HIGH COURT OF SIKKIM

GANGTOK

No.: 173/HCS/COMP/477 **Date: 13/01/2025**

The High Court of Sikkim invites sealed quotations from registered and authorized and experienced Distributors/Dealers/Suppliers of reputed brand for **Supply, Installation, Commissioning, Testing and Maintenance of high-performance Servers and other networking items to be installed at High Court of Sikkim**.

The last date for receipt of bid is **03.02.2025**. The bid shall be opened on **05.02.2025** in the office of the Central Project Coordinator, or any other officer authorized in this behalf by the Competent Authority, High Court of Sikkim. The bid shall be sealed in an envelope as described hereinafter and sent by post to the office of the Central Project Coordinator, High Court of Sikkim, Sungava Road, Pin-737101 or in person at the Office of the Registrar/Registrar (Judicial Service) during working hours. Bids received after the stipulated date and time, for reasons whatsoever, shall not be taken into consideration and will be summarily rejected.

1. The summarized component wise details is as under:

Sl. No	Items	Quantity	Technical Specification **(ANNEXURES)**
1.	2U Rack Server	1	A
2.	Racks	1	B
3.	Storage Network Attached Storage (NAS) 500 TB	1	C
4.	Network 48 port Switches	2	D
5.	Firewall	1	E

2. Scope of work: Supply, Installation, Testing, Commissioning, on-site maintenance & Support for five **(05) years**.

3. Bid Security/Earnest Money Deposit:

The bidder has to submit an interest-free Bid Security/ Earnest Money Deposit (EMD) of **₹10,37,500/-** *(Rupees Ten Lakh Thirty Seven Thousand and Five Hundred only)* in the form of a Cheque /Demand Draft drawn on a Nationalized Bank in favor of the **Central Project Coordinator, High Court of Sikkim** payable at Gangtok at the time of submission of bids.

a) Unsuccessful bidder's EMD shall be refunded back will be returned without any interest as promptly as possible.

b) The Bid Security of the successful bidder shall be returned, without any interest, only after the submission of their acceptance against the issued award of contract within the stipulated time period and furnishing of the Performance Bank Guarantee @5 % of the total order value.

4. Bid Price:

The Bidders would have to quote the prices in Rupees only, for the total scope of work including Supply, Installation, Testing and maintenance of Servers and other hardware as mentioned above. No separate itemized bids will be accepted. The Bidders are advised not to indicate discount separately. Discount, if any, should be mentioned in the quoted prices. The Price quoted should be inclusive of GST and all other applicable Taxes/Duties.

5. Licensing Requirements

a) All system software, licenses, etc. have to be procured in the name of the High Court of Sikkim.

b) The system software licenses mentioned in the Bill of Materials shall be genuine, perpetual, full use and should provide upgrades, patches, fixes, security patches and updates directly from the OEM.

c) A comprehensive warranty that covers all components shall be issued after the completion of the work by the successful bidder. The warranty should cover all materials, licenses, services, and support for all the related software, patches upgrades. The warranties shall be with serial number and warranty period.

6. Installation Process

a) During installation at site, if any item is found to be defective or broken, it will be replaced with new one by the vendor at its own cost and risk immediately.

b) Consolidated Installation Report, based on the successful installations of the individual items, shall be submitted to the High Court of Sikkim along with the bills.

7. Site Visit by interested eligible bidders: If required the bidder may visit the installation site i.e. High Court of Sikkim on prior intimation to the Computer Section of the High Court and obtain information at its own responsibility and risk. The costs of visiting the office shall be at the bidder's own expense. However, failure of a bidder to visit the site will not be a cause for its disqualification.

8. Right to Accept and Reject the Bid

Notwithstanding anything contained in this document, the Competent Authority, High Court of Sikkim, reserves the right to accept or reject any bids including the proposal of the lowest bidder in accordance to the policy in the subject. Likewise, they also reserve the right to cancel the bid process at any time prior to signing the contract.

9. Payment terms:

a) No advance payment will be made.

b) The final payment shall be made after completion of the work.

10. Superscripting quotation Proposal Envelope:

The Bidders shall submit their Bids in three separate sealed envelopes in the following format:

a) **COVER A** containing Earnest Money Deposit should be sealed in a separate envelope subscribing “ **EMD**”;
b) **COVER B** containing **TECHNICAL BID** should be sealed in a separate envelope subscribing **“Technical Bid”**.
c) **COVER C** containing **FINANCIAL BID** should be sealed in a separate envelope subscribing “**Financial Bid**”.

