise modulation of compressor rotation speed.
- Minimum modulation will be at least 30% of nominal capacity.
- R410A ecological refrigerant will be used; no alternatives are permitted.
- The cooling circuit will include: electronic thermostatic valve, solenoid valve, high and lowpressure switches, liquid sight glass and filterdrier. The low-pressure switch features automatic reset and activation can be delayed when restarting in winter. The highpressure switch requires manual reset.
- The circuit will also include an oil separator to guarantee oil return to the compressor and reduce the risk of shutdown, plus a liquid separator.

Active redundancy and shared mode:

The cooling units will be capable of providing active redundancy. To ensure this, all the units installed, including the redundant unit, must be able of operate at the same time and at part loads.

This feature must also be able to increase system efficiency by reducing energy consumption at part loads.

Humidifier:

The unit will read the relative humidity (RH) and control the level by activating humidification cycles only when the return air humidity is too low (<40%, settable).

The humidifier is an immersed electrode model with modulation of steam production. It also features automatic control of dissolved salt concentration so as to allow untreated water to be used.

Reheating:

- The unit will be equipped with electric heaters, to allow temperature control during dehumidification cycles.
- The electric heaters include stainless steel fins, and are fitted with safety thermostat to cutoff power supply and activate an alarm in the event of overheating. The heaters feature modulating operation, in 3 stages.

Main Disconnect Switch:

- The unit shall be provided with Main Disconnect Switch suitable for 220V, 50 Hz, 100 KA rating.
- The unit shall include individual disconnect switch for both Primary & Secondary power inputs.

Electrical Panel:

- Control cabinet to be as per OEM design, with grounding lug, combination magnetic starters with overload relays, circuit breakers and cover interlock, and fusible control circuit transformer.
- The construction of the unit electrical panel must be such to also provide space for microprocessor controller and without opening of any panels from the front of the unit the microprocessor panel must have direct access for operation. Return air T/H sensor shall be part of standard supply of the unit.
- The electric panel provided for the unit must be equipped with main incoming power isolation switch, additionally the unit must be provided with under voltage / over

voltage / phase reversal/ single phasing protection, all three phase motors must be operated only via 24V coil voltage contactors and MPCB’s, additionally step-down transformer must be provided for power supply to the unit controller. The electrical panel must also be providing with relay block for common alarm.

MICROPROCESSOR CONTROLLER:

- Monitoring and Configuration: The master display shall allow monitoring and configuration of the cooling unit through a touch screen control (ACRC300 series). Functions include status reporting, setup, and temperature set points. LEDs report the operational status of the connected air conditioning unit.

- Controls: The microprocessor controller shall allow the user to navigate between menus, select items, and input alpha numeric information.
- Alarms: The microprocessor controller shall activate a visible and audible alarm in the occurrence of the events listed in the Technical Specifications Manual.
- Logging: The microprocessor controller shall log and display all available events. Each alarm log shall contain a time/date stamp. Controller shall display the run time hours for major components.

NETWORK MANAGEMENT CARD:

- The unit shall include a network management card to provide management through a computer network through TCP/IP. Management through the network should include the ability to change set points as well as view and clear alarms.

MICROPROCESSOR DISPLAY UNIT:

- In normal operating mode the screen should display unit number, temperature and relative humidity set points and actual, operating status.
- The unit must have a large screen LCD display on controller with user friendly menus and minimum two level password protections.
- RS485 interface port for BMS compatibility with ModBus RTU protocol is required

Fire detection and suppression system:

- Delivery of an active extinguishing system that detects and extinguishes fires in closed server and network cabinets.
- The extinguishing process must not be electrically conducting and must be fast and residuefree.
- It should be rack mountable device that should have high sensitivity smoke detection with active sampling. It should have a builtin NOVEC 1230 suppression system. sufficient for 1 IT rack with integrated fire panel, actuator, discharge nozzle and complete piping with accessories.
- The Rack Mountable Device should not consume more than 3U of space.
- This device should monitor using potential free contacts.
- The Fire Detection system should be having two Zones for advance Detection.

Standard Rodent Replica System One for each rack.

B.O.Q.		
S. No.	Description	Number of Units
For 2 combined rack (Qty 2):		

1	Rack Size 42U/800x1450 (Colour Black)	4
2	Blank Panel/1U/Pk of 5	4
3	Blank Panel/2U/pk of 5	4
4	Lock/Master/1U	2
5	Lock/Add On/1U	2
6	Operating Module / Biometric Reader + Mifare	4
7	Swing Handle Lock/ Mechatronic/4Point	8
8	Door Status Sensor/Switch	8
9	Side panel /Lock/FM/NRS/NRSe/NHDC/Unique Key	4
10	1 1PH, 230V AC, 32A (32A rated); 24 outlets: 20x C13, 4x C19; plug: IEC 60309 2P+E 6h 32A (bottom feed), 7.4kVA; Unit Metered, Zero U vertical PDU, Secure Lock ady, high resolution color display with field replaceable controller, Ethernet, serial, 2x USBA, USBB and sensor connections.	8
11	Fire Detection and Suppression system/NOVAC 1230	4
12	Safe Transfer Switch/ 1Phase / 2 Pole / 32A/Black	4
13	Rack AC/Vertical/42U/300x1450/7KW/DX/Black	6
14	Lower Side work Refrigerant Piping between Indoor & Outdoor unit (Considered Distance between IDU & ODU is 25 RMT)	6
15	Installation & support 24* 7 for 5 years	4

B.O.Q.		
S. No.	**Description**	**Number of Units**
For 1 Standalone combined rack (Qty 1):		
1	Rack Size 42U/800x1450 (Colour Black)	1
2	Blank Panel/1U/Pk of 5	1
3	Blank Panel/2U/pk of 5	1
4	Lock/Master/1U	1
5	Lock/Add On/1U	1
6	Operating Module / Biometric Reader + Mifare	1
7	Swing Handle Lock/ Mechatronic/4Point	2
8	Door Status Sensor/Switch	2
9	Side panel /Lock/FM/NRS/NRSe/NHDC/Unique Key	1

10	1 1PH, 230V AC, 32A (32A rated); 24 outlets: 20x C13, 4x C19; plug: IEC 60309 2P+E 6h 32A (bottom feed), 7.4kVA; Unit Metered, Zero U vertical PDU, Secure Lock ady, high resolution color display with field replaceable controller, Ethernet, serial, 2x USBA, USBB and sensor connections.	2
11	Fire Detection and Suppression system/NOVAC 1230	1
12	Safe Transfer Switch/ 1Phase / 2 Pole / 32A/Black	1
13	Rack AC/Vertical/42U/300x1450/7KW/DX/Black	2
14	Lower Side work Refrigerant Piping between Indoor & Outdoor unit (Considered Distance between IDU & ODU is 25 RMT)	2
15	Installation & support 24* 7 for 5 years	1

Rack Servers With VM Ware & Window 2012 Server R2 STD(Qty 12) Specification’s:

Form Factor: Max. 2U rack mounted.

Configured CPU: Processors, (Intel Xeon Gold 6130 (2.10GHz/16core/22MB/) or better.

Memory slots: 24 DDR4 DIMM slots RDIMMS & LR DIMMS supporting speeds up to 2666MT/s. Optionally sup port up to 12 DIMM & 12 NVDIMM.

Memory configured: RAM 1024 GB.

Disk support: Front drive bays: Up to 16 x 2.5” SAS/SATA/ SSD, Up to 8 x 3.5” SAS/SATA. **Raid control:** 12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 8 GB Cache.

Disk configured: Hot pluggable SSD 2x480 GB, with min 06 no or higher internal Drive bays.

I/O slots : Up to 8x PCIe Gen3 Slots.

Ports: Ports 4 x 1G RJ45 LOM, 4*10 Gig SFP+, 4*FC HBA.

Certification and compliances: Microsoft Windows Server, HyperV, VMWare, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES).

Power Supply: Redundant Power Supply.

SD Modules slots : Dual SD Module slots supporting redundant configuration.

Management integration : Support for integration with any thirdparty server management platform. Power & temperature: Realtime power meter, graphing, thresholds, alerts & capping with historical power counters. Temperature monitoring & graphing.

Prefailure alert: Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD.

Configuration & management: Realtime outofband hardware performance monitoring & alerting, Agentfree monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & CNA & system health, Outofband hardware & firmware inventory. Automated hardware configuration and Operating System deployment to multiple servers, Virtual IO management/stateless computing, Support for APIs for simple and secure management of scalable platform hardware.

