RAILTEL CORPORATION OF INDIA LIMITED

(A Govt. of India Undertaking)

Registered & Corporate Office:

Plate-A, 6th Floor, Office Tower-2,
NBCC Building, East Kidwai Nagar, New Delhi-110023

Selection of Partner For

"Supply of IT Components to RCIL Customer"

EOI No: RCIL/EOI/CO/ITP/2023-24/IT services to RCIL customer/02 dated 26.04.23

EOI NOTICE

RailTel Corporation of India Limited Plate-A, 6th Floor, Office Tower-2,
NBCC Building, East Kidwai Nagar, New Delhi-110023

EOI No: RCIL/EOI/CO/ITP/2023-24/IT services to RCIL customer/02 dated 26.04.23

RailTel Corporation of India Ltd., (here after referred to as RailTel) invites EOIs from RailTel's Empaneled Partners for the selection of suitable agency for "IT Services to RCIL Customer".

The details are as under:

1	Last date for submission of EOIs by bidders	01.05.2023 before15:00Hrs.
2	Opening of bidder EOIs	01.05.2023at 15:30Hrs.
3	Earnest Money Deposit (EMD)	Rs. 2 Lakh
4	Number of copies to be submitted for scope of work	01 in Hard Copy
3	Place of Bid submission	RailTel Corporation of India Limited Plate-A, 6th Floor, Office Tower-2, NBCC Building, East Kidwai Nagar, New Delhi-110023

Prospective bidders are required to direct all communications related to this Invitation for EoI document, through the following Nominated Point of Contact persons:

Contact: Naresh Kumar
Position: DGM/IT
Email: naresh.kumar@railtelindia.com Telephone:
+91124 2714000 Ext 2222

NOTE:

I. **All firms are required to submit hard copy of their EOI submissions, duly signed by Authorized Signatories with Company seal and stamp.**

II. **The EOI response is invited from empanelled partners of RailTel. Only RailTel empanelled partners are eligible for participation in EOI process.**

1. RailTel Corporation of India Limited–Introduction

RailTel Corporation of India Limited (RCIL), an ISO-9001:2000 organization is a Government of India undertaking under the Ministry of Railways. The Corporation was formed in Sept 2000 with the objectives to create nationwide Broadband Telecom and Multimedia Network in all parts of the country, to modernize Train Control Operation and Safety System of Indian Railways and to contribute to realization of goals and objective of national telecom policy 1999. RailTel is a wholly owned subsidiary of Indian Railways.

For ensuring efficient administration across India, country has been divided into four regions namely, Eastern, Northern, Southern & Western each headed by Regional General Managers and Headquartered at Kolkata, New Delhi, Secunderabad & Mumbai respectively. These regions are further divided into territories for efficient working. RailTel has territorial offices at Guwahati, & Bhubaneswar in East, Chandigarh, Jaipur, Lucknow in North, Chennai & Bangalore in South, Bhopal, and Pune & Ahmedabad in West. Various other territorial offices across the country are proposed to be created shortly.

RailTel's business service lines can be categorized into three heads namely B2G/B2B (Business to Government and Business to Business) and B2C (Business to customers):

Licenses & Services

Presently, RailTel holds IP-1, NLD and ISP (Class-A) licenses under which the following services are being offered to various customers:

CARRIER SERVICES

1. National Long Distance: Carriage of Inter & Intra -circle Voice Traffic across India using state of the art NGN based network through its Interconnection with all leading Telecom Operators
2. Lease Line Services: Available for granularities from E1, DS-3, STM-1 & above
3. Dark Fiber/Lambda: Leasing to MSOs/Telco's along secured Right of Way of Railway tracks
4. Co-location Services: Leasing of Space and 1000+ Towers for collocation of MSC/BSC/BTS of Telco's

ENTERPRISE SERVICES

1. Managed Lease Line Services: Available for granularities from E1, DS-3, STM-1 & above
2. MPLS VPN: Layer-2 & Layer-3 VPN available for granularities from 64 Kbps to nx64 Kbps, 2 Mbps& above
3. Dedicated Internet Bandwidth: Experience the "Always ON" internet connectivity at your fingertips in granularities 2mbps to 155mbps

RETAIL SERVICES

RailWire: RailWire is the retail broadband service of RailTel. RailWire is a collaborative public private local entrepreneur (PPLE) model providing broadband services by leveraging the eco system available with different partners like RailTel, Access Network Provider, Aggregation Network Provider (AGNP) and Managed Service Provider (MSP) to offer high speed & cost-effective broadband to end customers. The model uses RailTel's nationwide Core fiber Backbone Network, Access Network available with Local entrepreneurs, FTTH Infrastructure providers etc. and Managed Service Partners/Application Service Providers having IT & management capabilities. The model has been tested for several years now with about 4 lakh+ home broadband users along with 5200+ local access network partners. It is noteworthy that this approach whereby about 54% of the revenue is

ploughed back into the local community not only serves the underserved but also creates livelihoods and jobs in the local communities.

2. Objective of EOI

RCIL is implementing IT-ICT projects like providing Infra & Cloud Services, Application Development, ERP/E-Office Implementation and Consultancy Services for its customers. RailTel is in process of selecting suitable empanelled partner for providing customer specific IT services.

3. Scope of Work

Selected bidder is required to provide "Supply of Hardware, software, and networking equipment and associated services along with 03 year on site comprehensive warranty as per SOR under clause number 8".

4. Language of Proposals

The proposal and all correspondence and documents shall be written in English. The hardcopy version will be considered as the official proposal.

5. Proposal Preparation and Submission

The Applicant/bidder is responsible for all costs incurred in connection with participationin this EOI process, including, but not limited to, cost incurred in conduct of informative and other diligence activities, participation in meetings/ discussions/presentations, preparation of proposal, in providing any additional information required by RCIL to facilitate the evaluation process or all such activities related to the EOI response process. RCIL will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

6. Bidding Document

The bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the bidding documents. Submission of bids, not substantially responsive to the bidding document in every aspect will be at the bidder's risk and may result in rejection of its bid without any further reference to the bidder.

All pages of the documents shall be signed and stamped by the bidder including the closing page in token of his having studied the EOI document and should be submitted along with the bid.

7. Payment terms

Full payment will be made after the installation of server along with required items and subjected to fund availability for that project. Selected bidder shall submit tax invoice.

8. Schedule of Rates (SOR)

S No.	**Item Description**	**Make & Model**	Qty	Unit Price	Total Cost(Excl Tax)	Total Cost(Incl Tax)
1	Application Blade Server with Blade Chassis. Specification of Blade Server and Blade Chassis as per Annexure-1		40 Nos.			
2	SAN Storage with redundant switches. Capacity: 50 TB. Specification as per Annexure-2.		1 Nos.			
3	Professional Services		1 Nos.			
4	Type-1 Layer-3 Switches (Ports- 10 x 100 Gigabit + 04 x 10 Gigabit, 2.08 Tbps throughput with RPS as per Annexure 3		2 Nos.			
5	Type-2 Layer-3 Switches (Ports- 02 x 100 Gigabit + 24 x 10 Gigabit, 880 Gbps throughput with RPS as per Annexure 4		4 Nos.			
6	Type-3 Layer-3 Switches (Ports- 02 x 100 Gigabit + 04 x 40 Gigabit + 12 x 10 Gigabit, 960 Gbps throughput with as per Annexure 5		2 Nos.			
7	Application Delivery Controller (4x10G + 4X 1G Ports, 15 Gbps L-7 throughput) as per Annexure 6		2 Nos.			
8	VPN Device (02x10G + 4X 1G Ports) Specifications as per Annexure 7.		2 Nos.			
9	Structured LAN Cabling (Specifications as per Annexure 8		1 Nos.			

Total Amount (including taxes) in words : _____

9. Evaluation criteria

Evaluation will be done on basis of lowest offer quoted by the bidder under Clause **8 SOR Total.**

10. Bidding Process

The bidder needs to submit the bid in sealed, signed and stamped envelope clearly mentioning of EOI number, EOI name, addressed to the EOI inviting officer as well as Bidding Agency Name and Contact person.

BID should consist the following:

1. Covering Letter
2. Signed and Stamped EOI Document
3. GST and PAN documents
4. EMD or MSE certificate in case of exemption from EMD submission as per latest MSE exemption rules
5. Duly filled SOR
6. Technical compliance of annexure 1 to 8.
7. Any other relevant documents

11. Period of Validity of bids and Bid Currency

Bids shall remain valid for a period of 180 days from the date of issue of Customer PO to RailTel. The prices in the bid document to be expressed in INR only.

12. RCIL's Right to Accept/Reject Bids

RCIL reserves the right to accept or reject any bid and annul the bidding process or even reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or without any obligation to inform the affected bidder or bidders about the grounds for RailTel's action.

13. Security Deposit / Performance Bank Guarantee (PBG)

13.1. Successful bidder has to furnish security deposit in the form of Performance Bank guarantee @ 3 % of issued PO/ LOA value with tax of validity 3 months beyond warranty period completion, the same should be submitted within 30 days of issue of LOA/PO, failing which a penal interest of 15% per annum shall be charged for the delay period i.e. beyond 30 (thirty) days from the date of issue of LOA/PO. This PBG should be from a Scheduled Bank and should cover warranty period plus three months for lodging the claim. The performance Bank Guarantee will be discharged by the Purchaser after completion of the supplier's performance obligations including any warranty obligations under the contract.

13.2. The Performa for PBG is given in Form No. 1. If the delivery period gets extended, the PBG should also be extended appropriately.

13.3. The security deposit/PBG shall be submitted to Corporate Office & will bear no interest.

13.4. A separate advice of the BG will invariably be sent by the BG issuing bank to the RailTel's Bank through SFMS and only after this the BG will become acceptable to RailTel. It is therefore in interest of bidder to obtain RailTel's Bank IFSC code, its branch and address and advise these particulars to the BG Issuing bank and request them to send advice of BG through SFMS to the RailTel's Bank.

13.5. The security deposit/Performance Bank Guarantee shall be released after successful completion of Contract, duly adjusting any dues recoverable from the successful tenderer. Security Deposit in the form of DD/Pay Order should be submitted in the favour of "RailTel Corporation of India Limited" payable at New Delhi Only.