All the above mentioned three envelopes together should be enclosed and submitted in a properly sealed separate envelope mentioning the name of the quotation as “**SERVERS BIDS**” along with the Quotation Ref. No. If any Bidder deviates from submitting its Bid in this prescribed format, the Bid shall be summarily rejected and shall not be taken into consideration for evaluation.

11. Submission of Documents:

The following documents are also to be submitted by the Bidders in the envelope ‘**COVER-B’** along with the Technical Bid:

a) Bidder’s Profile.
b) Documents in proof of GST Registration, TIN No, TAN No. and PAN No.;
c) Last three years Income-tax Clearance Certificate, if applicable;
d) Audited Balance sheets of last three years;
e) The bidder’s annual financial turnover during last three Financial Years.
f) Self-declaration on a duly Notarized Affidavit in a Stamp Paper of Rs.200/- that the Bidder has not been blacklisted by any High Court of the Country/Central/ State Government/ Public Sector Undertaking/ Autonomous Bodies under Central and State Governments in India.
g) Proof of office address.
h) Original Equipment Manufacturer (OEM) and Manufacturer’s Authorization Form(MAF) Compliance
i) Technical proposal indicating Make, Model and manufacturing year of items offered with detailed specifications.

12. On-site Warranty & Maintenance:

a) The onsite comprehensive warranty for the same shall be for minimum of **05 (Five) years**. Same to be calculated from the date of installation.

b) All cost of repairs/replace such as additional spare parts, patches, labor, transportation cost and any software updates/upgrades required to run the aforementioned hardware items shall be included in the warranty of the product at **<u>no extra cost</u>**.

c) Preventive Maintenance Service: Free onsite quarterly preventive maintenance service shall be provided by Seller during the period of warranty.

13. Service & Support:

a) The bidder must be able to provide service and support within 24 hours of reporting of a fault in the devices so that no any delay is caused in restoring the fault. Also, a Company Authorized Service Centre at Gangtok must be available.

b) In case of non-availability of service center at Gangtok (Capital City),the selected bidder shall empanel or authorize such service centers at Gangtok for maintenance and support.

c) Bidder has to complete the required Service / Rectification within 24 hours or a maximum extension of seven days days time which may be considered by the High Court of Sikkim in its discretion. If the successful bidder/awardee of the work fails to complete service / rectification with defined time limit, a penalty of 0.5% of Unit Price of the product shall be charged as penalty for each week of delay from the seller during the warranty period. No extra charges viz. hardware installation, maintenance, TA/DA will be paid.

14. Delivery & Installation

a) Delivery and installation will have to be done within 15 days from the date of issuance of work order.

b) The successful bidder has to do all the installation including civil works *viz*, laying of electrical cabling, network cable, etc whichever would be required for installation and commissioning.

c) All aspects of safe transportation of Goods and Material at installation site shall be the exclusive responsibility of the successful bidder.

d) The successful bidder should install and make his own arrangement for loading and unloading the goods at specified site without any additional charge.

e) Any deviation found in the specifications of the delivered goods from the tender specification, will lead to cancellation of the work order.

15. Terms and Conditions

a) Bidders are advised to study all technical and commercial aspects, instructions, forms, terms and specifications carefully in the said quotation document. Failure to furnish all information required in the Tender Document or submission of a bid not substantially responsive to the tender document in every respect will be at the Bidder's risk and may result in the rejection of the bid. It will be imperative on each bidder to fully acquaint himself with all the local conditions and factors, which would have any effect on the performance of the contract.

b) This tender document is not transferable

c) Consortium, Outsourcing and Subcontracting is not allowed at any stage of the project.

d) The High Court of Sikkim is not liable to bind itself for selecting L1 bid.

e) No Hardware/Software will be provided by the High Court. The successful Bidder is required to set-up all the necessary hardware/software at its own cost at the specified locations.

f) The High Court of Sikkim may terminate the agreement if the work done is not satisfactory without further liability.

g) The bidders while bidding are expressly required to mention all the terms and condition of this tender document or sign each and every page of this tender document and all the Annexures A to E, which shall be considered as acceptance of all the terms of this tender document.