LCD panel: Should display system ID, status information and system error code followed by descriptive text. LCD background should light up in different col ours during normal system operation & error conditions.

Server security: Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyberattacks, Should protect against firmware which executes before the OS boots, Should provide effective protection, reliable detection & rapid recovery.

Intrusion alert: Intrusion alert in case chassis cover being opened.

IPV 6 compliance: The Hardware should be IPV 6 Compliant ready.

Support & Warranty: 5 Years OEM Premium support bundle with 24x7x365 days TAC support.

DDoS (Qty 2) In HA, Specification’s:

- DDoS Detection & Mitigation solution being offered should be minimum EAL2+ certified or higher. OEM must be present in the latest Forrester "LEADER" Quadrant for DDoS solution.
- DDoS mitigation solution should be a dedicated appliance (not a part of Router, UTM, Application Delivery Controller, Proxy based architecture or any Stateful Device) with 20 Gbps of DDoS Mitigation Throughput.
- Support DoS Flood Attack Prevention Rate: upto 25 Mbps.
- Inspection Ports supported: 20 x 10G SFP+ (Bidder to populate appropriate SFP's as per the proposed solution)
- Automatic Real Time Signature generation within few seconds, without human intervention. Should have a dedicated outofband Ethernet management port.

Security Protections:

- BEHAVIORAL ANALYSIS using behavioural algorithms and automation to defend against IoT botnet threats, including Mirai DNS Water Torture, Burst and Randomized attacks.

- POSITIVE SECURITY MODEL should have advanced behaviour analysis technologies to separate malicious threats from legitimate traffic
- ZERO DAY ATTACK PROTECTION should be provided by behaviour based protection with automatic signature creation against within few seconds of unknown, zero day DDoS attacks.
- CUSTOM TAILORED HARDWARE must be proposed using dedicated DoS Mitigation platform which offloads high volume attacks, inspecting without impacting user experience.

Behavioural DoS Protection

- Behavioural DoS (Behavioural Denial of Service) Protection should defend against zero day network flood attacks, detect traffic anomalies and prevent zeroday, unknown, flood attacks by identifying the footprint of the anomalous traffic.

- Network flood protection should include:

  TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood

  UDP flood

  ICMP flood

  IGMP flood

Security Features – Signature Protections support

- Serverbased vulnerabilities: — Web vulnerabilities
  — Mail server vulnerabilities
  — FTP server vulnerabilities
  — SQL server vulnerabilities
  — DNS server vulnerabilities
  — SIP server vulnerabilities
- Worms and viruses
- Trojans and backdoors
- Clientside vulnerabilities
- IRC bots
- Spyware
- Phishing
- Anonymizers"

OEM DDoS Mitigation RESPONSE TEAM required from DAY1

The OEM has to provision for knowledgeable and specialized security experts who provide 24x7 (SLA defined), REAL TIME Professional Services for the network facing denialof service (DoS) attack in order to restore network and service operational status.

The ERT should support the following advanced services:

1) 24/7 monitoring of the customer’s service
2) Realtime response to any threat detected
3) Direct “hotline” access
4) Diverting the traffic when encountering a volumetric attack
5) Sending the customer, a summary of each realtime attack case
6) Sending the customer, a monthly report containing all threats
7) Periodically reviewing the networksecurity configuration

Centralized Monitoring and Historical Reporting solution should be provided from Day 1

The proposed solution should support Integration with OEM Cloud based Scrubbing

Centres, in case of Bandwidth Saturation attacks, using the same technology/OEM. The proposed solution must provide REALTIME attacker intelligence feeds from day 1, pertaining to a active attack sources recently involved in DDoS attacks.

B.O.Q.		
S. No.	**Description**	**Number of Units**
1	20*SFP+ (10GE) (All Populated) , 20Gbps attack capacity and Dual AC Power Supply - 25 MPPS DDoS Flood Attack Prevention Rate (Not limited to Syn Attacks Only)	2
2	Installation, configuration, 24X7 Premium Support & all related licenses superscription for 5 Years (OEM Premium back to back)	2

Next Gen Firewall (Qty 2) In HA, Specification’s:

Basic Criteria:

- The proposed vendor must have "Recommended" rating with min 97% Evasion proof capability and min 97% Security Effectiveness as per 2019 NSS Labs Next Generation Firewall Test Report.
- The proposed OEM must be in the Leader’s quadrant of the Enterprise Firewalls Gartner Magic Quadrant for consecutive 5 years
- Appliance should have ICSA, NEBS Level 3, FCC Class A, CE Class A, VCCI Class A, CB and Common Criteria Certified.

Form factor:

- Modular or Fixed

Fans and Power Supply:

- The offered firewall must have field replaceable redundant hot swappable fan trays and redundant hot swappable power supplies.

Architecture:

- The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc).
- The proposed firewall must have min 16 physical cores and 32 GB RAM with x86 processor and not an ASIC based solution. No work around this will be accepted.
- The administrator must be able to view report on the CPU usage for management

activities and CPU usage for other activities.

- The device or any of its family should not have any feature of wireless within its hardware or software.

Storage:

- Min 240GB SSD system disk

Interface Requirement:

- Min 12 x 10/100/1000 Copper interfaces from day one

8 x Gig/10Gig SFP/SFP+ ports with 8 tranceivers (SMF) from Day one, 4 x 40G
QSFP+ slots
Dedicated HA ports (Min 1 x 10G SFP and min 1 x RJ45) in addition to requested data ports, OOB, Management and USB Port

Performance Capacity:

- Application Aware Firewall application throughput – 8.5 Gbps

- Threat prevention throughput (with all features like AV, bot protection, zero day protection and logging enabled) – 4.5 Gbps
- IPsec VPN throughput – 4.5 Gbps
- Tunnels (SSL, IPSec, and XAUTH) – 6,000 from day 1
- Concurrent SSL Decryption sessions – 200,000. This should be substantiated with document from public website or testing/R&D report data. Declaration on letterhead will not be accepted.
- New sessions per second – Min 130,000
- Concurrent sessions – Min 3,000,000
- Virtual systems (from day one) – 5

High Availability: Active/Active and Active/Passive

Application Control Throughput:

A Minimum NG Firewall application control throughput in real world/production environment/Application Mix – 8.5 Gbps. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA

Total Threat Protection Throughput:

Minimum NG Threat prevention throughput in real world/production environment (by enabling and measured with ApplicationID/AVC, User-ID/AgentID, NGIPS, AntiVirus, AntiSpyware, C&C protection, Zeroday attacks and all other security threat prevention features enabled – 4.5 GBPS real world/production environment/Application Mix . The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA.

Interface Operation Mode:

The proposed firewall shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in:
Tap Mode
Transparent mode (IPS Mode)
Layer 2
Layer 3
Should be able operate mix of multiple modes

NGF Features:

- The proposed firewall shall have native network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactics.
- The proposed firewall shall be able to handle (alert, block or allow) unknown/unidentified applications like unknown UDP & TCP
- The proposed firewall should have the ability to create custom application signatures and categories directly on firewall without the need of any thirdparty tool or technical support.
- The NGFW must have GUI based packet capture utility within its management console with capability of creating packet capture filters for IPv4 and IPv6 traffic and ability to define the packet and byte count
- The proposed firewall shall be able to implement Zones, IP address, Port numbers, User id, Application id and threat protection profile under the same firewall rule or the policy configuration
- The firewall must support creation of policy based on wildcard addresses to match multiple objects for ease of deployment
- The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its filetransfer capability inside the chat application base on the content.
- The proposed firewall shall be able to protect the user from the malicious content upload or download by any application. Example Blocking a malicious file download via a chat or file sharing application.
- The firewall must have the ability to manage firewall policy even if management server is unavailable
- The firewall must disallow root access to firewall system all users(including super users) at all times.
- The firewall must be capable of prevention against flooding of new sessions with highvolume singlesession and multiplesession attacks to the extent of 5 Million pps/fps
- The firewall must have the capability to create DOS prevention policy to prevent against DOS attacks on per zone basis (outbound to inbound, inbound to inbound and inbound to outbound) and ability to create and define DOS policy based on attacks like UDP Flood, ICMP Flood, SYN Flood(Random Early Drop and SYN cookie), IP Address Sweeps, IP Address Spoofs, port scan, Ping of Death, Teardrop attacks, unknown protocol protection etc

Threat Protection:

- All the proposed threat functions like IPS/vulnerability protection, Antivirus, C&C protection etc should work in isolated air gapped environment without any need to connect with Internet.
- Should have protocol decoderbased analysis which can stateful decodes the protocol and then intelligently applies signatures to detect network and application exploits

- Intrusion prevention signatures should be built based on the vulnerability itself, A single signature should stop multiple exploit attempts on a known system or application vulnerability.
- Should block known network and applicationlayer vulnerability exploits
- The proposed firewall shall perform content based signature matching beyond the traditional hash base signatures
- The proposed firewall shall have on box AntiVirus/Malware, Anti Spyware signatures and should have minimum signatures update window of every one hour

All the protection signatures should be created by vendor base on their threat intelligence and should not use any 3rd party IPS or AV engines.