13.6. Any performance security upto a value of Rs. 5 Lakhs is to be submitted through DD/Pay order / online transfer only.

13.7. The claim period of PBG shall be 1 year after date of PBG validity

14. Earnest Money Deposit (EMD)/ Bid Security

14.1. The bidder shall furnish a sum as Earnest Money in the form of online transfer or Demand Draft from any scheduled bank in India in favour of "RailTel Corporation of India Limited" payable at New Delhi.

14.2. The EMD may be forfeited if a bidder withdraws his offer or modifies the terms and conditions of the offer during validity period and in the case of a successful bidder, if the bidder fails to accept the Purchase order and fails to furnish performance bank guarantee (security deposit) in accordance with clause 6.

14.3. Offers not accompanied with Earnest Money shall be summarily rejected.

14.4. Earnest Money of the unsuccessful bidder will be discharged / returned as promptly as possible as but not later than 30 days after the expiry of the period of offer / bid validity prescribed by the Purchaser.

14.5. The successful bidder's EMD will be discharged upon the bidder's acceptance of the purchase order satisfactorily and furnishing the performance bank guarantee in accordance with clause 7.

14.6. Earnest Money will bear no interest.

14.7. **For Micro and Small Enterprises (MSEs)**

14.7.1. The benefit of EMD exemption shall be extended to the registered MSEs as per guidelines issued in the latest notification of Ministry of MSME/ Government of India.

14.7.2. MSEs who are interested in availing themselves of these benefits will enclose with their offer the proof of their being MSE registered with any of the agencies mentioned in the notification of Ministry of MSME.

14.7.3. The MSEs must also indicate the terminal validity date of their registration and shall submit latest Udyam certificate issued by MSME.

14.7.4. Failing 15.7.2 and 15.7.3 above, such offers will not be liable for consideration of benefits detailed in the notification of Government of India.

15. Deadline for Submission of Bids

Bids must be submitted to RCIL at the address specified in the EOI document not later than the specified date and time mentioned. If the specified date of submission of bids being declared a holiday for RCIL, the bids will be received up to the specified time in the next working day.

16. Late Bids

Any bid received by RCIL after the deadline for submission of bids will be rejected and/or returned unopened to the bidder.

17. Modification and/or Withdrawal of Bids

Bids once submitted will treated as final and no modification will be permitted. No correspondence in this regard will be entertained. No bidder shall be allowed to withdraw the bid after the deadline

for submission of bids. In case of the successful bidder, he will not be allowed to withdraw or back out from the bid commitments.

18. Clarification of Bids

To assist in the examination, evaluation and comparison of bids the purchaser may, at its discretion, ask the bidder for clarification. The response should be in writing and no change in the price or substance of the bid shall be sought, offered or permitted.

19. Variation in Contract

+/-25% variation may be operated on SOR during the period of Project Schedule with the approval of competent authority with similar terms and procedure as specified in the agreement.

20. Bidder's Information

Company Name:	
Type of RCIL Business Partner	
Status of Applicant (Partnership, Company etc.)	
Number of Years of Experience	
Number of office locations in India (Provide details)	
Number of office locations globally (Provide details)	
Number of employees in India and global	

CONTACT DETAILS:			
First Name		Last Name	
Designation			
Address for correspondence			
Contact Number (Office Landline)			
Mobile Number			
Official Email ID			
GSTN No			
PAN No			
Bank Account No			
IFSC Code			
Registered Address of Company			

21. Format for statement of Deviation

The following are the particulars of deviations from the requirements of the Instructions to bidders:

SN	CLAUSE	DEVIATION	REMARKS (Including Justification)

Note: In case of no deviation, bidder shall fill up above format with NIL deviation and submit along with Bid document.

22. Period of Association/Validity of Agreement

The initial contract period shall be for the period of 3 years, however the contract period can be terminated earlier or extended further based on customer requirement and as per approval of RailTel competent authority.

23. Delivery Timelines: The selected bidder shall complete the supply and associated work within 3 months from date of issue of purchase order from RailTel. The 3 years warranty period shall start after go live.

24. LD

In case of services and equipment failure, applicable penalty shall be deducted from vendor invoice payment.

25. Other Terms and Condition

1. Bidders are requested to quote their best prices.
2. RCIL will execute the separate agreement with successful bidder before issuance of PO.
3. Unless otherwise specified all prices quoted must remain firm except for statutory variation in taxes and duties during contractual delivery period. Any increase in taxes and duties after expiry of the delivery period will be to vendor account.
4. Offer should preferably be typewritten and any correction or over- writing should be initialed. Rates to be indicated both in words and figures.
5. Sealed offer in envelope super scribing tender enquiry number and due date of opening must be sent by Registered or Speed Post or to be dropped in the Tender Box specified for the purpose. Offers received after specified date and time are liable to be rejected.
6. Offer should be valid for a minimum period of 180 days from the date of issue of Customer PO to RailTel.
7. Printed conditions on the back side of the offers will be ignored.
8. Any increase in taxes and duties after expiry of the delivery period will be to supplier's account. This will be without prejudice to the rights of RCIL for any other action including termination.
9. RCIL shall have the right to terminate the contract by giving 30 days notice without assigning any reasons thereof. However, in the event of any breach of terms of the contract, RCIL will have right to terminate the contract by written notice to the Seller.
10. FORCE MAJEURE: Any delay or failure to perform the contract by either party caused by acts of God or acts of Government or any direction or restriction imposed by Government of India which may affect the contract or the public enemy or contingencies

like strikes, riots etc. shall not be considered as default for the performance of the contract or give rise to any claim for damage. Within 7 days of occurrence and cessation of the event(s), the other party shall be notified. Only those events of force majeure which impedes the execution of the contract at the time of its occurrence shall be taken into cognizance.

11. In case of any dispute or difference arising out of the contract which cannot be resolved mutually between RCIL and vendor, it shall be referred to a Sole Arbitrator to be appointed by the CMD, RCIL.
12. The Arbitration and Conciliation Act, 1996 and rules made there under shall apply to the Arbitration Proceedings.
13. The contract shall be governed by and construed according to the laws in force in India and subject to exclusive jurisdiction of the Courts of Delhi only.
14. Copyrights : The copyrights of content and design of the finally complete project will rest with RCIL's customer.
15. RCIL may place the order in full or partial manner based on customer requirement.

26. Format for COVERING LETTER

COVERING LETTER (To be on company letter head)

EoI Reference No: RCIL/EOI/CO/ITP/2023-24/IT services to RCIL customer/02 dated 26.04.23

Date:

To,

DGM/IT
RailTel Corporation of India Ltd.
Plate-A, 6th Floor, Office Tower-2,
NBCC Building, East Kidwai Nagar,
New Delhi 110023

Dear Sir,

SUB: Participation in the EoI Process

Having examined the Invitation for EoI document bearing the reference number _____ released by your esteemed organization, we, undersigned, hereby acknowledge the receipt of the same and offer to participate in conformity with the said Invitation for EoI document. I/We also agree to keep this offer open for acceptance for a period of 180 days from the date of issue of Customer PO to RailTel and in default thereof,

If our application is accepted, we undertake to abide by all the terms and conditions mentioned in the said Invitation for EoI document.

We hereby declare that all the information and supporting documents furnished as a part of our response to the said Invitation for EoI document, are true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us, our EoI is liable to be rejected.

Authorized Signatory
Name
Designation
Contact Details

27. Proforma for Performance Bank Guarantee Bond

Form No. 1

PROFORMA FOR PERFORMANCE BANK GUARANTEE BOND
(On Stamp Paper of Rs one hundred)

(To be used by approved Scheduled Banks)

1. In consideration of the RailTel Corporation of India Limited, having its registered office at Plate-A, 6th Floor, Office Tower-2, NBCC Building, East Kidwai Nagar, New Delhi-110023 having agreed to exempt ……(Hereinafter called "the said Contractor(s)") from the demand, under the terms and conditions of an Purchase Order No……dated……made between……and…….. for (hereinafter called " the said Agreement") of security deposit for the due fulfillment by the said Contractor (s) of the terms and conditions contained in the said Agreement, on production of a Bank Guarantee for Rs. ……(Rs …….. only). We …… (indicate the name of the Bank) hereinafter referred to as "the Bank") at the request of…….…. Contractor(s) do hereby undertake to pay the RailTel an amount not exceeding Rs……..…. against any loss or damage caused to or suffered or would be caused to or suffered by the RailTel by reason of any breach by the said Contractor(s) of any of the terms or conditions contained in the said Agreement.

2. We, ……. Bank do hereby undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from the RailTel stating that the amount is claimed is due by way of loss or damage caused to or would be caused to or suffered by the RailTel by reason of breach by the said Contractor(s) of any of terms or conditions contained in the said Agreement or by reason of the Contractor(s) failure to perform the said Agreement. Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs . ……

3. We, …….. bank undertake to pay to the RailTel any money so demanded notwithstanding any dispute or disputes raised by the Contractor(s) / Tenderer(s) in any suit or proceedings pending before any court or Tribunal relating thereto our liability under this present being, absolute and unequivocal. The payment so made by us under this Bond shall be a valid discharge of our liability for payment there under and the Contractor(s) / Tenderer(s) shall have no claim against us for making such payment.

4. We, ……. Bank further agree that the Guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Agreement and that it shall continue to be enforceable till all the dues of the RailTel under or by virtue of the said Agreement have been fully paid and its claims satisfied or discharged or till RailTel certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said Contractor(s) and accordingly discharges this Guarantee. Unless a demand or claim under the Guarantee is made on us in writing on or before the …….…… We shall be discharged from all liability under this Guarantee thereafter.

5. We,…… (indicate the name of Bank) further agree with the RailTel that the RailTel shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the Agreement or to extend time of to postpone for any time or from time to time any of the powers exercisable by the RailTel against the said contractor(s) and to forbear or enforce any of the terms and conditions

relating to the said Agreement and we shall not be relieved from our liability by reason of any such variation, or extension to the said Contractor(s) or for any forbearance, act or omission on the part of RailTel or any indulgence by the RailTel to the said Contractor(s) or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have affect of so relieving us.

This Guarantee will not be discharged due to the change in the Constitution of the Bank or the Contractor(s) / Tenderer(s).