sd/-
Benoy Sharma(SSJS)
CENTRAL PROJECT COORDINATOR
e-Courts Project

Annexure A

SN	Description	Specification	Complied (Yes/No)
1	Form Factor	Rack Mount (Maximum 2U)	
2	Processor Make	x86 Architecture processor	
3	Max. Number of sockets available on chipset	To be mentioned by Vendor	
4	Max. Number of sockets populated with processor	Two (2)	
5	No. of Processor	Two (2)	
6	Processor Configuration	64-bit x86 processor fully binary compatible to 32-bit applications	
7	Number of cores per Processor	24 or more	
8	Processor base frequency	2.8 GHz or higher	
9	Chipset compatible with CPU	Yes (To mention chip set of Processor OEM)	
10	Motherboard (OEM compatible with CPU)	OEM	
11	PCI Slots (Express Gen 3.0 min.)	One Free	
12	Max Nos of PCI Lanes	To be mentioned by Vendor	
13	Memory (DDR4 RAM min.) (GB)	1.0 TB, DDR4-2666 or better	
14	DDR4 RAM upgradable up to (Minimum) (GB)	3.0 TB	
15	DIMM Slots (Minimum) (No.)	16/32	
16	Hard disk drive Capacity (GB)	480GB x 3 for OS and 4x1.92 TB SSD-SAS 12Gbps or better	
17	Hard disk drive RPM with SAS (hot plug or better) (RPM)	Hot Plug	
18	RAID Controller Caches (MB)	2000MB with battery backup	
19	RAID Controller	12 Gbps SAS RAID controller supporting RAID 0, 1, 5 and 10	

SN	Description	Specification	Complied (Yes/No)
20	RAID Controller Ports	8	
21	Video Controller (support VGA or above resolution)	Yes	
22	Keyboard	No	
23	Mouse	No	
24	Monitor	No	
25	Bays (min. 2 internal or more hot plug)	5	
26	USB Ports (version 2.0/3.0)	4	
27	Certifications, Compliance & support by Windows, Red Hat or Novell	OS Certification Compliance: Windows, Linux (RedHat, SuSe, CentOS, Ubuntu) and any other compatible OS Virtualization / Cloud Platform: Microsoft Windows, VMware, OpenStack, Kubernetes Certification for Compliance	
28	DVD ROM (or better)	NO	
29	Networking: dual LAN (10/100/1000) network card	Dual Port 10GbE Base-T Adapter, OCP NIC 3.0 Network Adapter	
30	FC HBA Dual port card	Single port FC HBA Card 16/32 Gbps or higher (Qty – 2) 5M LC-LC cable for each HBA port	
31	FC HBA Dual port card Speed	32 Gbps or higher	
32	Management Features-1	Remoter power on/ Shutdown of server,	
		Remote Management of Server over LAN & WAN with SSL encryption through gigabit management port,	
		Should have virtual Media support with all required licenses.	
		Remote KVM	
		Server Health Logging	
		Out of Band Management	
33	Management Features-2	Management of multiple Servers from single console with single source of truth	

SN	Description	Specification	Complied (Yes/No)
		for multiple sites.	
		Automated infrastructure management for patch upgrades, version upgrades, etc.	
		Simplified management with analytics driven actionable intelligence	
		Intelligence System tagging giving admin flexibility to provide metadata tags to each System to enable users to filter and sort systems based on user-assigned attributes	
		Hardware Profile based deployment to multiple Servers simultaneously	
		Policy template for deployment of single policy to multiple Servers simultaneously	
		Platform inventory and health status	
		Server utilization statistics collection (including firmware updates and diagnostic tools	
		Should provide an alert in case the system is not part of OEM hardware compatibility test	
		Solution should be open and programmable providing Rest API, SDK for programming languages like Python, power shell scripts etc.	
		Should have customizable dashboard to show overall faults/health/inventory for all managed infrastructure the solution should provide option to create unique dashboards for individual users.	
		the user should be flexibility to select name for dashboards and widgets (viz. health, utilization etc)	
		Single pane of glass for auto Provisioning across Multi vendor & multi hypervisor platform	
		Self service portal deployment for automated provisioning	
		Real-time out-of-band hardware performance monitoring & alerting	
34	Security Features-1	Secure Boot (Firmware and Bios Level Security)	
		Provision to lock the system on breach	
		Hardware root of trust/Dual Root of Trust	

SN	Description	Specification	Complied (Yes/No)
		Server should provide policy based security	
		Server should provide server intrusion detection,	
35	Security Features-2	Provision for Cryptographic firmware updates	
		Capability to stop execution of Application/Hypervisor/ Operating System on predefined security breach	
		Secure /Automatic BIOS recovery	
		Network Card secure firmware boot	
		In case of any security breach system should provide the lock down feature	
36	Redundant Power Supply	Redundant Power Supply should be Platinum Efficiency and hot Swappable	
37	Redundant Fan	Yes	
38	Server scalability to be achieved within the box & without adding nodes	Yes	
39	BIS Registration no. under CRS of Deity	Yes	
40	Declare max. power consumption of the system	Yes	
41	Availability of documentary evidence in support of model quoted in commercial production & due evaluation completed	Yes	
42	Details of benchmark indices with software & diagnostic software used to test server.	Processor SPEC CPU2017 benchmarked with SPEC rating of at least (350 - SPECrate2017_int_base score and 325 - SPECrate2017_fp_base scores). Benchmark rating of quoted processor for quoted model should be published on SPEC.ORG on date of bidding.	