Should be able to perform Antivirus scans for HTTP, smtp, imap, pop3, ftp, SMB traffic with configurable AV action such as allow, deny, reset, alert etc

- Should have DNS sink holing for malicious DNS request from inside hosts to outside bad domains and should be able to integrate and query third party external threat intelligence data bases to block or sinkhole bad IP address, Domain and URLs
- The URL filtering service should be able to categorize a site by multiple categories and not just a single and custom category
- The solution must be able to define AV scanning on per application basis such that certain applications may be excluded from AV scan while some applications to be always scanned
- Should be able to call 3rd party threat intelligence data on malicious IPs, URLs and Domains to the same firewall policy to block those malicious attributes and list should get updated dynamically with latest data
- It should have automatically push dynamic block list with latest threat intelligence data base on malicious IPs, URLs and Domains to the firewall policy as an additional protection service
- The NGFW should have native protection against credential theft attacks (without the need of endpoint agents) with ability to prevent the theft and abuse of stolen credentials and the following:

·Automatically identify and block phishing sites
·Prevent users from submitting credentials to phishing sites
· Prevent the use of stolen credential

Advanced Persistent Threat (APT) Protection (Service Only):

- This should be a cloud base unknown malware analysis service with guaranteed protection signature delivery time not more than 5 minutes
- Advance unknown malware analysis engine should be capable of machine learning with static analysis and dynamic analysis engine with custombuilt virtual hypervisor analysis environment
- Advance unknown malware analysis engine with real hardware, detecting VMaware malware to detect and protect from virtual sandbox evading advance unknown malware
- Cloud base unknown malware analysis service should be certified with SOC2 or any other Data privacy compliance certification for customer data privacy protection which is uploaded to unknown threat emulation and analysis . here should be provision to have hybrid architecture on premise as well as cloud. In case on premise is been asked then the same should be suppliued with upto 30 VM, RPS and 16 Disk bays.
- Cloud base unknown malware analysis service should be able to perform dynamic threat analysis on such as EXEs, DLLs, ZIP files, PDF documents, Office Documents, Java®, Android APKs, Adobe Flash applets, Web pages that include highrisk embedded content like JavaScript, Adobe Flash files. MAC OS and DMG file types

- The proposed next generation security platform should be able to detect and prevent zero day threats infection through HTTP, HTTPS, FTP, SMTP, POP3, IMAP use by any of application used by the users (eg: Gmail, Facebook, MS outlook)
- The solution must be able to use AV and zero day signatures based on payload and not just by hash values
- Advance unknown malware analysis engine should be able to creates automated highfidelity signature for command and control connections and spyware to inspect command and control http payload to create one to many payload base signatures protection from multiple unknown spyware and command and control channels using single content base signature
- The protection signatures created base unknown malware emulation should be payload or content base signatures that cloud block multiple unknown malware that use different hash but the same malicious payload.

SSL/SSH Decryption:

- The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forwardproxy).
- The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection.
- The firewall must have the capability to be configured and deployed as SSL connection broker and port mirroring for SSL traffic.
- The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections.
- The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and nonpersonal traffic.
- SSL decryption must be supported on any port used for SSL i.e. SSL decryption must be supported on nonstandard SSL port as well

Network Address Translation:

- The proposed firewall must be able to operate in routing/NAT mode
- The proposed firewall must be able to support Network Address Translation (NAT)
- The proposed firewall must be able to support Port Address Translation (PAT)
- The proposed firewall shall support Dual Stack IPv4 / IPv6 (NAT64, NPTv6)
- Should support Dynamic IP reservation, tunable dynamic IP and port oversubscription.

IPv6 Support:

- L2, L3, Tap and Transparent mode
- Should support on firewall policy with User and Applications
- Should support SSL decryption on IPv6
- Should support SLAAC Stateless Address Auto configuration

Routing and Multicast support:

- The proposed firewall must support the following routing protocols:
- Static
- RIP v2
- OSPFv2/v3 with graceful restart
- BGP v4 with graceful restart

- The firewall must support FQDN instead of IP address for static route next hop, policy based forwarding next hop and BGP peer address
- The firewall must support VXLANTunnel content inspection
- The firewall must support DDN sprovides such as DuckDNS, DynDNS, FreeDNS Afraid.org Dynamic API, FreeDNS Afraid.org, and NoIP.

The proposed firewall must have support for mobile protocols like GTP, SCTP and support for termination of GRE Tunnels Policybased forwarding

- PIMSM, PIMSSM, IGMP v1, v2, and v3
- Bidirectional Forwarding Detection (BFD)

Authentication:

Should support the following authentication protocols:
LDAP
Radius (vendor specific attributes)
Tokenbased solutions (i.e. Secure-
ID) Kerberos

The proposed firewall's SSL VPN shall support the following authentication protocols
LDAP
Radius
Tokenbased solutions (i.e. SecureID)
Kerberos
SAML
Any combination of the above

Monitoring, Management and Reporting:

- Should support on device and centralized management with complete feature parity on firewall administration
- The management solution must have the native capability to optimize the security rule base and offer steps to create applicationbased rules
- The proposed solution must allow single policy rule creation for application control, userbased control, host profile, threat prevention, Antivirus, file filtering, content filtering, QoS and scheduling at single place within a single rule and not at multiple locations. There must not be different places and options to define policy rules based on these parameters.
- Should have separate real time logging base on all Traffic, Threats, User IDs, URL filtering, Data filtering, Content filtering, unknown malware analysis, Authentication, Tunneled Traffic and correlated log view base on other logging activities
- Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis
- Should allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.
- Should have built in report templates base on Applications, Users, Threats, Traffic and URLs
- Should be able to create reports base user activity
- Should be able to create custom report base on custom query base any logging attributes
- On device management service should be able to provide all the mentioned features in case of central management server failure

Support & Warranty:

5 Years OEM Premium support bundle with 24x7x365 days TAC support, RMA (There should be at least 4 RMA depot in India), software updates and subscription update support. The NGFW should be proposed with 5 years subscription licenses for NGFW, NGIPS, AntiVirus, Anti Spyware, Anti Botnet and Anti APT.

B.O.Q.		
S. No.	**Description**	**Number of Units**
1	Next Generation Firewall with HA capability with the following per device : Min 16 Physical Cores, Min 32GB RAM, 240 GB SSD disk, 12x 10/100/1G Copper RJ-45 Interfaces, 8 x 10G SFP+ Slots with 4 x 10G SFP/SFP+ transceivers from day one, 4 x 40G QSFP Slots(no transceivers), Min 1 HA port(1 x 10G SFP/SFP+ and 1 x RJ-45), Dual Hot swap Power supplies, Hot swap fans, rack mounting kit with rails, power cords (India Type) of suitable rating.	2
2	Licences for Firewall from day one including but not limited to the following features : Application Visibility, User identification, IPS, Anti Virus, C&C Protection/Anti-Bot, URL Protection, Data Filtering, Content Inspection, Zero Day and Advanced Malware Protection for 5 Years	2
3	SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant	8
4	Installation, configuration, 24X7 Premium Support for Next Generation Firewall 5 Years (OEM Premium back to back)	2

Home Office Security Gateway (Qty-40):

Basic Criteria's (Performance Requirement):

- The security gateway device must be based on min 4 core Intel make multi core processor (J1900 or better) and not Atom processor based solution and security function must be provided by a security OEM present in the Leader's quadrant of the Enterprise Firewalls Gartner Magic Quadrant for last consecutive 5 years.
- The security gateway should have an application aware throughput of min 150 Mbps on real world traffic
- The security gateway must have a min threat prevention throughput of 70 Mbps with features like Firewall, application control, IPS, Anti-Virus, Anti-malware, zero day protection and C&C protection enabled.
- The proposed solution must support at least 2,000 new session per second.
- The proposed solution must support at least 70 Mbps of IPSEC VPN throughput from Day one without requiring any license.
- The security gateway must support min 8 GB RAM.
- The security gateway must have min onboard storage of min 32 GB
- The security gateway must support min 1*MINI-PCIE interface for loading wifi, 3G/4G modules/dongles (USB signal devices only) and min 4 Gigabit LAN RJ-45 interfaces and min 2 USB interfaces
- The security gateway must be low power consumption device with rugged fan less design.