(indicate the name of Bank) lastly undertake not to revoke this Guarantee during its currency except with the previous consent of the RailTel in writing.

……the day of 2023

for ……..
(indicate the name of the Bank)

Witness

1. Signature Name

2. Signature Name

Note: Claim Period of BG will be 365 days more than the BG Validity date.

ANNEXURE-I

TECHNICAL SPECIFICATIONS

Blade Chassis Specifications

S No	Item	Specification Description	Compliance (Yes/No)
1	Blade Chassis	Chassis should support minimum 8 number of blade servers(reference Annexure-SR1)	
		Should support redundant interconnect bays to configure	
		Should support built-in/external chassis management software appliance in redundancy with separate management network from production network	
		Should support technology for Auto-Discovery of resources	
		Same enclosure should support x86 based blades.	
		Dual network connectivity for each blade server with redundancy should be provided.	
		It should have occupying 6U-12U rack units.	
		DVD ROM can be internal or external, which can be shared by all the blades allowing remote installation of S/W and OS.	
		Support simultaneous remote access for different servers in the enclosure.	
		Minimum 25% slots for blades should be left empty for future expansion after populating the server.	
2	Interconnects support	Should support housing of Ethernet/FC/FCoE/iSCSI interconnect fabrics offering redundancy as a feature. Should support housing of Ethernet, FC/FCoE, iSCSI, interconnect fabrics, offering Hot Pluggable & Redundancy as a feature. Enclosure Should have No-Single-Point-of-Failure Architecture with adequate numbers of Interconnect Bays	
3	Ethernet/Converged Modules	Chassis should be configured with dual redundant hot Swappable Ethernet modules with minimum of four 10Gbps Uplink ports. The module should offer the capability to slice each 10G port on the server into 4 VNICs/physical functions. However, initially, these ports shall be used to connect 10 Gbps port on the CRIS Core Switch.	
4	Fibre Channel/FCoE Module	Chassis should be configured with dual redundant Hot-Swap 16 GB or higher Fibre Channel Modules and shall have no single point of failure. Each FC/FCoE module should have minimum of 4 x 32Gbps External uplink Ports.	
		Converged modules: In lieu of FC & Ethernet modules if a bidder choose to quote converged module than each module should have 4x10G Ethernet uplinks & 4x 16 Gbps or higher FC uplinks.	
5	Power Supply	The enclosure should be populated fully with power supplies of the highest capacity available with the vendor. Power supplies should be supplied with N+N. as well as N+1 redundancy configuration, where N is greater than 1.	

6	Cooling	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics.	
7	Warranty	Warranty should include 3-Year 24x7 comprehensive onsite OEM warranty with 6 Hours CTR proactive support along with dedicated service delivery team, priority call handling, half yearly review of service delivery, patches & firmware analysis of system and system health check report and implementation.	
8	System Software	Management/controlling software must be from the hardware OEM.	
9	Management capabilities	System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of upgrade of software and patches from a remote client using Media/image/folder; It should have support for multifactor authentication.	
		It should provision for a single console to monitor multiple enclosures; Should support simultaneous remote access for different servers in the enclosure.	
		The server should support monitoring of the server hardware and system configuration. Should be able to perform comprehensive system data collection and enable users to quickly produce detailed inventory reports for managed devices. Software should save the Reports in some format for further analysis.	
		Remote console sharing multiuser simultaneously during pre-OS and OS runtime operation	
		Should provide remote firmware update functionality. Should provide support for graphical remote console	
		System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support	
		Should have dashboard view to provide overall health of the blade chassis	
		The Systems Management software should provide Role-based security	
		The management software should provide proactive notification of actual or impending component failure alerts. Should support automatic event handling that allows notification of failures via e-mail.	
		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	
10	Deployment	Must have the capability of deploying multiple Operating Systems on the servers simultaneously.	
		Must have the capability of capturing and deploying OS images.	
		Must have the capability of configuring the hardware and	

		changing system settings such as RAID level before the deployment of the Operating System. Must also have the capability of capturing the hardware settings and replicating it across servers.	
11	Installation Services	All quoted products should be installed as per the project requirement.	
12	Cables and connectors	All required Cables and connectors are to be provided with full network tagging and cable management. Top of the Rack switches in case the solution does not provide it as built-in features in the chassis.	

Annexure-2: Application Blade Server Specifications

S No.	Item	Description of Server Requirement	Compliance (Yes/No)
1	Processor	Two numbers of latest generation 64 bit Intel Xeon Processor with minimum 8 cores, Base frequency 3.0 GHz or above	
2	Memory	64 GB scalable upto 128 GB using DDR4 memory operating at 2666 MT/s	
3	Memory Protection	Advanced ECC with multi-bit error protection	
4	Hard disk drive with carrier	2 * 600 GB or higher hot plug SSD or higher with Raid 1. Offered Server should support Latest SAS/ SSD and SATA /SSD disks.	
5	Storage Controller	Integrated or Add On PCIe 3.0 SAS Raid Controller with RAID 0, 1 with 1GB of Flash backed write cache onboard.	
6	Ethernet Connectivity	Two number of 10G or higher Ports per Blade server. All Ethernet ports must be auto sensing for 10G operations.	
7	FC Connectivity	Dual Ported 16G or higher FC HBA Ports per Blade server. Provision of full Patch-Cords for all supplied physical ports.	
8	Converge connectivity	If, bidder choose to quote converged in lieu of ethernet and FC connectivity (item 6 and 7) then server should have minimum 2 Nos. of 20G or higher converged Ports per Blade server	
9	Bus Slots	Minimum of 2 Nos of PCIe 3.0 based mezzanine slots supporting Converged / Ethernet/ FC adapters.	
10	Industry Standard Compliance	Microsoft® Logo certifications USB 3.0 Compliant WOL (Wake On LAN) enabled on specific adapters PXE (Preboot Execution Environment) support enabled TPM 2.0 (Trusted Platform Module) Support IEEE (specific IEEE standards depending on Ethernet adapter card(s) installed) SNMP SSL 2.0 DMTF Systems Management Architecture for Server	

		Hardware Command Line Protocol (SMASH CLP) Active Directory v1.0 PCIe 3.0 UEFI (Unified Extensible Firmware Interface)	
11	OS Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES)	
12	Virtualization Support	VmwareVsphere Microsoft Virtualization Red Hat Virtualization	
13	Firmware	Firmware from OEM should support Silicon/ Hardware Root of Trust or any equivalent Root of Trust.	
14	Warranty	Warranty should include 3-Year 24x7 comprehensive onsite OEM warranty with 6 Hours CTR proactive support along with dedicated service delivery team, priority call handling, half yearly review of service delivery, patches &firmware analysis of system and system health check report and implementation.	
15	Power & Cooling Fans	Dual & redundant through chassis/enclosure.	
16	Connectors and Cables	All necessary power cables &connectors, LAN Cable of OEM make only are to be provided.	

Annexure-3: SAN Storage with redundant SAN switches

S. No.	Parameter	Functionality	Compliance (Yes/No)
1	Connecting Ports (SAN)	Should have minimum of 08 nos. of 16 Gbps Fiber-Channel Host ports, across minimum Dual independent Controllers (Active-Active), for an aggregate host bandwidth of minimum 64 Gbps or higher. Provision of full Patch-Cords for all supplied physical ports.	
2	Operating System & Clustering Support	The storage array should support industry-leading Operating System platforms including: Linux, Windows, VMware, Sun Solaris, HP-UX, Sun Solaris and IBM-AIX. Any software licenses required to connect to these OS must be supplied with array. The licenses supplied should be perpetual in nature. Offered Storage must support all above operating systems in Clustering.	
3	Capacity & Scalability	The storage array shall offer 50 TB usable storage (uncompressed)space in raid5/ 6 using SSD Drives of not more than 4 TB. It should be scalable to 150 TB or more of raw capacity of offered drives within the same storage system without adding additional controller and all drives should be hot-	

		pluggable.	
4	RAID Controller/Cache Memory	64 GB or highe Cache should be provide with minimum dual redundant, hot-pluggable Active-Active controller with failover to other in case of anyone controller failure and minimum 72 hour battery backup/ de-stage to disk.	
5	Hot Spare	There should be a provision for minimum of 1 global hot spare disk or as per OEM's best practice	
6	No Single point of Failure	Offered Storage Array shall be configured in a No Single Point of configuration including Array Controller card, Cache memory, FAN, Power supply etc. There should be no single point of failure in the Storage system.	
7	Disk Drive Support	1. Offered Storage Array shall support dual-ported 300 / 600 / 1200 /1800 GB hot-pluggable Enterprise SAS hard drives, Minimum of 1 TB SSD Drives along with nearline SAS 2TB / 4TB / 6TB drives.	
		2. Offered Storage shall support higher capacity SSD drives of more than 6TB.	
8	Raid Support	Offered Storage Subsystem shall support RAID 1 /mirroring, RAID 5/single parity and RAID 6/dual parity.	
9	Data Protection	In case of Power failure, Storage array shall be able to hold data in the cache for at-least 72 hours of time or de-stage to disk drives to avoid any data loss.	
10	Protocols	Offered Storage array shall support all well-known protocols like FC, ISCSI, SMB 3.0, NFS V4 etc.	
11	Storage Connectivity	Redundant Connectivity to the SAN Fabric	
12	Fans & Power Supplies	Dual redundant, hot-swappable.	
13	Maintenance	Offered storage shall have online non-disruptive firmware upgrade for both Controller and disk drives.	
14	Rack Support	Suitable for industry-standard Industry standard/OEM Racks and PDUs.	
15	Form factor	The proposed system must be Blade chassis based or rack mounted	
16	Storage Array Configuration & Management Software	1. Vendor shall provide Storage Array configuration and Management software.	
		2. Software shall be able to manage more than one array of same family.	
		3. Storage shall be provided with Performance Management Software & analysis tools.	
		4. Full licensed software is to be provided. License for the full configured capacity to be provided from day one for PIT/Snapshot, thin provisioning, remote replication, and Management Software. If the storage management require Server/Desktop for management, then the management desktop/server of required configuration along with necessary operating system is to be also provided.	
		5.Must include GUI based Storage Management software	

		to centrally manage disk, storage subsystem, security software, OS based load balancing/ multi-pathing, should support RAID migration, Storage front end port monitoring, Disk Monitoring, LUN management, Dynamic Volume Expansion & Dynamic disk segment sizing.	
17	SAN Switches	The Storage should be supplied with 2 SAN Switches each with 24 Ports each running at 16 Gbps, redundant power supply and 24 x 15M or 24 x 10M Cables. Switches should be supplied with all Licenses for integration of supplied servers and existing Storage and SAN Switches. It should have web-based Management for administration and Configuration.	
18	Warranty	Warranty should include 3-Year 24x7 comprehensive onsite OEM warranty with 6 Hours CTR support and proactive support along with assigned account team, priority call handling, half yearly review of service delivery, patches & firmware analysis of system and system health check report and implementation	

