दि खामगांव अर्बन
को.ऑप. बँक लि., खामगांव
(मल्टीस्टेट शेड्युल्ड बँक)
मुख्य कार्यालय, खामगांव ☎(07263)254631
www.khamgaonbank.in
नातं विश्वासाचं...!

THE KHAMGAON URBAN CO-OP. BANK LTD

(KUCB)

RFP(BID) DOCUMENT

For

"Supply & Implementation of SDWAN Technology for KUCB"

Dated – 01-6-2023

Issued By

IT Department

Glossary

Abbreviations and Acronyms	Description
AMC	Annual Maintenance Contract
BEC	Bid Evaluation Committee
BOM	Bill Of Material
CA	Contract Agreement
EMD	Earnest Money Deposit
FMS	Facilities Management Service Provider
IA	Implementation Agency
IP	Internet Protocol
ISO	International Organization of Standardization
IT	Information Technology
LAN	Local Area Network
LLB	Link Load Balancer
KUCB	The Khamgaon Urban Co-operative Bank Limited
MIS	Management Information System
NGFW	Next Generation Fire Wall
O&M	Operation and Maintenance
OEM	Original Equipment Manufacturer
OS	Operating System
PAN	Permanent Account Number
PBG	Performance Bank Guarantee
RFP	Request For Proposal
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
DC	Data Center
DR	Disaster Recovery
DRS	Disaster Recovery Site

TENDER NOTICE

RFP FOR SUPPLY & IMPLEMENTATION OF SDWAN TECHNOLOGY

Date of issue of RFP	01-06-2023
Last date for seeking clarifications.	07.06.2023 before 6.00 p.m.
Last date for submission of bids	19-06-2023 before 6:00 p.m.
Date & Time of Opening of Technical bid	20-06-2023 at 3.00 p.m.
Date & Time of Opening of Commercial bid	Will be communicated by email

This Request for Proposal document ('RFP document' or RFP) has been prepared solely for the purpose of RFP is to Outsource the Supply & Implementation of SDWAN technology, which includes the warranty & support (24x7x 365) for a period of five years (3+2) Years under two Bid System viz.

1) Technical Bid & 2) Commercial Bid. The RFP document is not a recommendation, offer or invitation to enter into a contract, agreement or any other arrangement, in respect of the services. The provision of the services is subject to observance of selection process and appropriate documentation being agreed between KUCB and any successful Bidder as identified by KUCB, after completion of the selection process as detailed in this document.

VAPT

Successful Bidder has to give VAPT of all devices provided at its own expenses.

1.1. Disclaimer

Subject to any law to the contrary, and to the maximum extent permitted by law, Bank and its directors, officers, employees, contractors, representatives, agents, and advisers disclaim all liability from any loss, claim, expense (including, without limitation, any legal fees, costs, charges, demands, actions, liabilities, expenses or disbursements incurred therein or incidental thereto) or damage, (whether foreseeable or not) ("Losses") suffered by any person acting on or refraining from acting because of any presumptions or information (whether oral or written and whether express or implied), including forecasts, statements, estimates, or projections contained in this RFP document or conduct ancillary to it whether or not the Losses arise in connection with any ignorance, negligence, inattention, casualness, disregard, omission, default, lack of care, immature information, falsification or misrepresentation on the part of Bank or any of its directors, officers, employees, contractors, representatives, agents, or advisers.

1.2. Costs to be borne by Respondents

All costs and expenses incurred by Respondents in any way associated with the development, preparation, and submission of responses, including but not limited to the attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by KUCB, will be borne entirely and exclusively by the Respondent.

1.3. No Legal Relationship

No binding legal relationship will exist between any of the Respondents and KUCB until execution of a contractual agreement.

1.4. Recipient Obligation to Inform Itself

The Recipient must apply its own care and conduct its own investigation and analysis regarding any information contained in the RFP document and the meaning and impact of that information.

1.5. Evaluation of Offers

The issuance of RFP document is merely an invitation to offer and must not be construed as any agreement or contract or arrangement nor would it be construed as any investigation or review carried out by a Recipient.

1.6. Acceptance of Selection Process

Each Recipient / Respondent having responded to this RFP acknowledges to have read, understood and accepts the selection & evaluation process mentioned in this RFP document. The Recipient / Respondent ceases to have any option to object against any of these processes at any stage subsequent to submission of its responses to this RFP .

1.7. Errors and Omissions

Each Recipient should notify KUCB of any error, fault, omission, or discrepancy found in this RFP document not later than seven days prior to the due date for lodgment of Response to RFP.

1.8. Acceptance of Terms

Recipient will, by responding to KUCB for RFP, be deemed to have accepted the terms of this RFP including Introduction and Disclaimer.

1.9. Requests for Proposal

Recipients are required to direct all communications related to this RFP, through the Nominated Point of Contact person:

Contact	**:**	**Santosh Jadhao**
Position	**:**	**Chief Manager**
Email	**:**	**santoshjadhao@khamgaonbank.in**
Telephone	**:**	**9881745840**

KUCB may, in its absolute discretion, seek additional information or material from any Respondents after the RFP closes and all such information and material provided must be taken to form part of that Respondent's response.
Respondents should provide details of their contact person, telephone, fax, email and full address(s) to ensure that replies to RFP could be conveyed promptly. If KUCB, in its absolute discretion, deems that the originator of the question will gain an advantage by a response to a question, then KUCB reserves the right to communicate such response to all Respondents.
KUCB may, in its absolute discretion, engage in discussion with any Respondent (or simultaneously with more than one Respondent) after the RFP closes to improve or clarify any response.