Basic Criteria's (Functional Security Requirement):

- The proposed solution shall have native network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactics.
- The proposed solution shall be able to handle (alert, block or allow) unknown/unidentified applications like unknown UDP & TCP
- The proposed solution should have the ability to create custom application signatures and categories directly on device without the need of any third-party tool or technical support.
- The solution must have GUI based packet capture utility within its management console with capability of creating packet capture filters for IPv4 and IPv6 traffic and ability to define the packet and byte count.
- The proposed solution shall be able to implement Zones, IP address, Port numbers, User id, Application id and threat protection profile under the same firewall rule or the policy configuration
- The solution must support creation of policy based on wildcard addresses to match multiple objects for ease of deployment

- The proposed solution shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application base on the content.
- The proposed solution shall be able to protect the user from the malicious content upload or download by any application. Example Blocking a malicious file download via a chat or file sharing application.
- The solution must have the ability to manage firewall policy even if management server is unavailable
- The solution must disallow root access to firewall system all users(including super users) at all times.
- Solution should support Session based load sharing (not packet based) over multiple equal cost paths. It should work with both static and dynamic routing.
- The device should be capable to identify and prevent in-progress phishing attacks by controlling sites to which users can submit corporate credentials based on the site's URL category thus blocking users from submitting credentials to untrusted sites while allowing users to continue to submit credentials to corporate and sanctioned sites.
- The proposed solution must support Policy Based forwarding based on: - Zone - Source or Destination Address - Source or destination port - Application (not port based) - AD/LDAP user or User Group - Services or ports
- The solution must support Firewall, Application visibility and control, IPS, Anti-virus, Anti-malware, Anti-bot, Zero Day Protection(cloud based) from day one.
- Solution should support Session based (not packet based) differentiated services code point (DSCP) classification.
- Solution must support end-to-end (firewall-to-client) priority policing and C2S & S2C direction enforcement.
- Solution must support Link Layer discovery protocol (LLDP) for simplified network management
- Solution should correlate and detect hosts that have received malware, and have also exhibited command-and-control (C2) network behaviour corresponding to the detected malware.
- The proposed solution must support validation of policy for shadowed rules before rule application
- The proposed solution must support on appliance Per policy SSL and SSH decryption for both inbound and outbound traffic.
- The proposed must support on appliance SSL decryption policy based on IP, User, web category.
- The proposed solution should support the ability to create QoS policy on a per rule basis: -by source address -by destination address -by application (such as Skype, Bittorrent, YouTube, azureus) -by static or dynamic application groups (such as Instant Messaging or P2P groups) -by port and services
- Solution should detect probable exploit kit activity targeted at a host on the network. Exploit kits should be identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature.
- The solution must have option to be managed from both ie directly from the device and from a centralized console
- The solution must have a web based management console with capability of doing a packet capture directly from the GUI.
- The proposed solution must have native SD WAN like capabilities for monitoring parameters like latency, jitter etc.

B.O.Q.		
S. No.	Description	Number of Units
1	Home Office Security Gateway with Firewall, IPS, AV, URL Filtering and zero Day Protection from day one	40
2	Installation, Configuration, 24x 7 Premium Support for Home Office Security Gateway for 5 Years (OEM Premium back to back)	40

Anti APT Appliance(Single), Specification's :

Basic Criteria:

- Appliance should have FIPS Certified.

Form factor:

- Modular or Fixed **Architecture:**
- The solution should be provided with a purposebuilt onpremise appliance with integrated support for sandboxing and should be from same OEM as that of NGFW.
- APT hardware provided must have integration with NGFW appliance to detect multi stage attacks the solution should include static analysis technologies like IPS, antivirus, antimalware /anti bot, application awareness, URL Filtering and advanced threats through the APT appliance.
- The APT appliance should be able to handle min 50 NGFW appliance.
- The device should have at least Dual 6Core Processor.
- Appliance should have minimum 2 x 1 TB storage in RAID 1.

Interface Storage and VM Requirement:

- The APT appliance should support upto 30 virtual machines running simultaneously
- Min 3 or higher Copper/Fiber ports should be provided in APT appliances for achieving functionalities mentioned
- Minimum one number of 1G Copper ports for management.
- The device should have 20 disk drive bays and redundant power supply.

Features:

- OEM should ensure the delivery of the signature in 5 minutes from the time of detection and it should be mentioned on public documents.
- The single device should be able to analyse upto 6000 files in single device and scalable to more than 100,000 in cluster mode
- The solution must be able to detect and report malware by using multiple images of Windows XP, 7 and 8 etc

- The solution must support Pdf, Adobe flash, JAR files, PE files, MS office files and links within email analysis.
- AntiAPT solution should be able to work independently of signature updates from OEM website. The solution must provide an option for not sharing any Threat Intelligence with the OEM and must create signatures/file hash without any OEM cloud support.
- The solution must be able to support scanning links inside documents for zero days & unknown malware and support sandboxing of file sizes between 2 Kb and 10 MB or higher. Solution should have an ability to remove all the active content, harmful links in documents and macros sending only a clean document to the end user
- The solution should support vminterface that can provide network access for the systems to enable sample files to communicate with the Internet
- Should support alteast PE files (EXE, DLL and others), MS Office, PDF, Flash, Java applets (JAR and CLASS), analysis of links within email messages, compressed (ZIP) and encrypted (SSL) files.

Support & Warranty:

5 Years OEM Premium support bundle with 24x7x365 days TAC support, RMA(There should be atleast 3 RMA depot in India), software updates and subscription update support. The APT should be proposed with 5 years subscription licenses.

B.O.Q.		
S. No.	**Description**	**Number of Units**
1	On Premise Device for Anti APT device for sandboxing with Dual 6 Core processors, min 128 GB RAM, 16 Disk bays with 2 TB in RAID 1, 4 x 10/100/1000 RJ-45 Copper Interfaces and Dual Hot swap power supplies, rack mounting kit with rails, power cords (India Type) of suitable rating	1
2	Licence for Anti APT Device, if any for 5 Years	1
3	Installation, Configuration, 24X7 Premium Support for Anti APT Device a 5 Years (OEM Premium back to back)	1

Server Load Balancers (Qty-4) in HA for each pair, Specification’s:

OEM should be present in Gartner's "LEADER" magic quadrant in the latest ADC report. The proposed solution should be present in leader’s quadrant of Gartner/ Forrester report at-least 1 Times in last 5 published report.

Architecture:

- Traffic ports supported: 20 x 10 GbE SFP+ (Bidder to populate appropriate SFP's as per the proposed solution)
- Layer 4 connections per second: 1 Million CPS

- Layer 7 requests per second: 1 Million RPS
- RSA CPS (2K keys) : 30K CPS
- ECC CPS (ECP256) : 20K CPS
- SSL Throughput: 20 Gbps.
- Should provide minimum 25 Gbps throughput and can be scalable to 50 Gbps throughput without changing the hardware (license upgrade only).
- Device must have Dynamic routing protocols like OSPF, RIP1, RIP2, BGP from Day 1.

These Server Load Balancing Topologies should be supported:

- Virtual Matrix Architecture / Equivalent
- Client Network Address Translation (Proxy IP)
- Mapping Ports
- Direct Server Return
- One Arm Topology Application
- Direct Access Mode
- Assigning Multiple IP Addresses
- Immediate and Delayed Binding
- IP Address Ranges Using imask / Equivalent.

The SLB should support the below metrics:

- Minimum Misses
- Hash
- Persistent Hash
- Tuneable Hash
- Weighted Hash
- Least Connections
- Least Connections Per Service
- RoundRobin
- Response Time
- Bandwidth.