Annexure-3 : Type-1 Layer-3 Switches (Ports- 10 x 100 Gigabit + 04 x 10 Gigabit, 2.08 Tbps throughput with RPS)

S. No.	Item Description	Compliance (Yes/No)
	General Requirements:	
1	The Switch shall be designed for continuous operations. The bidder shall furnish the MTBF (Mean Time Between Failure) predicted and observed values along with calculations by the manufacturer.	
2	In case of full system failure, Switch shall maintain a trace area in the NVRAM / Flash which would be used for analysis / diagnosis of the problem.	
3	Switch shall have built in power-on diagnostics system to detect hardware failures.	
4	Switch shall have suitable Visual Indicators for diagnostics and healthy / unhealthy status of Ports & modules.	
5	Spine switch & all optics shall be from the same OEM of leaf switches.	
	Hardware Capabilities & High Availability Features:	
6	Switch shall have 10 nos. 100G Base-X ports complying to IEEE 802.3ba standard which is able to drive the link up to 100 m at a speed of 100 Gbps on a Multi-Mode Fibre. The hardware of all these ports should be complete in all respect.	
7	Switch shall have 04 nos. 10G Base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 m at a speed of 10 Gbps on a Multi-Mode Fibre. The hardware of all these ports should be complete in all respect.	
8	The switching fabric for all the LAN ports shall be non-blocking and each port shall run at wire speed / line-rate.	
9	Switch shall have 2.08 Tbps forwarding bandwidth at Layer-2/3 switching fabric. The performance of the switch shall not degrade for	

	IPv4 and IPv6 individually as well as for dual stack operations (IPv4 & IPv6).	
10	Switch shall have minimum 1.54 Billion packets (64 Byte packet) per second forwarding rate. The performance of the switch shall not degrade for IPv4 and IPv6 individually as well as for dual stack operations (IPv4 & IPv6).	
11	Switch shall support minimum 100,000 active IPv4 or 50,000 IPv6 routes.	
12	The switch hardware shall be designed to run both IPv4 & IPv6 simultaneously (Dual Stack) from day one.	
13	Switch shall be capable of working with AC Power supply with a Voltage varying from 170 – 240 Volts at 50 +/- 2 Hz.	
14	Switch shall have internal Redundant Power Supply (RPS). The primary as well as redundant power supply shall be hot swappable and no downtime / reboot shall be required for addition / removal of power supply module.	
15	Switch shall have Hot Swappable Fan Tray.	
16	Switch shall support 19" rack mountings.	
	Functional Requirements:	
17	Switch shall have following Layer-2 features:	
	a. IEEE 802.1Q VLAN tagging.	
	b. 802. 1Q VLAN on all ports with support for minimum 3900 VLANs.	
	c. Support for minimum 75,000 MAC addresses	
	d. Self-learning of unicast mac addresses and associated VLANs	
	e. Jumbo frames up to 9000 bytes	
	f. Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.	
	g. Minimum 16 Multi-link Trunks with 4 links per multi-link group.	
	h. "Port Spanning" functionality for measurements using a network analyzer.	
	i. Broadcast, Multicast and Unicast storm control on per port basis to prevent degradation of overall system performance occurred due to faulty end stations.	
18	Switch shall have following Layer-3 features:	
	a. Inter-VLAN IP routing for full layer 3 routing between two or more VLANs.	
	b. IP unicast routing protocols (static, OSPFv3, BGP).	
	c. Virtual Router Redundancy Protocol (VRRP)	
	d. Classless Inter Domain Routing (CIDR)	
	e. Variable Length Subnet Masking (VLSM)	
19	Switch shall have following SDN capabilities:	
	a. Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN (RFC 7348)/Geneve.	
	b. Switch should support VXLAN (RFC7348)/Geneve and EVPN for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data centre	
	c. Switch must support VXLAN/Geneve Switching/Bridging and VXLAN/Geneve Routing without any performance degradation.	
	d. The Switch shall integrate with Fabric controller through OpenFlow/REST APIs/Netconf/Opflex from Day One.	

	e. The Switch should Allow the separation of data (packet forwarding) and control (routing decision) paths, to be controlled by Fabric Controller, utilizing OpenFlow protocol/REST APIs/ Netconf/ XMPP/ BGP/Opflex.	
	f. The switch should support 1k Layer 2 VNIs and 500 layer 3 VNIs.	
20	Switch shall support aggregating multiple interfaces of different switches into a single logical aggregated link in order to implement uplinks with redundancy, higher throughput and to avoid broadcast loops.	
21	Switch shall support NTP (Network Time Protocol) or SNTP (Simple Network Time Protocol) for date & time synchronization from NTP Server. The switch shall also be configured as NTP Server for serving time to clients.	
22	Switch shall support FTP / TFTP.	
23	Switch shall support IGMP Version-1, 2 & 3 as well as IGMP V-1, 2 & 3 snooping.	
	Quality of Service (QoS) Features:	
24	Switch shall support classification and scheduling as per IEEE 802.1P on all ports.	
25	Switch shall support minimum four hardware queues per port.	
26	Switch shall support QoS configuration on per switch port basis.	
27	Switch shall support classification and marking based on IP Type of Service (TOS) and DSCP	
28	Switch shall provide traffic shaping and rate limiting features (for egress traffic) for specified Host, network, Applications using standard TCP/ UDP Ports etc.	
	Security Features:	
29	Switch shall support MAC Address based Filters / Access Control Lists (ACLs) on all switch ports.	
30	Switch shall support Filters / Access Control Lists (ACLs) based on Network Address, Mask, Protocol Type and Socket Type on all switch ports.	
31	Switch shall support Port as well as VLAN based Filters / ACLs.	
32	The Switch shall support authentication, authorization and accounting through RADIUS / TACACS+.	
	Management Features:	
33	Switch shall have a console port with RS-232 Interface or RJ-45 interface for configuration and diagnostic purposes.	
34	Switch shall be SNMP manageable with support for SNMP Version 1, 2 and 3.	
35	Switch shall support all the standard MIBs (MIB-I/II).	
36	Switch shall support TELNET and SSH Version-2 for Command Line Management.	
37	Switch shall support 2 groups of embedded RMON (history, statistics, alarm and events).	
38	Switch shall support System & Event logging functions as well as forwarding of these logs onto a separate Server for log management.	
39	Switch shall support on-line software reconfiguration to implement changes without rebooting. Any changes in the configuration of switches	

	related to Layer-2 & 3 functions, VLAN, STP, Security, QoS shall not require rebooting of the switch.	
40	Switch shall have comprehensive debugging features required for software & hardware fault diagnosis.	
41	Switch shall support multiple privilege levels to provide different levels of access on console port and telnet sessions.	
42	Switch shall support following in the user level of access i.e. the user with minimum privileges:	
	i) Ping	
	ii) Telnet	
	iii) Traceroute	
	iv) Display of pre-configured description / label on each interface.	
	v) Display of Input and Output error statistics on all interfaces.	
	vi) Display of Input and Output data rate statistics on all interfaces.	
	vii) Display of Dynamic ARP table.	
	viii) Display of MAC Address table.	
	ix) Display of Routing Table.	
43	Fabric Controller shall provide management, Logging and Monitoring of all the Spine and Leaf switches.	
44	Fabric Controller must Auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy.	
45	Fabric Controller shall provide dynamic device inventory of the Fabric as well as current network topology of the fabric.	
46	Fabric Controller must run in "N + 1 or N + 2" redundancy to provide availability as well as function during the split brain scenario.	
47	In case of all Fabric Controller fails, the Spine must function with the current configuration without any performance degradation.	
	Regulatory Compliance:	
48	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standard like IS-13252:2010 or better for Safety requirements of Information Technology Equipment.	
49	Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standard like IS 6873 (Part 7): 2012 or better for EMC (Electro Magnetic Compatibility) requirements.	
50	Switch shall be manufactured in accordance with the international quality standards ISO 9001:2008 or latest for which the manufacturer should be duly accredited.	

Annexure-4: Type-2 L-3 Switch (Compute Leaf with 02 x 100 Gig + 24 x 10 Gig LAN ; Forwarding bandwidth 880 Gbps with RPS)