SN	Description	Specification	Complied (Yes/No)
	Benchmark report (snapshots and full description report) should be submitted (for an exactly same configuration as what is being quoted) along with the bid.		
43	Server main supply 200V to 230V		
44	CE or UL certified or Ertl/Etdc certified for safety (IEC-60950-1)	Yes	
45	RoHS Compliance	Yes	
46	Warranty	Five(5) YearsOEM onsite comprehensive warranty Acceptance Testing before delivery Root of Trust Security Enabled. Due to security reasons defective HDD will not be returned back on replacement.	
48	MAF from OEM is Required	Yes	

Note: All the above specifications should be read as equivalent or higher.

Annexure B

SN	Parameter	Minimum Specifications	Complied (Yes/No)
1	**Scope of Work**	This specification covers Intelligent Integrated Mini Data center Infrastructure, standalone system design, engineering, manufacture, assembly, testing at manufacturer's works, supply, delivery at site, unloading, handling, proper storage at site, erection, testing and commissioning at site of complete infrastructure for the proposed Smart Rack solution to be installed at Customer as detailed in the specification, complete with all accessories required for efficient and trouble-free operations	
		The critical components of the Mini Data center solution can be maintained easily in the events of failure. All the components of the infrastructure should be such that it can be easily dismantled and relocated to Different Locations.	
		The Integrated Mini Data center Solution of 3 Nos of 800mm Width x 1400mm Depth x 2100mm Height with inbuilt hot and cold aisle containment and Each rack should cater IT load up to 7KW with N+N redundancy over the cooling and UPS system.	
		Integrated Mini Data Center Solution essentially should include environmental controls, Side Mounted 200mm Width 1400mm Depth 2100mm height air conditioning with N+N Redundancy, PDU's, smoke detection, Water leak detection and humidity sensors and security devices. Environmental monitoring shall be done from IP based monitoring. Cooling Unit should not occupy any U space inside the Racks.	

		Cooling unit should be Mounted Externally beside the Rack both on LH and RH side with N+N redundancy.	
2	**Side Mounted closed Loop Airconditioning.**	The Mini Data Center should be equipped with side mounted cooling unit to provide closed loop cooling system which should be able to cool the equipment’s uniformly right from 1st U to 42nd U of Rack and it should not occupy any U space and also should not mounted inside the Racks , should be able to maintain the cooling system without disturbing the IT Network systems.	
		Side Mounted Air-Cooling unit should be of 2 nos of 10kW/2TR capacity, Capacity mode topology (02 no. of 10kW rack-based cooling unit). Rack based Air Cooling with indoor - out door design, SHR >0.9, 100% Duty cycle, Inverter Rotary compressor, and should not occupy any U Space inside the racks, Speed Controlled fans, High Pressure & Low-Pressure protection, R407C/R410A Refrigerant.	
		The unit should support indoor to outdoor copper piping distance up to 20 mtrs including vertical piping distance up to 5 mtrs.	
		Unit should have on Stainless Drain Tray for protection for any accidental water leakage	
3	**Power Distribution.**	0U, Vertical Rack PDU, 32A, 230V/230V, 1 phase 7kVA, with 18 no. IEC C13, 06 no. IEC C19, 2.5m power cord with 3P+N+E, Black Powder Coat (02 no. per rack) RAL 9005	
4	**Electrical Distribution System**	Electrical Power Distribution System: (i)Provisioning of structured power distribution system. The 1-Phase commercial conditioned 230V/50Hz power supply will be made available by the user at the Distribution panel along with MCB. (ii)This Main	