VIRTUALIZATION:

- The proposed SLB should have Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources.
- Each virtual ADC instance contains a complete and separated environment of the Following: Resources, Configurations, Management, OS.
- The proposed device should support upto 30 Virtual Instances.
- The virtual instance management should have two management roles: o Creates, initially configures, and monitors vADCs. Should be able to dynamically allocate CPU and throughput resources by assigning capacity units and adjusting throughput limits to a vADC. o Another role – should have daytoday configuration and maintenance of virtual instance using the same tasks as with traditional ADCs, except for those virtual instance tasks that only the capacity.
- The device should support DNS SEC Global Server load Balancing functionality.
- The proposed framework should enables to**:** Extend Server Load Balancer Fabric services with delivery of new applications, Quickly deploy new services, Mitigate application problems without changing the application, Preserve infrastructure investment by adding new capabilities without additional equipment investment.
- Should support Web Performance Optimization feature that should employ different acceleration treatments for different application and browser scenarios: Simplifying large, complex web pages, Caching, Accelerate entire web transaction, ThirdParty timing and SLAs, Content Minification / Equivalent, Acceleration for mobile devices- Mobile Caching, Image resizing, Touchtoclick conversion / Equivalent.
- DNSSEC based Global Load Balancing should be supported in the proposed device.
- The Server Load balancer should support the Application Performance Monitoring feature and should support the following: Real user monitoring for any client with no

agent software, Centralized monitoring of performance across Local and Datacenter, Measurement of real users and their actual transactions including errors – eliminating manual scripting of synthetic transactions, Diagram allowing to visually see which transactions breach SLA, Breaking down the measurements by specific application, location or transaction, SLA is userdefined – allowing full control over application, Ability to see which transactions were not completed due to errors.

- Should support serverside web compression and proximity based LLB
- Should Support standard VRRP (RFC 2338)
- SLB Device should be accessed through the: Using the CLI, Using SNMP, REST API, Using the Web Based Management, Dedicated Management Port.

-

B.O.Q.		
S. No.	**Description**	**Number of Units**
1	20*10GE SFP+(All Populated) Dual AC power supply - 500GB Storage and 25 Gbps throughput.	4
2	Installation, Configuration, 24X7 Premium Support & all related licenses superscription for 5 Years (OEM Premium back to back)	4

Web Application Firewall (WAF) In (Qty-2) HA, Specification's:

OEM should be present in Gartner Magic quadrant in the latest WAF report and the proposed Web Application Firewall should be ICSA certified. The proposed solution should be present in leaders/ Challenger or Strong Players quadrant of Gartner/ Forrester report at-least 1 Time in last 5 published report.

The proposed Hardware Should support the below mentioned Sizing Parameters:

- **WAF Throughput:** 5 Gbps, RSA CPS (2K keys) : 50K CPS, ECC CPS (ECP256) : 25K CPS, SSL Throughput : 20 Gbps.
- **Traffic ports supported:** 20 x 10 GbE SFP+ (Bidder to populate appropriate SFP's as per the proposed solution).
- **VIRTUALIZATION:** The proposed device should have Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. Each virtual instance contains a complete and separated environment of the Following: Resources, Configurations, Management & OS. The proposed device should support upto 30 Virtual Instances.
- **WAF should have the flexibility to be deployed in the following modes:**

o Reverse proxy o Out of Path (OOP) support

- The proposed solution should support standard VRRP (RFC 2338) for High Availability purpose (no proprietary protocol).
- The WAF should support the following escalation modes: Active, Bypass, Passive.

ROLEBASED SECURITY POLICIES:

- The WAF should support Policy Enforcement based in different policies on different apps or roles.
- The solution must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification.
- Advanced BOT Management service to be provided from Day1 in the proposed WAF.
- Hiding Sensitive Content Parameters: It should be able to Mask values of sensitive parameters (for example, passwords, credit card and social security details).
- WAF should support for IPv4 and IPv6 traffic.
- The proposed WAF should support signalling mechanism based on IP blocking to the DDoS solution.

Auto Policy Optimization:

- Known Types of Attack Protection Rapid Mode
- Zero Day Attack Blocking Extended Mode
- Security Filter Auto Policy Generation, Full Auto, Auto Enabled, Auto Refinements
- Working in Learn Mode
- Auto Discovery
- Web Crawler.

Following threats should be protected by the proposed WAF solution:

- Parameters Tampering
- Cookie Poisoning
- SQL Injection
- Session Hijacking
- Web Services
- Manipulation
- Stealth Commands
- Debug Options
- Backdoor
- Manipulation of IT Infrastructure Vulnerabilities
- 3rd Party Misconfiguration
- Buffer Overflow Attacks
- Data Encoding
- Protocol Piggyback
- CrossSite Scripting (XSS)
- Brute Force Attacks
- OS Command Injection
- Cross Site Request Forgery (CSRF)
- Hot Link
- Information Leakage
- Path (directory) Traversal
- Predefined resource location
- Malicious file upload
- Directory Listing
- Parameter Pollution (HPP)

The proposed WAF should support the following Security Features/Functionalities:

- Allow List Security Protection feature

- Brute Force Security Protection feature
- Database Security Protection feature
- Files Upload Security Protection feature
- Global Parameters Security
- Protection feature
- HTTP Methods Security Protection feature
- Logging Security Protection feature
- Safe Reply Security Protection feature
- Web Services Security Protection feature
- XML Security Protection feature
- Parameters Security Protection feature
- Path Blocking Security Protection feature
- Session Security Protection feature
- Vulnerabilities Security Protection feature.

The proposed WAF should support the Activity Tracking, which should include the following:

- Mimicking user behaviour
- Dynamic IP
- Anonymity
- Scraping
- Clickjacking.

WAF should support Device Fingerprint technology by involving various tools and methodologies to gather IP agnostic information about the source. Fingerprint information should include the Client Operating System, browser, fonts, screen resolution, and plugins etc.

It should support running JavaScript on the client side. Once a JavaScript is processed, an AJAX request is generated from the client side to the WAF with the fingerprint information.

WAF should support the Historical Security Reporting from Day 1 :

- Customizable dashboards, reports, and notifications
- Advanced incident handling for security operating centers (SOCs) and network operating centers (NOCs)
- Standard security reports
- Indepth forensics capabilities Ticket workflow management
- Centralized Logging, Management, Configuration and Learned Policy Synchronization across proposed WAF Devices
- Should have minimum 100 predefined reports, including perapplication PCI Compliance
  reporting.

B.O.Q.		
S. No.	**Description**	**Number of Units**
1	20*10GE SFP+(All Populated) - Dual AC power supply - 500GB Storage and 5 Gbps throughput.	2

2	Installation, Configuration, 24X7 Premium Support & all related licenses superscription for 5 Years (OEM Premium back to back)	2

Storage Area Network (SAN) Switch (Qty 2), Specification’s:

- The switch should have nonblocking architecture with 64 ports in a single domain concurrently active at 32 Gbit/sec full duplex with no oversubscription.
- The switch should be configured with minimum 24 ports and can be upgarded to 64 ports with PODs.
- The switch should support autosensing 32,16,10 , 8 & 4 Gbit/sec FC capabilities. It should also support optional 10G FC for connecting to WDM devices.
- The switch shall support different port types such as D_Port (ClearLink Diagnostic Port),
  E_Port, EX_Port, F_Port, optional porttype control.
- The switch should be rack mountable in a standard EIA Rack.
- Non disruptive Microcode/ firmware Upgrades and hot code activation.
- The switch shall support advanced zoning and ACL to simplify administration and significantly increase control over data access.
- Switch shall support POST and online/offline diagnostics, including RAStrace logging, environmental monitoring, non-disruptive daemon restart, FCping and Pathinfo (FC traceroute), port mirroring (SPAN port).
- Should provide redundant and hot pluggable components.
- The switch should support automation that simplifies policy based monitoring and alerting.
- The switch should support cable and optic diagnostics that simplify the deployment and support of large fabrics.
- The switch should support 10G FC for DWDM connections.
- The Switch should support Frame-based trunking with up to eight 32 Gbps SFP+ ports per ISL trunk or up to two 128 Gbps QSFP ports per ISL trunk.
- The switch should support Front to back and back to Front airflow , 1U form factor.
- The switch should have industry's most efficient power consumption i.e.0.10 watts/Gbps ; 204 W with all 64 ports populated with 48×32 Gbps SFP+ SWL optics and 4× (4×32 Gbps) QSFP SWL optics.
- The switch should have industry's lowest latency 700 ns through cut through routing technology or even lessor.
- The switch should have maximum 15,360 dynamically allocated buffers.
- The switch shall be optionally supplied with a GUI management software, capable of managing more than 36 fabrics and 15000 ports.

B.O.Q.		
S. No.	Description	Number of Units
1	Unified Storage System	1
2	Power Cable,India BIS	4
3	SAN Switch,24-Pt 32G SW SFP	2
4	4-Post Rail Kit	2
5	FC Cable ,5m,LC/LC,Op	48
6	Installation, Configuration and all Support upto 5years (OEM Premium back to back)	1

Centralised 100 + 4 TB Storage, Specification's:

Storage Quality Certification: The Storage OEM should be established in the Gartner Leader Quadrant for at last five years.