S. No.	Item Description	Compliance (Yes/No)
	General Requirements:	
1	The Switch shall be designed for continuous operations. The bidder shall furnish the MTBF (Mean Time Between Failure) predicted and observed values along with calculations by the manufacturer.	
2	In case of full system failure, Switch shall maintain a trace area in the NVRAM / Flash which would be used for analysis / diagnosis of the	

	problem.	
3	Switch shall have built in power-on diagnostics system to detect hardware failures.	
4	Switch shall have suitable Visual Indicators for diagnostics and healthy / unhealthy status of Ports & modules.	
5	Leaf switch & all optics shall be from the same OEM of spine switches.	
	Hardware Capabilities & High Availability Features:	
6	Switch shall have 02 nos. 100G Base-X ports complying to IEEE 802.3ba standard which is able to drive the link up to 100 m at a speed of 100 Gbps on a Multi-Mode Fibre. The hardware of all these ports should be complete in all respect.	
7	Switch shall have 24 nos. 10G Base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 m at a speed of 10 Gbps on a Multi-Mode Fibre. The hardware of all these ports should be complete in all respect.	
8	The switching fabric for all the LAN ports shall be non-blocking and each port shall run at wire speed / line-rate.	
9	Switch shall have 880 Gbps forwarding bandwidth at Layer-2/3 switching fabric. The performance of the switch shall not degrade for IPv4 and IPv6 individually as well as for dual stack operations (IPv4 & IPv6).	
10	Switch shall have minimum 655 Million packets (64 Byte packet) per second forwarding rate. The performance of the switch shall not degrade for IPv4 and IPv6 individually as well as for dual stack operations (IPv4 & IPv6).	
11	Switch shall support minimum 100,000 active IPv4 or 50,000 IPv6 routes.	
12	The switch hardware shall be designed to run both IPv4 & IPv6 simultaneously (Dual Stack) from day one.	
13	Switch shall be capable of working with AC Power supply with a Voltage varying from 170 – 240 Volts at 50 +/- 2 Hz.	
14	Switch shall have internal Redundant Power Supply (RPS). The primary as well as redundant power supply shall be hot swappable and no downtime / reboot shall be required for addition / removal of power supply module.	
15	Switch shall have Hot Swappable Fan Tray.	
16	Switch shall support 19” rack mountings.	
	Functional Requirements:	
17	Switch shall have following Layer-2 features:	
	a. IEEE 802.1Q VLAN tagging.	
	b. 802. 1Q VLAN on all ports with support for minimum 3900 VLANs.	
	c. Support for minimum 75,000 MAC addresses	
	d. Self learning of unicast mac addresses and associated VLANs	
	e. Jumbo frames up to 9000 bytes	
	f. Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.	
	g. Minimum 16 Multi-link Trunks with 4 links per multi-link group.	
	h. “Port Spanning” functionality for measurements using a network analyzer.	
	i. Broadcast, Multicast and Unicast storm control on per port basis to prevent degradation of overall system performance occurred due to	

	faulty end stations.	
18	Switch shall have following Layer-3 features:	
	a. Inter-VLAN IP routing for full layer 3 routing between two or more VLANs.	
	b. IP unicast routing protocols (static, OSPFv3, BGP).	
	c. Virtual Router Redundancy Protocol (VRRP)	
	d. Classless Inter Domain Routing (CIDR)	
	e. Variable Length Subnet Masking (VLSM)	
19	Switch shall have following SDN capabilities:	
	a. Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN (RFC 7348)/Geneve.	
	b. Switch should support VXLAN (RFC7348)/Geneve and EVPN for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data centre	
	c. Switch must support VXLAN/Geneve Switching/Bridging and VXLAN/Geneve Routing without any performance degradation.	
	d. The Switch shall integrate with Fabric controller through OpenFlow/REST APIs/Netconf/Opflex from Day One.	
	e. The Switch should Allow the separation of data (packet forwarding) and control (routing decision) paths, to be controlled by Fabric Controller, utilizing OpenFlow protocol/REST APIs/ Netconf/ XMPP/ BGP/Opflex.	
	f. The switch should support 1k Layer 2 VNIs and 500 layer 3 VNIs.	
20	Switch shall support aggregating multiple interfaces of different switches into a single logical aggregated link in order to implement uplinks with redundancy, higher throughput and to avoid broadcast loops.	
21	Switch shall support NTP (Network Time Protocol) or SNTP (Simple Network Time Protocol) for date & time synchronization from NTP Server. The switch shall also be configured as NTP Server for serving the time	
22	Switch shall support FTP / TFTP.	
23	Switch shall support IGMP Version-1, 2 & 3 as well as IGMP V-1, 2 & 3 snooping.	
	Quality of Service (QoS) Features:	
24	Switch shall support classification and scheduling as per IEEE 802.1P on all ports.	
25	Switch shall support minimum four hardware queues per port.	
26	Switch shall support QoS configuration on per switch port basis.	
27	Switch shall support classification and marking based on IP Type of Service (TOS) and DSCP	
28	Switch shall provide traffic shaping and rate limiting features (for egress traffic) for specified Host, network, Applications using standard TCP/ UDP Ports etc.	
	Security Features:	
29	Switch shall support MAC Address based Filters / Access Control Lists (ACLs) on all switch ports.	
30	Switch shall support Filters / Access Control Lists (ACLs) based on Network Address, Mask, Protocol Type and Socket Type on all switch ports	

31	Switch shall support Port as well as VLAN based Filters / ACLs.	
32	The Switch shall support authentication, authorization and accounting through RADIUS / TACACS+.	
	Management Features:	
33	Switch shall have a console port with RS-232 Interface or RJ-45 interface for configuration and diagnostic purposes.	
34	Switch shall be SNMP manageable with support for SNMP Version 1, 2 and 3.	
35	Switch shall support all the standard MIBs (MIB-I/II).	
36	Switch shall support TELNET and SSH Version-2 for Command Line Management.	
37	Switch shall support 2 groups of embedded RMON (history, statistics, alarm and events).	
38	Switch shall support System & Event logging functions as well as forwarding of these logs onto a separate Server for log management.	
39	Switch shall support on-line software reconfiguration to implement changes without rebooting. Any changes in the configuration of switches related to Layer-2 & 3 functions, VLAN, STP, Security, QoS shall not require rebooting of the switch.	
40	Switch shall have comprehensive debugging features required for software & hardware fault diagnosis.	
41	Switch shall support multiple privilege levels to provide different levels of access on console port and telnet sessions.	
42	Switch shall support following in the user level of access i.e. the user with minimum privileges:	
	i) Ping	
	ii) Telnet	
	iii) Traceroute	
	iv) Display of pre-configured description / label on each interface.	
	v) Display of Input and Output error statistics on all interfaces.	
	vi) Display of Input and Output data rate statistics on all interfaces.	
	vii) Display of Dynamic ARP table.	
	viii) Display of MAC Address table.	
	ix) Display of Routing Table.	
43	Fabric Controller shall provide management, Logging and Monitoring of all the Spine and Leaf switches.	
44	Fabric Controller must Auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy.	
45	Fabric Controller shall provide dynamic device inventory of the Fabric as well as current network topology of the fabric.	
46	Fabric Controller must run in "N + 1 or N + 2" redundancy to provide availability as well as function during the split brain scenario.	
47	In case of all Fabric Controller fails, the leaf must function with the current configuration without any performance degradation.	
	Regulatory Compliance:	
48	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standard like IS-13252:2010 or better for Safety requirements of Information Technology Equipment.	
49	Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standard like IS	

	6873 (Part 7): 2012 or better for EMC (Electro Magnetic Compatibility) requirements.	
50	Switch shall be manufactured in accordance with the international quality standards ISO 9001:2008 or latest for which the manufacturer should be duly accredited.	

Annexure-5: Type-3 L-3 Switch (Border Leaf with 02 x 100 Gig + 04 x 40 Gig + 12 x 10 Gig LAN ; Forwarding bandwidth 960 Gbps with RPS)

S. No.	Item Description	Compliance (Yes/No)
	General Requirements:	
1	The Switch shall be designed for continuous operations. The bidder shall furnish the MTBF (Mean Time Between Failure) predicted and observed values along with calculations by the manufacturer.	
2	In case of full system failure, Switch shall maintain a trace area in the NVRAM / Flash which would be used for analysis / diagnosis of the problem.	
3	Switch shall have built in power-on diagnostics system to detect hardware failures.	
4	Switch shall have suitable Visual Indicators for diagnostics and healthy / unhealthy status of Ports & modules.	
5	Leaf switch & all optics shall be from the same OEM of spine switches.	
	Hardware Capabilities & High Availability Features:	
6	Switch shall have 02 nos. 100G Base-X ports complying to IEEE 802.3ba standard which is able to drive the link up to 100 m at a speed of 100 Gbps on a Multi-Mode Fibre. The hardware of all these ports should be complete in all respect.	
7	Switch shall have 04 nos. 40G Base-X ports complying to IEEE 802.3ba standard which is able to drive the link up to 100 m at a speed of 40 Gbps on a Multi-Mode Fibre. The hardware of all these ports should be complete in all respect.	
8	Switch shall have 12 nos. 10G Base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 m at a speed of 10 Gbps on a Multi-Mode Fibre. The hardware of all these ports should be complete in all respect.	
9	The switching fabric for all the LAN ports shall be non-blocking and each port shall run at wire speed / line-rate.	
10	Switch shall have 960 Gbps forwarding bandwidth at Layer-2/3 switching fabric. The performance of the switch shall not degrade for IPv4 and IPv6 individually as well as for dual stack operations (IPv4 & IPv6).	
11	Switch shall have minimum 710 Million packets (64 Byte packet) per second forwarding rate. The performance of the switch shall not degrade for IPv4 and IPv6 individually as well as for dual stack operations (IPv4 & IPv6).	
12	Switch shall support minimum 100,000 active IPv4 or 50,000 IPv6	

	routes.	
13	The switch hardware shall be designed to run both IPv4 & IPv6 simultaneously (Dual Stack) from day one.	
14	Switch shall be capable of working with AC Power supply with a Voltage varying from 170 – 240 Volts at 50 +/- 2 Hz.	
15	Switch shall have internal Redundant Power Supply (RPS). The primary as well as redundant power supply shall be hot swappable and no downtime / reboot shall be required for addition / removal of power supply module.	
16	Switch shall have Hot Swappable Fan Tray.	
17	Switch shall support 19" rack mountings.	
	Functional Requirements:	
18	Switch shall have following Layer-2 features:	
	a. IEEE 802.1Q VLAN tagging.	
	b. 802. 1Q VLAN on all ports with support for minimum 3900 VLANs.	
	c. Support for minimum 75,000 MAC addresses	
	d. Self learning of unicast mac addresses and associated VLANs	
	e. Jumbo frames up to 9000 bytes	
	f. Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.	
	g. Minimum 16 Multi-link Trunks with 4 links per multi-link group.	
	h. "Port Spanning" functionality for measurements using a network analyzer.	
	i. Broadcast, Multicast and Unicast storm control on per port basis to prevent degradation of overall system performance occurred due to faulty end stations.	
19	Switch shall have following Layer-3 features:	
	a. Inter-VLAN IP routing for full layer 3 routing between two or more VLANs.	
	b. IP unicast routing protocols (static, OSPFv3, BGP).	
	c. Virtual Router Redundancy Protocol (VRRP)	
	d. Classless Inter Domain Routing (CIDR)	
	e. Variable Length Subnet Masking (VLSM)	
20	Switch shall have following SDN capabilities:	
	a. Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN (RFC 7348)/Geneve.	
	b. Switch should support VXLAN (RFC7348)/Geneve and EVPN for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data centre	
	c. Switch must support VXLAN/Geneve Switching/Bridging and VXLAN/Geneve Routing without any performance degradation.	
	d. The Switch shall integrate with Fabric controller through OpenFlow/REST APIs/Netconf/Opflex from Day One.	
	e. The Switch should Allow the separation of data (packet forwarding) and control (routing decision) paths, to be controlled by Fabric Controller, utilizing OpenFlow protocol/REST APIs/ Netconf/ XMPP/ BGP/Opflex.	
	f. The switch should support 1k Layer 2 VNIs and 500 layer 3 VNIs.	
	Switch shall have following SDN capabilities:	
21	Switch shall support aggregating multiple interfaces of different switches into a single logical aggregated link in order to implement	