		Distribution panel will be used to distribute power to all power consuming devices used in Smart EDGE rack such as: UPS, Air Conditioning system	
		Electrical Metered Power Distribution should be inbuilt with Branch Circuit Monitoring and should monitor all the parameters for each and every Breaker. PDM should Monitor the Information Individual Racks power Data and cooling Units Power Data through Data Center Monitoring Software	
5	**Environmental Controls**	Intelligent Mini Data center should include basic environmental controls: • Smoke Detector • Water Leak Detection system • 3 Zone Temperature Sensor and 1x humidity Sensor • Door Sensor • Alarm beacon and Alarm Lights	
		Rack & accessories 3 Nos	
		Rack is 42U 19" mounting type with 2100 (Height) x 800 (Width) x 1400 (Depth) with safe load carrying capacity of 1400 Kg on enclosure frame and 1000 Kg on 19" mounting angles and should be capable to mount Higher Depth Server and switches.	
		Front Glass door with HMI Interface Panel and rear plane/split door with Emergency Door Opening system incase of High Temperature during cooling Units failure	
		Cable entry provision from top & bottom both side of rack	
		Cut outs with rubber/brush grommet on top and bottom cover of rack for cable entry	
		Vertical Cable manager on both LHS & RHS on rear side	
		Thermally insulated cold aisle chamber	
		70% Blanking panels to prevent air	

		mixing	
		Status based LED light to be provided on each rack	
6	**U Space**	Intelligent Smart rack should have Min 114 U(total) space available for IT equipments and network Equipments.	
7	**Monitoring**:	Detailed Monitoring & Diagnostics monitoring unit Zero U with redundant power supplies & capable of single window monitoring of all the environmental parameters along with air conditioning through a single window dashboard over ethernet & Capable for sending Email Alerts and SMS Alerts.	
		Monitoring unit should integrate & monitor environmental parameters like temperature, humidity, door access, smoke etc. with UPS & cooling unit in a single dashboard along with other environmental parameters like temperature, humidity, smoke etc	
		Air conditioning should be integrated with the monitoring unit to monitor all critical parameters (Cooling unit: Unit status, supply & return air temperature, humidity; UPS (Optional from Same make if supported): Input – Output Voltage, current, pf, battery remaining time, battery charging status) of both the systems in a single dashboard.	
8	**Safety & Security**	Access Control System The system deployed will be rack based access control system based on Biometric Technology for the Front Doors and & rear rack doors will be provided with electromagnetic locks and should be operated through switch Provided inside the Rack, and Rear Door should open during Emergency condition during Cooling units failure..	
		External Mounted Rack based Fire suppression system based on novec	

		1230 should be provided as per the NFPA Standard, Smoke Sensor Nozzles should be positioned properly so that the system should actuate the suppression system incase of fire in order to protect the Racks from fire Safety.	
		01 no. IP Based Camera mounted inside the Rack with 1 TB hard disc and it should take the snap whenever a person opens the Door on the Front side.	
9	**Certifications**	Smart Rack OEM or Manufacturer should be ISO 9001: 2000, ISO 14001, and ISO 45001 certified.	
10	**Warranty**	Five(5) Years Onsite Comprehensive Warranty	
Note: All the above specifications should be read as equivalent or higher.			

Annexure C

SN	Parameters	Minimum specifications	Complied (Yes/No)
1	Storage System Type	Unified Storage	
2	Storage Capacity (TB)	500 TB Usable	
3	Hardware Form Factor of Storage System (RU)	To be provided by vendor	
4	Disk Type	SAS	
5	Speed of dual ported disk drive in Gbps	12	
6	Total Numbers of Drive Slots	To be provided by vendor	
7	Number of Drive Slots Populated with drives of different type in the Storage System	To be provided by vendor	
8	Total no of drive slot populated with SSD	To be provided by vendor	
9	Total no of drive slot populated with Flash Drive	To be provided by vendor	
10	Total no of drive slot populated with SAS	To be provided by vendor	
11	Total no of drive slot populated with NL-SAS	To be provided by vendor	
12	Drive Type Wise Storage Capacity of System in GB	To be provided by vendor	
13	Automated Storage tiering feature across the populated drives types (in case of multiple drive system)	No	
14	Automated Storage tiering Software License Included	No	
15	Hot Spares	Yes	
16	Number of populated disks per Hot Spare	30	
17	Provision for additional capacity	Yes	