Storage Controller: The Storage system must have at least two controllers running in an active-active mode with automatic failover to each other in case if one controller fails for both NAS and SAN. The storage system should be a true unified architecture with a single Microcode / operating system instead of running different Microcode/ Operating system / Controllers for File & block. All necessary software and hardware required to provide SAN & NAS functionalities must be supplied for the full capacity supported by the storage system.

The system should have minimum 256 GB usable cache (post cache protection overheads) memory across the two controllers with an ability to protect data on cache if there is a controller failure or power outage. The cache on the storage should have 72hrs or more battery backup (OR) should have designating capability to either flash/disk.

NVMe/SSD as Extended Cache: The system must provide capability to use SSD/flash/NVMe as an extended/secondary cache. The system must be supplied with atleast 4TB of SSD/Flash/NVMe for this purpose**.**

Drive Support: The system must support intermixing of SSD, SAS and SATA drives to meet the capacity and performance requirements of the applications. The system must support a minimum of a 470 disks under the supplied dual controllers for scalability purpose.

Protocols: The storage should be configured with FCP, iSCSI, NFS (NFSv3, NFSv4, NFSv4.1) SMB (SMB2 & SMB3) , pNFS protocols for use with different applications. All the mentioned protocols should be natively supported on the same offered controllers.

RAID configuration: Should support various RAID levels like Single parity, Dual parity, Triple parity and Mirroring or equivalent.

Storage Capacity \ Spare Drives:

- 100 TB usable capacity with 10K SAS drives should be configured with Dual Parity protection configured in RAID6 or equivalent configuration which provides minimum dual failure protection in a Raid Group.

- System should be configured with additional 4TB Cache using SSD/ Flash drives.

FrontEnd and Backend connectivity: The proposed storage system should have minimum 8 numbers of 12Gb backend SAS ports and 16 nos. 16Gbps FC and 8 nos. of 10GbE frontend ports available.

Rack Mountable: The storage should be supplied with rack mount kit. All the necessary patch cords (Ethernet and Fiber) shall be provided and installed by the vendor.

Storage Scalability:

- The proposed system should be field upgradeable to a higher model through data-in-place upgrades.
- The Unified Storage should be a true scale-out architecture allowing mixing of Controller/Nodes within same product line with higher configurations. Also, proposed storage system should allow mixing of Hybrid Storage Controllers with All Flash Storage configurations in a same cluster.
- The storage should be configured in Cluster so that new controllers (totaling upto 8 controllers) can be added to the existing cluster on-line.
- Unified Storage system should allow re-usage of Disk Shelves with higher models of the same product line.

Storage functionality:

- The storage shall have the ability to expand LUNS/Volumes on the storage online and instantly.

- The storage shall have the ability to create logical volumes without physical capacity being available or in other words system should allow over-provisioning of the capacity. The license required for the same shall be supplied for the maximum supported capacity of the offered storage model.

- The storage should be configured with Quality of Service feature.
- The storage shall support logical partitioning of controllers in future such that each partition appears as a separate Virtual storage in itself.
- The proposed storage system should be configured to provide data protection against two simultaneous drive failures.
- The required number hard disks for parity & spares, should be provided exclusively of the usable capacity mentioned. At least 2 drives should be configured as spare drives with the subsequent disk types
- System should have redundant hot swappable components like controllers, disks, power supplies, fans etc.

Point-in-times images:

- The storage should have the requisite licenses to create point-in-time snapshots. The storage should support minimum 250 snapshots per volume/LUN. The license proposed should be for the complete supported capacity of the system.
- The system should support instant creation of clones of active data, with near zero performance impact.

Management:

- Easy to use GUI based and web enabled administration interface for configuration, storage and replication management and performance analysis tools.
- The solution should also include storage manageability software to generate performance graphs, utilization reports, centralized monitoring for multiple storage systems and should be able to send alerts over e-mail in case of any warning/error event generation.

OS support:

- Support for industry-leading Operating System platforms including: LINUX , Microsoft Windows, HP-UX, SUN Solaris, IBM-AIX, etc.
- Any Multipathing software required for the solution must be supplied for unlimited host connectivity.

Operational Efficiency: (De-Duplication and Compression) Proposed storage should support block level data de-duplication and compression for all 3 types of disks (SSD,SAS,NL-SAS) and for all kinds of data (structured & unstructured). If the proposed system doesn't support both de-duplication and compression for all 3 types of disk, please propose double (2X) capacity to compensate the benefits of same.

Data Security: The storage system should have capability to keep Data encrypted both at rest and in motion. All necessary software and hardware required to achieve these functionalities must be supplied for the full capacity supported by the storage system.

Warranty & AMC: The Hardware and software quoted should have 5 years support along with upgrade and updates**.**

“Faulty Hard disks shall not be returned back.”

B.O.Q.		
S. No.	**Description**	**Number of Units**
1	Unified Storage System	1
2	Front-End Ports –16 Gbps FC	16
3	Front-End Ports - 10GbE	8
4	Back-end SAS ports 12 Gbps	8
5	100TB Usable capacity with 10K SAS including 2 hot spares	1
6	Installation, Configuration and all Support upto 5years (OEM Premium back to back)	1
7	Required cables & rail kits	1

5070" Monitor/screen LED displays (Qty 6):

- Active screen diagonal 55 inch
- Resolution (px) 1920 x 1080
- Pixel pitch 1,91mm or more
- Pixels per tile 320 x 180 px (HxV) or more
- LED lifetime 100.000h (video) or more
- Processing 16 bit or more
- Colors 281 trillion or more
- Refresh rate 3.840 Hz or more
- Hor. viewing angle minimum 155° +/5° (@50% brightness) □ Vert. viewing angle minimum 145° +/5° (@50% brightness)
- Power consumption 271W/m²(typ.) or lessor
- Operation power voltage 100240V / 5060Hz
- Operational temperature 10°C to +40°C / 14°F to 104°F
- Operational humidity 1080%
- Size (mm) 1213.53 x 683.05 x 102.36
- Serviceability Front service only

- Certifications CE, UL/ETL, FCC class A, CB, RoHS, WEEE, REACH, CCC
- Warranty Installation & Configuration upto 5 years (OEM Premium back to back)

NMS/ EMS, Gate pass, Ticket login system Software, Specification's:

- All in one integrated solution with Fault and Performance management along with NCM.

  Web based GUI for easy access with no client installations required. FCAPS based monitoring & management.
- Agent less deployments using standard protocols.
- Modular and Distributed architecture o Multilevel distribution support with local and centralized access.
- Support for remote operations on local servers.
- Secure data transfer between remote and central servers.
- Scalable solution with multi location expansion.
- Easy adaptation to new devices / applications.

Fault Management:

- Immediate fault detection via polling & traps.
- Multilevel threshold with colorcoded severity types.
- Generic thresholds. Multimode notification with escalation.
- Inbuilt autocorrelation mechanism for RCA.
- Holdtime support to neglect false alerts.
- Instant diagnosis options with auto correction triggering. Status propagation to all levels of network.
- Syslog management with extensive filtering and alerting options.

Performance Management:

- Multiaspect performance tracking for proactive management.
- Network performance.
- System performance.
- Server performance.
- Maintenance of historical data for indepth analysis.
- Flexible dashboards for multiangle information.
- Multilevel data aggregation of network.
- Extensive Performance based reports.

Inventory Management:

- Complete network asset management.
- Consolidated Node View for viewing both Performance & Inventory data.
- Agentless data capturing.
- Audit reports for complete network.
- User friendly search and filter options.

Flexible & Customizable Reports :

- Highly Informational preconfigured reports.
- Strong, fully configurable, reporting module.
- Option of generating multiple reports in parallel for comparison and analysis.
- User specific access to reports.
- Scheduled automatic Reports directly sent by the system.

- Report copying.
- Multiple graph support (Trend, Bar, Pie, Area etc.).
- Export to multiple formats like PDF, Excel etc.

Customizable Dashboard:

- Configurable dashboards.
- Wide variety of Widgets to configure.
- Copy Dashboard.

Network Configuration & Change Management:

- Scheduled Backup of Device Configurations.
- Download both startup and running configuration.
- Configuration Change Comparison with colorcoded highlighting.

Baseline Tagging of Stable Configurations.

- Notifications on Configuration Changes.
- Option to upload Configurations.
- Reports.