	uplinks with redundancy, higher throughput and to avoid broadcast loops.	
22	Switch shall support NTP (Network Time Protocol) or SNTP (Simple Network Time Protocol) for date & time synchronization from NTP Server. The switch shall also be configured as NTP Server for serving the time	
23	Switch shall support FTP / TFTP.	
24	Switch shall support IGMP Version-1, 2 & 3 as well as IGMP V-1, 2 & 3 snooping.	
	Quality of Service (QoS) Features:	
25	Switch shall support classification and scheduling as per IEEE 802.1P on all ports.	
26	Switch shall support minimum four hardware queues per port.	
27	Switch shall support QoS configuration on per switch port basis.	
28	Switch shall support classification and marking based on IP Type of Service (TOS) and DSCP	
29	Switch shall provide traffic shaping and rate limiting features (for egress traffic) for specified Host, network, Applications using standard TCP/ UDP Ports etc.	
	Security Features:	
30	Switch shall support MAC Address based Filters / Access Control Lists (ACLs) on all switch ports.	
31	Switch shall support Filters / Access Control Lists (ACLs) based on Network Address, Mask, Protocol Type and Socket Type on all switch ports	
32	Switch shall support Port as well as VLAN based Filters / ACLs.	
33	The Switch shall support authentication, authorization and accounting through RADIUS / TACACS+.	
	Management Features:	
34	Switch shall have a console port with RS-232 Interface or RJ-45 interface for configuration and diagnostic purposes.	
35	Switch shall be SNMP manageable with support for SNMP Version 1, 2 and 3.	
36	Switch shall support all the standard MIBs (MIB-I/II).	
37	Switch shall support TELNET and SSH Version-2 for Command Line Management.	
38	Switch shall support 2 groups of embedded RMON (history, statistics, alarm and events).	
39	Switch shall support System & Event logging functions as well as forwarding of these logs onto a separate Server for log management.	
40	Switch shall support on-line software reconfiguration to implement changes without rebooting. Any changes in the configuration of switches related to Layer-2 & 3 functions, VLAN, STP, Security, QoS shall not require rebooting of the switch.	
41	Switch shall have comprehensive debugging features required for software & hardware fault diagnosis.	
42	Switch shall support multiple privilege levels to provide different levels of access on console port and telnet sessions.	
43	Switch shall support following in the user level of access i.e. the user	

	with minimum privileges:	
	i) Ping	
	ii) Telnet	
	iii) Traceroute	
	iv) Display of pre-configured description / label on each interface.	
	v) Display of Input and Output error statistics on all interfaces.	
	vi) Display of Input and Output data rate statistics on all interfaces.	
	vii) Display of Dynamic ARP table.	
	viii) Display of MAC Address table.	
	ix) Display of Routing Table.	
44	Fabric Controller shall provide management, Logging and Monitoring of all the Spine and Leaf switches.	
45	Fabric Controller must Auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy.	
46	Fabric Controller shall provide dynamic device inventory of the Fabric as well as current network topology of the fabric.	
47	Fabric Controller must run in "N + 1 or N + 2" redundancy to provide availability as well as function during the split brain scenario.	
48	In case of all Fabric Controller fails, the leaf must function with the current configuration without any performance degradation.	
	Regulatory Compliance	
49	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standard like IS-13252:2010 or better for Safety requirements of Information Technology Equipment.	
50	Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standard like IS 6873 (Part 7): 2012 or better for EMC (Electro Magnetic Compatibility) requirements.	
51	Switch shall be manufactured in accordance with the international quality standards ISO 9001:2008 or latest for which the manufacturer should be duly accredited.	

Annexure-6: Application Delivery Controller (04 x 10 G LAN ports, 15 Gbps L-7 Throughput)

S. No.	Item Description	**Compliance (Yes/No)**
	Hardware Details:	
1	The Application Delivery Controller shall be purpose built dedicated stand-alone appliance.	
2	The Application Delivery Controller shall have at least 04 nos. 10G base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 Meter at speed of 10 Gbps on Multi Mode fiber.	
3	The Application Delivery Controller shall have a 100/1000 Base Tx Port for out of bound management.	
4	The Application Delivery Controller shall have a console port based on RS-232 / RJ-45 for configuration and diagnostic purposes.	
5	The number of ports specified vide item no. 2, 3 & 4 are excluding the	

	physical ports required for High Availability Cluster.	
6	The Application Delivery Controller shall have enough CPU capacity and Memory so as to efficiently meet all the capability parameters as well as functionalities laid down in the specifications.	
7	The Application Delivery Controller hardware shall be designed to run both IPv4 & IPv6 simultaneously (Dual Stack) from day one.	
8	The Application Delivery Controller shall be capable of working with AC Power supply with a Voltage varying from 170 –240 Volts at 50 +/- 2 Hz.	
9	The Application Delivery Controller shall have internal Redundant Power Supply (RPS). The primary as well as redundant power supply shall be hot swappable and no downtime / reboot shall be required for addition / removal of power supply module.	
10	The Application Delivery Controller shall support 19" Rack mounting.	
	Solution Capabilities:	
11	The Application Delivery Controller shall have minimum 10 Million concurrent TCP connections.	
12	The Application Delivery Controller shall have minimum 15 Gbps Layer-7 throughput.	
13	The Application Delivery Controller shall have minimum 01 Lakh L4 TCP connections / second.	
14	The Application Delivery Controller shall have minimum 01 Lakh HTTP Request / second.	
15	Application Delivery Controller Solution shall support minimum 30000 (RSA 2K public key) and 20000 (ECDSA P-256 key) SSL transactions per second. SLL TPS rating specify the number of new SSL connections (Key exchanges) per second without session key reuse. In this case, 30000 new users (through RSA 2K public key) and 20000 (Through ECDSA P-256 key) per second should be able to connect through SSL.	
16	The Application Delivery Controller shall support minimum 10 Gbps SSL throughput.	
17	The Application Delivery Controller shall support minimum 7 Gbps server side http compression.	
18	The Application Delivery Controller shall support IPv4 to IPv6 address translation and vice-versa.	
19	The Application Delivery Controller shall have virtualization feature with minimum 05 virtual instances (vADCs) and proposed solution shall have capability to dedicate hardware resources including CPU, memory, network, and acceleration resources to each virtual Application Delivery Controller (vADC). Each vADC instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management.	
20	The Application Delivery Controller shall be configured in High Availability Mode and in case of failure of one of the equipment; the other equipment shall serve all the requests without any disruption or degradation in overall performance as defined vide item 11 to 19 above. In addition to this, the offered HA setup shall support all functional requirements specified vide item no. 21 to 46 below.	
	Application Delivery Functional Requirements:	
21	The Application Delivery Controller shall support TCP and UDP	

	applications.	
22	Application Delivery Controller Solution shall support HTTP1.0, HTTP1.1 & HTTP/2 protocols.	
23	Application Delivery Controller Solution shall support TLSv1.0, TLSv1.1, TLSv1.2 & TLSv1.3 protocols.	
24	The Application Delivery Controller shall perform 'TCP Multiplexing' i.e. it shall initiate fewer connections to Servers in order to serve relatively large no. of connections from clients.	
25	The Application Delivery Controller shall perform 'TCP Optimization' as well as 'TCP Buffering' functions for overall improvement of response.	
26	The Application Delivery Controller shall support different TCP keep alive policy for Client connections and server connection.	
27	The solution shall support following Load Balancing Features	
	(i) Support for 1000 servers	
	(ii) Should support load balancing algorithms	
	a) Least amount of Bytes	
	b) Least number of users/session.	
	c) Cyclic.	
	d) Weighted Cyclic	
	e) SNMP Parameters; like Server CPU utilization, memory utilization and combination of both.	
	f) Fastest Response from the Servers	
	(iii) In case of Server failure traffic should be diverted to another Server automatically	
	(iv) Should support following content based Load balancing features	
	a) URL, cookie etc.	
	b) HTTP header as well as payload.	
	c) Type of Internet Browser used by the client	
	d) Source IP Address	
	e) TCP port number	
	(v) Should support TCP optimization and TCP Multiplexing	
	(vi) Should support HTTP 1.1 & HTTP/2 protocol based dynamic caching	
28	The Application Delivery Controller shall be able to support different cookie persistence methods such as passive, insert, rewrite, hashing.	
29	The Application Delivery Controller shall be able to support persistence based on any variables in the packet header and payload.	
30	The Application Delivery Controller shall be able to support limitation of users sessions (cookies) per application/vserver. Through this feature, ADC shall insure that new user (beyond the configured threshold limit) get blocked, So as to insure availability of resources on WEB / APP servers already logged in users to complete their transactions.	
31	The Application Delivery Controller shall b able to support following caching and compression features:	
	a) URI based caching & compression	
	b) Size base caching & compression	
	c) Content type based caching & compression	
32	The Application Delivery Controller shall be able to read into the FULL payload (data) of the packet to make traffic management decision (pool	