SN	Parameters	Minimum specifications	Complied (Yes/No)
18	Type of Front-end Ports	FC, iSCSI, Ethernet, Fibre Channel over Internet	
19	No. & Speed of front-end Ports in Gbps	8X32GbFC or higher, 8 x 10 GbE or higher	
20	Type of Back-end Ports	SAS	
21	Number of Back-end Ports	4 or higher	
22	Speed of Back-end ports in Gbps	12	
23	Number of Remote Replication Ports (FC/Ethernet)	2	
24	Controllers	To be provided by vendor	
25	Number of Controllers/VSD/ Node available in the storage System on common back plane without using external switch/device OR without common backplane using switches	2	
26	RAID Level Support	5/6 or equivalent	
27	Active-Active Controllers Configured in HA	Yes	
28	Active Stand by Controller Configured in HA	No	
29	Cache Availability Type	Federated	
30	Total Configurable Cache (GB)	768	
31	Wide Stripping or equivalent feature	Yes	
32	No of Snapshot Copies Per Volume	255	
33	License for Snapshot included	Yes	
34	Remote Replication (for all the protocols asked in the RFP i.e., FC, iSCSI, NFS.)	Yes	
35	Remote Replication license included	Yes	
36	Synchronized Replication Support	Yes	

SN	Parameters	Minimum specifications	Complied (Yes/No)
37	Synchronous Replication license included	Yes	
38	Asynchronous Replication Support	Yes	
39	Asynchronous Replication license included	Yes	
40	3-DC Zero Data Loss Support	No	
41	Type of Data Compression NA		
42	Type of Data Deduplication	NA	
43	No Single point of Failure with Non-Disruptive replacement of Hardware	Yes	
44	The Storage provide Non disruptive Firmware /Microcode upgrade	Yes	
45	Firmware upgrade without any controller reboot	No	
46	Encryption Required	Yes	
47	Type of Data at Rest Encryption	HW Controller Based/SED based	
48	Storage management software for configuration and multi-pathing (part of the supply	Yes	
49	Multi-pathing and load balancing and fail over software (part of supply) with license for windows/Linux servers or shall support native multipathing of OS.	Yes	
50	Protocols Supported by the storage system from day one	FC, iSCSI, CIFS, NFS, Fibre Channel over Internet	
51	Operating System Platform and Clustering Supported by the Storage from day one	Windows, Linux	

SN	Parameters	Minimum specifications	Complied (Yes/No)
52	Storage System is compliant with IPv6	Yes	
53	Scope of Supply	It includes installation, commissioning & integration together with all necessary software to make the system fully functional as intended	
54	Comprehensive On Site OEM Supported Warranty	Five(5) Years	

Note: All the above specifications should be read as equivalent or higher.

Annexure D

SN	Parameter	Specification	Complied (Yes/No)
1	Port Count	24 or 48 ports	
2	Speed and Duplex	10/100/1000 Mbps or 2.5/5/10 Gbps	
3	Uplink Ports	SFP (Small Form-factor pluggable) or SFP+ (10 Gigabit Ethernet SFP) for fiber optic connections.	
4	Switching Capacity	Higher switching capacities	
5	VLAN Support	Yes	
6	PoE (Power over Ethernet)	Yes	
7	Management Options	Web-based interfaces, command-line interfaces (CLI), and SNMP (Simple Network Management Protocol)	
8	Redundancy and Resilience	For mission-critical networks, switches may support features like link aggregation (e.g., LACP or EtherChannel)	
9	Comprehensive On Site Warranty	Five(5) Years	
10	Certification:	IPv6 Ready, UL/IEC/EN 60950-1; FCC and RoHS	

Note: All the above specifications should be read as equivalent or higher.

Annexure E

SN	Description	Specification	Complied (Yes/No)
1	Type	Next Generation Enterprise Firewall	
2	Equipment Test Certification	FCC Class A, CE Class A, VCCI Class A, UL and CB Certified.	
3	Fans and Power Supply	The offered firewall must be a single appliance and not a cluster and should be provided with redundant Fans and power supplies	
4	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	
		The proposed firewall must have min 8 physical cores with x86 processor	
		The administrator must be able to view report on the CPU usage for management activities and CPU usage for other activities.	
5	Storage	The NGFW should have 120 GB solid-state drives for System storage.	
6	Interface Requirement	Min 8 x 1 Gig Copper interfaces from day one	
		Minimum 6*1G SFP and Minimum 4x 1/10Gig SFP/SFP+ ports fully populated with SR transceivers from day 1	
		Dedicated 2x HA ports with active	