Portal Views:

- Dashboard.
- Maps (SVG Maps, Topology/Flat view, Geo Maps & Network diagram as a service).
- Alarm Dashboard. Events / Traps / Syslogs.
- Node view.
- Resources.

Notification and Escalation:

- Multimode notification.
- Rule based alerts.
- SMS, email, batch, syslog. SNMP trap, XML, etc.
- Multilevel escalation support.
- Support for bulk notifications by grouping based on: Time periods & Nodes / Devices.

Robust Discovery of Resources :

- Topology Discovery.
- Scheduled Automatic Discovery. CSV based Discovery.
- Support for wide range of Protocols such as SNMP v1,v2c, and v3, WMI, Netflow,
- CORBA, Syslog, SSH, HTTP, HTTPS, FTP, SMTP, POP3, Trace route, ping, CDP, NDP, Spanning Tree, MPLS proxy ping, Cisco SAA etc.. VM Discovery.

User Friendly Tools: PING. SNMP Walk.SNMP Set.Trace Route.SSH.Telnet .MIB Browser.

Self Monitoring Capability:

- Health Check.
- Usage Tracking.
- Resource Details for load monitoring.
- Process Details provides instance details.
- Thread Status View to monitor internal threads.
- Parameters for UIbased application tuning.
- Database Status to view DB details.

Personalized Accounts & Role Management:

- Role based preference.
- User Groups.
- User Accounts.
- Logged in Users.

Enhanced File Format Support: PDF Export. Excel/CSV Export.
Comprehensive Security:

- Encrypted Password.
- Rolebased Access Privileges & DES Encryption.

Flexible Deployment Architectures:

- Single Server Deployments.
- Distributed Deployment architecture for load balancing.
- MSP architecture with inbuilt replication to aid RIMSbased monitoring.

Data Management:

- Configurable data purging thresholds.
- Database Backup and Restore Help.
- Online Help. Tech Support Contact.

Key Monitored Performance Statistics : Network Availability.

- Application Availability.
- Resource Availability. Database Availability.
- Network Utilization.
- Network Throughput.
- Error Traffic.
- Overflow traffic.
- CPU Utilization.
- Disk Utilization.
- Memory Utilization.
- Buffer Overflow.
- Latency. Packet Loss. Jitter. Ping Response time.
- Web Response Time.
- DNS Response Time.
- Email Response Time & FTP Response Time And many more..

Supportive Network Devices: Cisco Networks,Juniper Networks , Avaya Networks ,Foundry Networks, Extreme Networks ,Alcatel Routers ,Network Printers ,Power backup devices ,Etc.
Servers Network OS : Windows Servers,Unix Servers,Linux Servers ,Solaris Servers ..

Supportive RDBMS: MySQL. MSSQL.Oracle. **Supportive Hypervisors:** VMWare,vCenter, XenServer ,Nutanix . **Supportive Services**: DNS, IMAP2, NTP, SMTP ,JBoss ,HTTP ,POP ,NNTP ,SNMP ,FTP ,NFS ,Radius ,SSH ,Oracle ,Syslog.

B.O.Q.		
S. No.	**Description**	**Number of Units**
1	Network Devices Complete Monitoring	1000
2	Network Configuration Management	100
3	Virtualization Monitoring	100
4	Ping Devices Monitoring	3000
5	Wi-Fi & IP Phones	1000
6	NetFlow Analyser	5000
7	Help Desk Tool with 10 process Pink Elephant	1
8	Helpdesk Technician	50
9	Installation, Configuration & all support upto 5 years (OEM Premium back to	1

	back)	

Centralised Backup Software (Storage capacity-based license for 10TB), Specification’s:

- Proposed solution should be available on various OS platforms and be capable of supporting backup/ restores from various platforms including Windows, Linux and Solaris. Both Backup Management Server, Media Server and Client software should be capable of running on all these platforms.
- The Proposed Backup software Must be present as Leaders in Gartner’s Magic Quadrant for backup software report consistently from last 10 years.
- Proposed Backup Software should be capable of supporting SAN based backup using client footprint instead of additional media/storage server footprint which takes more server resources for backups from various platforms including IBM AIX, HPUX, Linux, Solaris and Windows.
- Backup Solution should support various level of backups including full, incremental, synthetic, optimized synthetic and user driven backup along with various retention period.
- Backup Software must provide Source (Client & Media Server) & Target base data Deduplication capabilities. It should provide Global deduplication across backup jobs and different workloads.
- Proposed Backup Software must provide both Fixed Length and Variable Length Data Deduplication to allow users choose the dedup option based on the backup workload.
- The proposed Backup Solution must offer capacitybased licensing. The license should be proposed for 10TB frontend data capacity with all Operating System and Database online backup Agents included.
- The proposed backup solution must include Agent/Modules for online backup of files, applications and databases such as MS SQL, Oracle, DB2, Sybase, MySQL, PostgresSQL, Exchange, Sharepoint and distributed databases/filesystems like NoSQL, MongoDB, Bigdata and hadoop.
- Proposed solution must provide Bare Metal Recovery, deduplication, encryption, database online backup, deduplication, backup data replication etc. with installation of single agent on clients. Multiple Agents/Binaries should not be installed on the production Servers to achieve all above features.
- Proposed Backup software should be certified to protect applications and workloads deployed in docker Containers.
- Backup Solutions should have capabilities to tape/diskout backup catalog and deduplication catalog separately. Also should be able to replicate all catalog information along with replication of backup images to DR site.
- Backup solution should have integrated SourceSide and TargetSite data de-duplication engine with multivendor storage support to save deduplication data. The deduplication engine should also facilitate IP base replication of dedupe data; without any extra charge.
- Solution should be proposed along with OEM professional services for onetime installation direct by OEM Vendor.
- Backup solution should not have any special disk (SSD) requirement for Deduplication even for large datasize (100+ TB data). Deduplication feature should work with SAS, SATA and nearline SATA low cost disk technologies.
- Proposed backup solution must support ESX backup in nonwindows environment, even without the need of windows backup server. There should not be any limitation from media server on supporting number of ESX/virtual guest host per media server.

- Backup solution to support Cloud/object storage as Backup Target over generic S3 protocol.
- Proposed backup solution should be provided with integrated DR orchetation tool which can automate the recovery of Virtual Machines between DC and DR site if required.
- Proposed Backup Solution should provide optimized deduplicated replication and reverse replication of Backup Images between source and target site.
- Backup Solution must have integrated data classification and file analytics which can identify stale, risky and unnecessary data to be addressed for data privacy compliance using backup Metadata source.
- Installation, Configuration & all support upto 5 years

B.O.Q.		
S. No.	**Description**	**Number of Units**
1	Installation, Configuration & all support upto 5 years (OEM Premium back to back)	1

Wifi Controller (Qty-2) & Access Points (Qty-250) Specifications:

Specification for Wireless controller:

General:

WiFi Controller can be integrated with UTM or can be an independent appliance.

Wireless Controller:

- The appliance should support wireless controller feature for at least 256 Access Point
- The appliance should support IEEE 802.11a/b/g/n/ac standardsbased wireless Access Points
- Supports strong Authentication and Encryption Standards Include Open/ WEP64/ WEP128/ Shared, Guest Captive Portal, WPA /WPA2 802.11i Preshared key,WPA / WPA2 802.11i with Radius support
- The wireless controller support the following types of client load balancing:
  - a) Access Point Handoff the wireless controller signals a client to switch to another access point. o b) Frequency Handoff the wireless controller monitors the usage of 2.4GHz and 5GHz bands, and signals clients to switch to the lesserused frequency automatically
- Allow IP connectivity between the Controller and the APs for external VLAN routing where the Controller and the APs are on different management VLANs

- The wireless controller should include the following features.
  - Wireless guest management o Captive portal with Email capture login o Wireless Mesh, Bridging Features o BYOD (Bring Your Own Device) Support o User and application control o Encrypted Remote Access point support o Content security and filtering

- BYOD should be having below features
  - Detect client device Mac address, device type(such as windows device, Android device, Iphone, Ipad, blackberry, etc) and host name

- o Controller should be able to allow or deny traffic based on device type (such as windows device, Android device, Iphone, Ipad, blackberry, etc) or user or both
- o Controller should be able to block or allow websites and applications based on device type(such as windows device, Android device, Iphone, Ipad, blackberry, etc) or user or both

- Controller should be able controll the bandwidith based on device type(such as windows
  device, Android device, Iphone, Ipad, blackberry, etc) or user or both