	selection, redirect, forward, reject, drop, log etc).	
33	The Application Delivery Controller shall support adding custom HTTP header in request and response.	
34	The Application Delivery Controller shall support Proxy SSL for non-terminated SSL sessions.	
35	The Application Delivery Controller shall to support scripting language for events based rules creation to make traffic management decision using scripting language.	
36	Application Delivery Controller Solution shall be able to transform HTTP1.0 to HTTP1.1 & HTTP1.1 to HTTP/2 for server connection consolidation.	
37	The Application Delivery Controller shall be able to detect the health status of Servers	
	a. Health check of the Servers using ICMP and SNMP.	
	b. Health check for each Server & Application	
	c. Health check on protocols like HTTP, HTTPS, SMTP, POP etc	
	d. Check the health of Server, Application & contents as well	
	e. Check the health of Server on the basis CPU & Memory utilization.	
38	The Application Delivery Controller shall have options to stop forwarding of requests to specified Server/s for planned shutdown of the Server/s.	
39	The Application Delivery Controller shall support Virtual Router Redundancy Protocol (VRRP) or equivalent.	
40	The Application Delivery Controller shall support SNTP / NTP for date & time synchronization from NTP server	
41	The Application Delivery Controller shall perform caching of the Static Data and serve this data to clients without generating a request to Servers.	
42	The Application Delivery Controller shall compress the HTTP, SHTML, DHTML, JHTML, PHTML, XML, JavaScript, J2EE, JSP, SOAP Application 'Outbound' traffic using industry standard GZIP & Deflate algorithm (as per RFC 1951 and 1952).	
43	The Application Delivery Controller shall perform SSL offloading wherein the equipment will engage in the SSL handshake and cipher negotiation and free the server of SSL processing.	
44	The Application Delivery Controller shall perform HTTPS client authentication during SSL Handshake and shall forward the information of client's SSL certificate like subject, serial number, validity, issuer etc. in custom HTTP headers to web servers. In absence of client certificate, Application Delivery Controller shall be capable to perform following actions:	
	a. Respond with customised HTML page with customised HTTP status code.	
	b. Redirect such requests to another URL.	
	c. Drop such requests.	
45	The Application Delivery Controller shall have feature for obtaining certificate revocation status for HTTPS client authentication.	
46	The Application delivery Controller shall have feature of rewrite (delete or modify http headers for specific URL/URI) client's requests before forwarding to web servers.	

47	The Application delivery Controller shall have feature to perform following actions based on the requested URL/URI, Request Method & HTTP headers without forwarding requests to web servers:	
	a. Respond with customised HTML page with customised HTTP status code.	
	b. Redirect such requests to another URL.	
	c. Drop such requests.	
48	Application Delivery Controller Solution shall support below rules/policies based on following:	
	a. Source IP address & destination IP address and subnet Port	
	b. Service Port/Protocol	
	c. Domain Name	
	d. IP Geolocation	
	e. IP Reputation	
	f. Customized URL Categorization	
	g. Policy-based block & bypass actions	
49	The Web Application Delivery Controller shall have static routing capabilities for IPv4 & IPv6.	
	Management & Reporting:	
50	The Application Delivery Controller shall support Syslog, SNMP (v2 &v3), MIB-II.	
51	The Application Delivery Controller shall be manageable (both GUI and CLI) using telnet , SSH, Web based management (HTTPS) etc.	
52	The Bidder shall provide Central Management & Reporting Solution and offered Application Delivery Controller Solution shall also be manageable through offered Management & Reporting Solution. In case management & reporting solution is virtual appliance, bidder shall provide requisite server Hardware & Operating System as per the recommendations duly vetted by the OEM of the Application Delivery Controller.	
53	The Management server / ADC shall also be able to provide 'At-a-glance-Dashboard' to provide overall status health (CPU, Memory etc), network traffic , concurrent sessions , connections /sec, Top attacks etc.	
54	The Application Delivery Controller shall have feature to provide role based user's access for management.	
55	The Application Delivery Controller shall support authentication & authorization through Radius / TACACS+.	
56	The Application Delivery Controller shall support upload /download of device configuration through secure communication with Management Server.	
57	The Application Delivery Controller shall be able to take manual or scheduled backup of configuration.	
58	The management server must support the archiving & backup of events and it shall be able to export logs/events using NFS/SMB/SCP/sFTP.	
59	Application Delivery Controller Solution shall support integration with SIEM. The Application Delivery Controller shall be able to send logs to SIEM Servers.	
60	The Application Delivery Controller shall generate alarms w.r.t. health status of Server/s.	
61	Central Management & Reporting Solution shall provide comprehensive	

	reports (both Realtime as well as Historical for at least 03 months) that can be customized as per requirement. Following are few examples of the reports:	
	a. Client-side concurrent TCP connections per virtual server/application/URL.	
	b. Client-side new TCP connections per second per virtual server/application/URL.	
	c. Server-side concurrent TCP connections per server.	
	d. Server-side new TCP connections per second per server.	
	e. Total Input as well as Output "Bytes per second" OR "Bits per second" per vserver/application/URL in order to have the usage of Internet Bandwidth.	
	f. Total Input as well as Output "Bytes per second" OR "Bits per second" between the equipment and a particular Server.	
	g. Compression Statistics & comparison between data size before and after compression per vserver/application/URL.	
	h. Caching statistics.	
	i. SSL client handshake per second vserver/application/URL.	
	j. Server Uptime and downtime reports.	
	k. CPU and Memory utilization of the equipment.	
	l. Audit and access reports	
62	The Historical Reports shall be provided for multiple timeframe i.e. hourly, daily, weekly, monthly and customized period.	
63	The communication between ADC and Management Server shall be authenticated and encrypted with one or more of standard authentication and encryption mechanisms like SSH, MD5, SHA, DES, 3DES &IPSec.	
64	The authentication between management server & ADC shall be based on username, password & restricted to specific IP address.	
65	The ADC shall provide access control mechanisms based on IP address, ports, users.	
	Regulatory Compliance:	
66	The Application Delivery Controller shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standard like IS-13252:2010 or better for Safety requirements of Information Technology Equipment.	
67	The Application Delivery Controller shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standard like IS 6873 (Part 7): 2012 or better for EMC (Electro Magnetic Compatibility) requirements.	
	Product / OEM Evaluation Criteria:	
69	The Application Delivery Controller / Application Delivery Controller's Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions or under Indian Common Criteria Certification Scheme (IC3S) by STQC, DEIT, Govt. of India.	

Annexure-8: Technical Specification of Cabling Component

S. No.	Item Description	Compliance (Yes/No)
1	Multimode 10G Fiber optic patch cords -2cores (3 Mtrs, 15 Mtrs,25 Mtrs, 60 Mtrs)	
a	Meet all TIA/EIA-568-C.3 Standard	
b	constructed from high performance OM4 50/125 μm multimode cable	
c	Low Smoke Zero Halogens (LSZH) Cable	
d	100 % factory tested for insertion loss	
e	Insertion loss data recorded for every Multi Mode patch cord	
f	LC Duplex Patch Cords to include LC Duplex Clips to maintain polarity incase of LC -LC patch cords	
g	Meet UL1666 (OFNR) or (IEC 60332-3C) flame ratings for standard compliant safety	
h	RoHS Compliance	
2	Fiber Adapter Panel:-	
a	Standards FOCIS-3 TIA/EIA-568-C.3 complied	
b	Adapters can be used with multi-mode connectors and patch cords	
c	Zirconsia ceramic split sleeves	
d	Protective cap to fully surrounds split sleeves opening Zirconia ceramic split sleeves	
e	Integrated retention clip to create a snug fit to reduce rattles	
f	including adapter	
g	RoHS Compliance	
3	Optic Fiber Distribution Unit Or Enclosure:-	
a	Slides out Drawer for easy front access	
b	1U Fiber Connect Panel with 24 Port	
c	19” rack mountable	
d	Include fiber optic cable routing accessory kit	
e	Unused slots should be covered with blank adapter plates	
f	Removable rear tray cover for easy access to splices and cable storage	
g	Side and rear cable entry	
h	RoHS Compliance	
	Item Description(UTP)	
4	Category-6 UTP Cable :-	
a	Meet all TIA/EIA-568-C.2-1 Cat 6 or ISO/IEC 11801 Class E Standards	
b	Low Smoke zero Halogens (LSZH) Cable	
c	Component compliance for Category-6	
d	(24 AWG or better) Solid Bare Copper	
e	RoHS Compliance	
f	UL LISTED or STQC-ERTL or ETL	
5	Category-6 Wall UTP I/O :-	
a	Meet all TIA/EIA-568-C.2-1 Cat 6 standards	
b	Capable of re-termination	

c	Minimum 6 colors	
d	Component compliance for Category-6	
e	Single Cat 6 Wall Mounting Outlet	
f	RoHS Compliance	
g	UL LISTED or STQC-ERTL or ETL	
6	Category-6 Patch Cord (1m, 2m, 3m) :-	
a	Meet all TIA/EIA-568-C.2-1 Cat 6 standards	
b	Factory Crimped	
c	24 AWG or better Copper Conductors	
d	Tangle free plug design	
e	Minimum 5 colors	
f	Component complaint for Category-6.	
g	RoHS Compliance	
h	UL LISTED or STQC-ERTL or ETL	
7	Modular Patch Panel:-	
a	Modular design (unloaded)	
b	Fit in standard 19" rack occupying 1U space	
c	Accept 24 individual colored I/O Jacks	
d	Lables with lable-holders	
e	RoHS Compliance	
8	Cable Manager :-	
a	Single -sided Plastic horizontal cable manager with Duct fingers and covers (1U)	
b	RoHS Compliance	

Note:-

1. Penta-Scan Test shall be done for UTP Cables.
2. Optical loss test set (OLTS) with an optical time domain reflectometer (OTDR) shall be done for Optical fiber cable.
3. Testing shall be performed on each cabling link (connector to connector) and the test report shall be documented.
4. Installation shall be rectified / fine-tuned till results of all the parameters are within acceptable limit as per relevant standards.

Annexure-7: Technical Specifications for VPN Solution

S. No.	Item Description	Compliance (Yes/No)
	Hardware Details:	
1	The VPN device shall be purpose built dedicated standalone appliance/chassis.	