SN	Description	Specification	Complied (Yes/No)
		optical cable of minimum 5 meter length in addition to requested data ports, OOB, Console Management and USB Port.	
7	Performance Capacity	A Minimum NG Firewall application control throughput – minimum 8 Gbps considering 100% HTTP flows with 64KB transaction size including Application-Identification / AVC/ Application control and Logging enabled. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC Minimum NG Threat prevention throughput by enabling and measured with Application-ID/AVC, User-ID/ Agent-ID, NGIPS, Anti-Virus, Anti-Spyware, Anti Malware, File Blocking, Sandboxing, advanced DNS Security and logging security threat prevention features enabled – minimum 3 Gbps considering 100% HTTP flows with 64KB transaction size . The bidder shall submit the performance test report reference from public documents or from Global Product Engineering	
		IPsec VPN throughput with logging enabled– minimum 4 Gbps with 64KB HTTP	
		New Layer 4 sessions per second – 300,000 or New Layer 7 sessions per second.	
		Concurrent Layer 4 sessions – Min 4 Million or Concurrent Layer 7 sessions – Min.	
8	High Availability	Active/Active and Active/Passive and should support session state synchronisation among firewalls in a	

SN	Description	Specification	Complied (Yes/No)
		high availability cluster.	
9	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	
10	Next Generation Firewall 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 third-party tool or technical support. Also the device should have capability to provide detailed information about dependent applications to securely enable an application .	
		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	

SN	Description	Specification	Complied (Yes/No)
		numbers, User id, Application id and threat protection profile under the same firewall rule or 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 file-transfer capability inside the chat.	
		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	
		The firewall must have the ability to manage firewall policy even if management	
		The firewall must disallow root access to firewall system all users(including super	
		Should support insertion of customer 2 factor authentication into any application before permitting the connection.	
		Solution should be have machine learning capabilities on the dataplane to analyse web page content to determine if it contains malicious JavaScript or is being used for credential phishing. Inline ML should prevent web page threats from infiltrating network by providing real-time analysis capabilities.	
		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	

SN	Description	Specification	Complied (Yes/No)
		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.	
11	Threat Protection	Should have protocol decoder-based analysis which can perform Stateful decode upon the protocol and then intelligently applies signatures to detect network and application.	
		Intrusion prevention signatures should be built based on the vulnerability itself, A single signature should stop multiple exploit attempts on a known system or.	
		Should block known network and application-layer vulnerability exploits.	
		The proposed firewall shall perform content based signature matching beyond the traditional hash base signatures .	
		The proposed firewall shall have on box Anti-Virus/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 Anti-virus 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	

SN	Description	Specification	Complied (Yes/No)
		third party external threat intelligence data bases to block or sinkhole bad IP address, Domain and URLs .	
		Should support inspection of headers with 802.1Q for specific Layer 2 security group tag (SGT) values and drop the packet based on Zone Protection profile .	
		The device should support zero day prevention by submitting the executable files and getting the verdict back in five minutes post detection.	
		The device should have protection for min 20000 IPS signatures excluding custom.	
		Should have. threat prevention capabilities to easily import IPS signatures from the most common definition languages Snort and Suricata.	
		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.	
		The solution must have data loss prevention by defining the categories of sensitive information that is required to filter.	
		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.	
		Vendor should automatically push dynamic block list with latest threat intelligence data base on malicious IPs, URLs and Domains to the firewall policy as an additional.	

SN	Description	Specification	Complied (Yes/No)
		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.	
		Automatically identify and block phishing sites. Prevent users from submitting credentials to phishing sites	
		Prevent the use of stolen credential	
12	Advanced Persistent Threat(APT) Protection	There should be provision to enable the APT solution if required in Future with following features. This should be a both on premise and cloud base unknown malware analysis.	
		Advance unknown malware analysis engine should be capable of machine learning with static analysis and dynamic analysis engine with custom-built virtual.	
		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.	
		The solution must be able to use AV and zero day signatures based on payload and not just by hash values and it should support bare metal analysis if required using.	
		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.	
13	URL Filtering Feature enabled from	NGFW should protect against evasive techniques such as cloaking, fake	

SN	Description	Specification	Complied (Yes/No)
	day 1	CAPTCHAs, and HTML character encoding based attacks	
		NGFW should allow creation of custom categories according to different needs around risk tolerance, compliance, regulation, or acceptable use	
		NGFW should support policy creation around end user attempts to view the cached results of web searches and internet archives from day 1	
		NGFW should have a vast categorisation database where websites are classified based on site content, features, and safety in more than 70 benign and malicious	
14	DNS Security Features from day 1	The Solution should support DNS security in line mode and not proxy mode	
		Solution should support database maintenance containing a list of known botnet command and control (C&C) addresses which should be updated dynamically	
		DNS Security should have predictive analytics to disrupt attacks that use DNS for Data theft and Command and Control	
		DNS security capabilities should block known Bad domains and predict with advanced machine learning technology and should have global threat intelligence of at least 10 million malicious domains if needed for any future consideration	
		It should prevent against new malicious domains and enforce consistent protections for millions of emerging domains.	
		The solution should support integration	