- The wireless Controller should support the following RF Management features o Having Automatic Channel Allocation o Having Automatic Power Control
  - o Supporting Neighbourhood scanning of RF environment to minimise neighbouring AP interference and leakage across floors.
  - o Having Coverage Hole Detection o Providing alerts when APs are down or compromised RF environment is detected o Having Self healing Automatic neighbouring AP power increase to fill in for coverage losses

- The wireless Controller should support Rogue AP detection and Blocking Should support Spectrum Analysis

Interface and Connectivity:

- Should have at least 4 10/100/1000 Ethernet ports
- Should have 1 x 10/100/1000 Gigabit Interfaces for Management
- Should have 1 console port

Network/ Routing:

- Should support Static routing.
- Should support IPV6 Policy based Routing Authentication:
- Should have authentication for Users/Admins (Local and Remote – RADIUS, LDAP & TACACS+)
- Should support PKI / Digital Certificate based two factor Authentication for all type of -
  users

Encryption /VPN:

- Should support protocols such as DES & 3DES, MD5, SHA 1, SHA 256 authentication, - -
  Diffie Hellman Group 1, Group 2, Group 5, Group 14,-
- Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm, The new encryption standard AES 128, 192 & 256"
- IPSec VPN should support XAuth over RADIUS and RSA SecurID or similar product.
- Should have integrated SSL VPN with no user license restriction. If license is required
  add license for 20 concurrent SSL VPN users
- Should also support PPTP and L2TP over IPSec VPN protocols.

Specification for Wi FI Access Point:

Architecture:

- The Access Point should support IEEE 802.11a/b/g/n/ac Wave2 standards
- Should have the dual radio option and should be able to support devices on 2.4GHz and 5 GHz simultaneously.
- Should support radio1 as 2.4 GHz b/g/n and radio2 as 5 GHz a/n/ac
- Should have at least 4 Internal Antennas
- Should have minimum 1 x 10/100/1000 PoE Interface.
- Should support Power over Ethernet (PoE) 802.3af ((12.9 W)
- Access point should support Wave 2 2x2 MIMO with 2 spatial streams.
- The access Point should support throughput in Radio 1: Up to 300 Mbps, and Radio 2: Up to 867 Mbps

Mobility:

- Should support L2 and L3 wireless controller discovery Should support auto-selection of RF channel and transmit power
- Access point must have following wireless monitoring capabilities:
    - Frequencies scanned for 2.4 and 5 GHz o Background scan with client access on 2.4 and 5 GHz o Fulltime scan as dedicated monitor o Full-time scan with client access on 5G GHz o Should support one radio for air monitor and another radio for client access.
- WME Multimedia Extensions support 4 priority queues for voice, video, data and background traffic
- Certified by the WiFi Alliance’s WiFi Multimedia™ certification program
- Should support 16 Simultaneous SSIDs
- Should support following EAP types: EAPTLS EAPTTLS/MSCHAPv2 EAPv0/EAP MSCHAPv2 PEAPv1/EAPGTC EAPSIM EAPAKA EAPFAST
- Should support selfhealing, selfoptimizing local mesh extending network availability to areas without an Ethernet infrastructure. Include if any license required
- Should support transmit BeamForming
- Should support Peak antenna gain of minimum 4 dBi for 2.4 GHz, 5 dBi for 5 GHz"
- Should support atleast 23dBm Transmission Power
- Should support Local AP diagnostic web portal
- Access Points must support Hardware based DTLS encryption on CAPWAP Standard
- Should have physical security lock (such as Kensington lock)

Management:

- Should be centrally managed through the wireless controller
- Should support DNS based Controller discovery, DHCP Based Controller discovery and static discovery
- Should support webbased secured management interface
- Should support Command line(CLI) to access point
- Should support mounting options of Ceiling, TRail and wall all these accessories should included with box. If not quote all mounting kit.

Environment:

- Operating Temperature 32 – 104 ˚F (0 – 40 ˚C)
- Access Point must be WiFi Alliance Certified
- Low Voltage Directive , RoHS complaint
- Access point should have the Power Consumption 7.8W(Average) and 15.72 W(Maximum)

Controller B.O.Q.		
S. No.	Description	Number of Units
1	18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 16 x GE SFP slots, SPU NP6 and CP9 hardware accelerated	2
2	Installation, Configuration & all 24x7 support upto 5 years (OEM Premium back to back)	2

Access Point B.O.Q.		
S. No.	Description	Number of Units
1	Indoor wireless wave 2 AP - dual radio (802.11 a/b/g/n and 802.11 a/n/ac, 2x2 MU-MIMO), 1 x GE RJ45 port, Ceiling/wall mount kit included. 4 internal antennas, Order 802.3af PoE injector GPI-115. For AC power adapters	250
2	Installation, Configuration & all 24x7 support upto 5 years (OEM Premium back to back)	250

A.V. (Endpoint protection), ((Qty -1500 Licenses) 1000 License for Ubuntu & 500 for Windows)) Specifications:

- OEM should be capable to cater endpoint protection for Window’s, Ubuntu & Linux environment.
- The proposed solution should be positioned in the leader quadrant from last three published Gartner Magic quadrant report for Endpoint Protection
- Solution should support Stateful Inspection Firewall, AntiMalware, Deep Packet Inspection with HIPS, Integrity Monitoring, Application Control & log inspection in a single agent
- Solution should support realtime and schedule malware Scans
- Proposed solution should protect against distributed DoS attack and should have the ability to lock down a computer (prevent all communication) except with management server.
- Firewall rules should filter traffic based on source and destination IP address, port, MAC address, etc. and should detect reconnaissance activities such as port scans and Solution should be capable of blocking and detecting IPv6 attacks and Product should support CVE cross referencing when applicable for vulnerabilities.
- Host IPS should be capable of recommending rules based on the existing vulnerabilities and also protect the vulnerability with the virtual patching

- HIPS solution should also be also to schedule the recommendation scan to remove (patched vulnerability using the OEM issued patch and add new virtual patching signatures against the newly discovered vulnerability
- Host based IPS should support virtual patching both known and unknown vulnerabilities until the next scheduled maintenance window.
- The solution should have the application control feature to lock down the server to stop execution of other nonwhitelisted applications
- Solution should have Security Profiles allows Integrity Monitoring rules to be configured for groups of systems, or individual systems.
- Demonstrate compliance with a number of regulatory requirements including PCI DSS, HIPAA, NIST, SSAE 16
- Should be Common Criteria EAL 4 and FIPS 1402 validated
- Container security automated processes for critical security controls to protect containers and the Docker host. Bake security into the CI/CD pipeline for frictionless automation
- APIfirst, developerfriendly tools to help you ensure that security is baked into DevOps processes
- HIPS Solution Should not has the need to provision HIPS Rules from the Policy Server as the Rules should be automatically provisioned and de provisioned
- OEM of proposed solution should have local 24x7 TAC support in India
- Installation, Configuration & all support upto 5 years

Blade Enclosure Description (Qty 1):

Specification :

Make : HPE

Model No. : Blade System C7000 Enclosure G3

Description: Blade System C7000 Enclosure G3 Containing 10 cooling FAN, 6 (HP 2400W 80 PLUS PLATINUM) Power Supply , 2 (HP VC FlexFabric 10Gb/24-Port Module) , 2 (c7000 DDR2 Onboard Administrator with KVM)

ANNEXURE-'D'

Supreme Court of India
Admn. Material (P & S)

F. No.: Data Center/2019
Dated : 15th February, 2020

Last date for Submission of Tender: 06th March, 2020 up to 03:00 p.m.

NOTICE INVITING TENDER FOR SUPPLY OF DATA CENTER HARDWARE

(Proforma to be filled by the Tenderer)

Financial Bid

Sl. No.	Item	Quantity	Price Per Unit In Lakhs	GST % Extra Applicable in lakhs	Total Net Price Per Unit in Lakhs
1	Modular Rack's				
2	Rack Servers With Windows 2012 Server R2 Std & VM Ware				
3	DDoS's				
4	Next Genration Firewalls				
5	Anti APT Appliance(On Premise)				
6	Server Load Balancer's				
7	Web Application Firewall's (WAF)				
8	Storage Area Network (SAN) Switch's				
9	Centralised 104 TB Storage				
10	5070" Monitor/screen LED displays				
11	NMS/ EMS, Gate pass, Ticket login system Software				

12	Centralised Backup Software (Storage capacity based license for 10TB)				
13	Wifi Controller & Access Points				
14	Four resident engineers for one year				
15	All Documentation & Training to the SC-CC Staff	Service			