2	The VPN device shall have 02 Nos. 10G Base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 meters at a speed of 10 Gbps on a Multi-Mode Fibre. The hardware of all these ports should be complete in all respect.	
3	The VPN device shall have 04 nos. 1000Base-T ports complying to IEEE 802.3ab standard, full duplex mode and auto-negotiation on each port to optimize bandwidth. The hardware of all these ports should be complete in all respect.	
4	The VPN device shall have dedicated / separate physical ports (other than ports required vide item no 2 & 3 above) for HA (High Availability) connectivity .	
5	The VPN device shall have a separate 100/1000 Base Tx Port and a console port based on RS-232 / RJ-45 dedicated for management purposes like configuration, diagnostics etc.	
6	The VPN solution hardware shall be designed to run both IPV4 & IPV6 simultaneously (Dual Stack) from day one.	
7	The VPN solution shall work with AC Power supply with a Voltage varying from 170 – 240 Volts at 50 +/- 2 Hz.	
8	The VPN device shall have internal Redundant Power Supply (RPS). The primary as well as redundant power supply shall be hot swappable and no downtime & reboot shall be required for addition / removal of power supply module.	
9	The VPN device shall have redundant FANS to eliminate single point of failure.	
10	The VPN device shall support standard 19" rack mounting.	
	Device Capabilities:	
11	The VPN device shall have minimum of 10 Gbps VPN throughput in real world.	
12	The VPN device shall be able to handle minimum 10000 concurrent client-server IPSec VPN user sessions.	
13	The VPN device shall be able to handle minimum 2000 concurrent site to site (peers) IPSec VPN tunnels.	
14	The VPN device shall be able to handle minimum 2000 concurrent client-server SSL/TLS VPN user sessions.	
15	The VPN device shall have the capacity to run all the parameters simultaneously which are mentioned vide items 11 to 14 without any degradation in performance of the Device.	
16	The CPU & Memory utilization of the VPN device shall not exceed 70% while providing minimum performance parameters specified at item no. 11 to 14 above.	
17	The VPN solution shall provide all necessary features for IPv4, IPv6 and dual stack (IPv4 & IPv6) operations from day one. The performance of the Device shall not degrade for IPv4 and IPv6 individually as well as for dual stack operations (IPv4 & IPv6).	
18	The VPN device shall be configured in 1:1 High Availability (HA) mode with following features:	
	a. Stateful failover of all existing sessions.	
	b. Active/Passive fail over design.	
	c. In case of failure of one of the VPN device, the other VPN device shall serve all the requests without any disruption or degradation in	

	overall performance as defined vide item 11 to 14 above.	
19	The VPN device shall be able to operate in standard Layer 3 mode of configuration with Interface IP addresses.	
20	The VPN device shall support VLAN tagging (IEEE 802.1q) supporting up to minimum 1000 VLANs.	
	Functional Requirements:	
21	The VPN device shall support following minimum set of TCP/IP Protocols/Applications	
	a. Internet protocol Version-4	
	b. Internet protocol Version-6	
	c. Dual stack IPv4 & IPv6	
	d. Transmission Control Protocol	
	e. User Datagram Protocol	
	f. SNTP / NTP	
	g. Internet Control Management Protocol Version-4	
	h. Internet Control Management Protocol Version-6	
	i. Address Resolution Protocol	
	j. Domain Name System	
	k. Simple Network Management Protocol	
	l. Hypertext Transfer Protocol	
	m. File Transfer Protocol	
	n. Trivial File Transfer Protocol	
	o. Telnet	
	p. NetBIOS over IP (Microsoft Networking)	
	q. Point-to-Point Tunneling Protocol	
	r. SQL *Net (Oracle client /server Protocol)	
	s. Remote Procedure Call Services	
	t. Network File System	
	u. AAA Server Groups / Secure Shell	
	v. H.323 and SIP based Multimedia Application	
	w. SMTP & POP3 for Mail Servers	
	x. Lotus Notes	
	y. Internet Message Access Protocol	
	z. Server Message Block	
22	The VPN device shall provide static as well as dynamic policy-based Network Address Translation (NAT) and Port Address Translation (PAT) functionality.	
23	The number of VPN policies / rule set configurable on VPN device shall be more than 10000. The VPN device shall perform packet filtering based on following parameters:	
	a. Source Address	
	b. Destination Address	
	c. Protocol Type	
	d. Port number	
	g. Custom Defined	
24	The VPN device shall support packet filtering based on schedule (one time / recurring).	
25	The VPN device shall support scheduled VPN profiles based on time and date basis.	

26	The VPN device shall have capability to connect client (IPSec& SSL Client) on recent versions of Mac, Linux, Windows and Mobile OS (Android 4.4 Kitkat or above).	
27	The VPN device shall support authentication for VPN users through following:	
	a. PKI Certificate Authority & Certificate Revocation List	
	b. Two Factor Authentication	
	c. Native local user database	
	d. Random Password Tokens	
	e. RADIUS / TACACS+	
	f. Active Directory / LDAP integration	
28	The VPN device shall support following ESP encryption algorithms :	
	a. DES	
	b. 3DES	
	c. AES	
	d. AES-256	
29	The VPN device shall support following ESP authentication algorithms :	
	a. MD-5	
	b. SHA-1	
	c. SHA-256	
	d. SHA-512	
30	The VPN device shall support Diffie–Hellman key exchange group 1, 2 ,5 and 14.	
31	The VPN device shall support MD-5 , SHA-1 and SHA-2 hash.	
32	The VPN device shall support TLSv1.0, TLSv1.1, TLSv1.2 & TLSv1.3 protocols for SSL/TLS VPN.	
33	The VPN device shall support following End point Security policy enforcement before permitting access to the resources:	
	a. Pre-Specified checks such as Antivirus update, Malware, Spyware, Ports check, Process check, File check, Registry check, Software version check like antivirus version and custom checks based on user flexibility.	
	b. Auto-logoff with countdown prompt	
34	The VPN device shall be able to mitigate following attacks:	
	a. Denial of Service (DoS)	
	b. Distributed Denial of Service (DDoS)	
	c. Buffer Overflows	
	d. Ping of Death	
	e. TCP SYN Flood	
	f. UDP Flood	
	g. FIN scanning attacks	
	h. DNS based attacks	
	i. IP Spoofing	
35	The VPN device shall support authentication through following:	
	a. LDAP	
	b. Active Directory	
	c. Radius/ TACACS+	
36	The VPN device shall support authorization and accounting through RADIUS / TACACS+.	
37	The VPN device shall support the following features/functions	

	a. NTP (Network Time Protocol)/SNTP for date & time synchronization from NTP Server	
	b. DHCP Client / Server	
	c. DNS Client	
38	The VPN solution should support integration with SMS & e-mail gateway for generating OTP for VPN users which shall be delivered to users through SMS & e-mail gateway.	
39	The VPN device shall provide bandwidth management & QoS features like Diffserv marking, traffic prioritization, rate limiting etc.	
	Management and Reporting:	
40	The offered solution shall provide Logging/Monitoring through	
	a. Comprehensive event logging	
	b. Historical Reporting (at least 6 months)	
	c. Report generation	
	d. Syslog	
	e. SNMP v2 & v3	
	f. Real Time Monitor	
	g. E-mail Notification	
	h. GUI based interface	
41	The offered solution shall be manageable through:	
	a. Web User Interface HTTPS / client software for GUI access	
	b. Command Line Interface (console)	
	c. Command Line Interface (SSH)	
42	The offered solution shall be manageable from a centralized management & reporting server.	
43	Central Management & Reporting Server shall be appliance/server based and the specifications should be as per the recommendations of the OEM. All requisite hardware and software for Central Management & Reporting Server shall be provided by the bidder.	
44	The VPN device shall also be manageable by directly logging into VPN device through the web browser over HTTPS / client software over secure connection for configuration (addition, deletion, disable and edit) of VPN policies. In case direct access to VPN device for management purposes is not available, the bidder shall provide an additional Central Management server which shall be configured in 1:1 HA mode (Active / Passive) along with the Central Management Server specified in item no. 43. This is required so that if one of the management server fails, the VPN device shall be manageable through other central management server for making configuration changes in VPN policies.	
45	The Central Management & Reporting Server shall be able to handle 10 GB logs / day. The Central Management & Reporting Server shall have storage configured in RAID 1.	
46	The offered VPN solution shall also be able to provide 'At-a-glance-Dashboard' to provide overall status of the VPN device health (CPU, Memory etc), VPN traffic, concurrent user sessions, active IPSec tunnel etc.	
47	The centralized management & reporting server shall support IPv4, dual stack (IPv4 & IPV6) and IPv6 from day one.	
48	The communication between all the components of VPN solution (viz	

	VPN device and the GUI/WebUI/management Console) shall be authenticated and encrypted.	
49	The VPN solution shall provide access control mechanisms for its management based on IP address, ports & users.	
50	The Historical Reports shall be available for multiple time frames i.e. hourly, daily, weekly, monthly and customized period.	
51	It shall be possible to take manual or scheduled backup of configuration and policies of VPN solution.	
52	The VPN solution must support the archiving and backup of events and export to NFS/SMB/SCP/SFTP.	
53	The VPN solution shall support integration with SIEM (Security Information and Event Management). It shall be able to send logs to SIEM, Log Servers etc.	
54	The management solution should have in built database revision control for tracking the changes in policy ecosystem with option for administrators to allow installing specific version of policy.	
55	Management, Logging and Reporting shall not impact performance of VPN device.	
	The centralized management & reporting Server shall generate comprehensive GUI based Reports (both Realtime as well as Historical for at least 03 months period) for VPN related activity:	
	a. User sign-in and sign-out.	
	b. User file requests, uploads, downloads, etc.	
	c. Admin user connects and disconnects via telnet/SSH function to VPN device.	
	d. Bytes transferred for client/server application requests	
	e. User/admin authentication	
	f. Resources accessed by VPN user etc.	
56	The Historical report shall be available in formats as PDF, HTML, XML and CSV.	
57	The VPN solution shall support filtering of Reports based on various factors such as Username, Source / Destination IP Address, TCP/UDP Port Number, Protocol etc.	
58	The VPN solution shall provide forensic / investigative features wherein, in case of some attack, it would indicate type of attack, source destination of attack and other relevant information.	
59	Automatic online updates, patches against new exploits /vulnerabilities shall be provided by the OEM/OEM's partner.	
	Product / OEM Criteria:	
60	The VPN device / device Operating System should be tested and certified for EAL 4 / NDPP (Network Device Protection Profile)/NDCPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions or under Indian Common Criteria Certification Scheme (IC3S) by STQC, DEIT, Govt. of India.	