SN	Description	Specification	Complied (Yes/No)
		and correlation to provide effective prevention against New C2 domains, file download source domains, and domains in malicious email links. Integrate.with URL Filtering to continuously crawl newfound or uncategorised sites for threat indicators. Should have OEM human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honeypots	
		Should support simple policy formation for dynamic action to block domain generation algorithms and sinkhole DNS queries.	
		Solution should have prevention against DNS tunnelling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel	
		The solution should be capable to neutralise DNS tunnelling and it should automatically stop with the combination of policy on the next-generation firewall and blocking the parent domain for all customers	
		The solution should have support for dynamic response to find infected machines and respond immediately. There should be provision for administrator to automate the process of sink-holing malicious domains to cut off Command and control	
15	SSL/SSH Decryption	The proposed firewall should have SSL decryption in Hardware and shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward)	
		The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection	

SN	Description	Specification	Complied (Yes/No)
		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 non-personal	
		The device should be capable of SSL automatic exclusions for pinned applications.	
		The firewall supports TLSv1.3 decryption in all modes (SSL Forward Proxy, SSL Inbound Inspection, Broker and SSL Decryption Port Mirroring.	
		SSL decryption must be supported on any port used for SSL i.e. SSL decryption must be supported on non-standard SSL port as well	
16	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	
17	IPv6 Support	L2, L3, Tap and Transparent mode	

SN	Description	Specification	Complied (Yes/No)
		Should support on firewall policy with User and Applications	
		Should support SSL decryption on IPv6	
		Should support SLAAC Stateless Address Auto configuration	
		Should be IPv6 Logo or USGv6 certified	
18	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 VXLAN Tunnel content inspection	
		The firewall must support DDN provides such as DuckDNS, DynDNS, FreeDNS Afraid.org Dynamic API, FreeDNS Afraid.org, and No-IP.	
		The proposed firewall must have support for mobile protocols like GTP, SCTP and support for termination of GRE Tunnels	
		The device should support load balancing of traffic on multiple WAN links based on application, latency, cost and type.	
		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	

SN	Description	Specification	Complied (Yes/No)
		User Group - Services or ports	
		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)	
		PIM-SM, PIM-SSM, IGMP v1, v2, and v3	
		Bidirectional Forwarding Detection (BFD)	
19	Authentication	Solution should support the following authentication protocols:	
		- LDAP	
		- Radius (vendor specific attributes)	
		- Token-based solutions (i.e. secure-ID)	
		- Kerberos	
		The proposed firewall's SSL VPN shall support the following authentication	
		- LDAP	
		- Radius	
		- Token-based solutions (i.e. secure-ID)	
		- Kerberos	
		- SAML	
		- Any combination of the above	
20	Monitoring, Management and Reporting	Should provide on device as well as centralized management and reporting solution with complete feature parity on firewall administration. The Central	

SN	Description	Specification	Complied (Yes/No)
		Management and Reporting Solution should be a dedicated OEM appliance with	
		There should be provision to permanently block the export of private keys for certificates that have been generated or imported to harden the security posture in order to prevents rogue administrators from misusing keys	
		The management solution must support the native capability to optimize the security rulebase and offer steps to create application based rules	
		The proposed solution must allow single policy rule creation for application control, user based control, host profile, threat prevention, Anti-virus, 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	
		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	
		Should support the report generation on a manual or schedule (Daily, Weekly)	
		Should allow the report to be exported into other format such as PDF, HTML, CSV,	
		Should have built in report templates base on Applications, Users, Threats, Traffic	
		Should be able to create report base on	

SN	Description	Specification	Complied (Yes/No)
		SaaS application usage	
		Should be able to create reports base user activity	
		Should be able to create custom report base on custom query base any logging	
		On device management service should be able to provide all the mentioned features in case of central management server failure	
21	Authorization	Original Manufacturer Authorization Certificate to be submitted along with the bid. We reserves the right to reject in case deviation on the basis of technical compliance as submitted in the tender document.	
22	Support & Warranty	OEM should be present in India from at least Five(5) Years and should be proposed with Five(5) Years OEM support. The NGFW should be proposed with Five(5) Years subscription licenses for NGFW, NGIPS, Anti Virus , Anti Spyware, URL Filtering, DNS	
23	Training	In addition to the support, requisite training of firewall configuration, management and monitoring etc. should be provided to the technical team of the Computer Cell of the High Court Of Sikkim	
Note: All the above specifications should be read as equivalent or higher.			