1.10. Notification

KUCB will notify all short-listed Respondents in writing or by email as soon as practicable about the outcome of their RFP. KUCB is not obliged to provide any reasons for any such acceptance or rejection.

1.11. Rights to Terminate the Process

1. KUCB may terminate the bid process at any time and without assigning any reason. KUCB makes no commitments, express or implied, that this process will result in a business transaction with anyone.

2. This bid document does not constitute an offer by KUCB. The Bidder's participation in this process may result in KUCB selecting the Bidder to engage in further discussions and negotiations towards execution of a contract. The commencement of such negotiations does not, however, signify a commitment by KUCB to execute a contract or to continue negotiations. KUCB may terminate negotiations at any time without assigning any reason.
   - In case of the successful vendor, if the vendor fails:
     - ✓ To sign the contract in the form and manner to the satisfaction of KUCB
     - ✓ To furnish performance security in the form and manner to the satisfaction of KUCB

   - In case the successful Bidder fails to provide the Performance Bank guarantee within ONE month from the date of issue of Purchase Order by the Bank or signing of the contract, whichever is earlier, for any reason whatsoever?

1.12. Submissions of Bids

1. Complete bidding process will be offline in two bid system. All the notification and details regarding terms and conditions related to this bid notice hereafter will be published online on bank website www.khamgaonbank.in
2. Bidding documents can be downloaded from KUCB website. The deadline for submission of bid is specified in tender highlight of this document.
3. Technical bids will be opened as per the details found in tender highlight of this document.
4. Bidder should submit information in two bid system 1) Technical Bid (Technical bid) & 2) Commercial Bid as mentioned in the Bid Document.
5. Bidder may be requested to submit original documents for verification during evaluation of technical bids as and when required.
6. Time and date of opening of financial/commercial bid will be informed by email to technically qualified bidders.
7. KUCB reserves the right to accept or reject any or all the Bids without assigning any reason. Moreover, if no intimation is provided by KUCB then the documents submitted cannot be deemed as accepted.

1.13 Language of Bids

The Application and all related correspondence and documents in relation to the Bidding Process shall be in English language. Supporting documents and printed literature furnished by the Applicant with the Application may be in any other language provided that they are accompanied by translations of all the pertinent passages in the English language, duly authenticated and certified by the Applicant. Supporting materials, which are not translated into English, may not be considered. For the purpose of interpretation and evaluation of the Application, the English language translation shall prevail.

1.14 Bid Submission Format

1. The entire bid shall strictly be as per the format specified in this bid.

1.15 Documents Comprising of Bids

1. Following table is provided as the guideline for submitting various important documents along with the bid.

#	Type of Envelope	Documents to be submitted
01	Technical Bid	To be submitted OFFLINE
	Technical Bid Folder(Packet A)	● The Bidder must be authorized by OEM/ Distributer / Dealer "Technical Bill of Material and Bill of Quantity ● OEM declaration by Authorized Signatory to certify that the products quoted are not end of life for the next 7 years or end of sale products ● Compliance sheet of all hardware proposed in the bid along with Data sheet (clear highlighting the compliance in datasheet) ✓ **Technical Bill of Material with make and model of hardware** ✓ **Features and benefits** ✓ **Client List with contact address and telephone numbers**
02	BID Address	The Khamgaon Urban Co-operative Bank Ltd., Khamgaon [Multi-State Schedule Bank] Head Office: - Dhanwardhini, Shriram Shaligram Plot, Near A.K. National Highschool , In front of SBI(Main). Khamgaon, At-PO-Tq - Khamgaon (444303) Dist-Buldhana.
03	Commercial Bid Folder (PACKET B)	Material and services cost with details description Warrantee terms AMC Cost.

2. Bidders shall furnish the required information on their technical and financial bids in enclosed formats only. Any deviations in format may make the bid liable for rejection. Disclosure of Commercial information of the bid Technical Envelope shall be sufficient grounds for rejection of the bid.
3. The bidders shall categorically provide their Email-ID in packet 'A'.
4. Please provide following information about the Company (Attach separate sheet if required):

S. No	Information	Particulars / Response
1	Company Name	
2	Date of Incorporation	
3	Company Head Office / Registered Office and Addresses Contact Person(s) Phone Fax E-mail Website	
	Name of the CEO / MD	
	Nature of Organization (Proprietary / Partnership /Pvt. Ltd. Co / Public Ltd. Co)	
	Registered / Corporate Office Location	

4	Provide the range of services /options offered by you covering service description and different schemes available for: • Supply of Devices • Implementation Support • Warranty • Post-implementation • Ongoing Support for: - ▪ AMC ▪ Training ▪ Documentation ▪ Others (specify)			
	Number of Employees by Function: 1. Development 2. Quality Assurance 3. Implementation 4. Sales and Support 5. Administrative 6. Management			
	Support Centre details and products supported by these centres			
	Any affiliates / associated businesses			
5	Any pending or past litigation (within three years)? If yes please give details. Also mention the details of claims and complaints received in the last three years (About the Company / Material that are sold / licensed by the company).			
6	Please mention turnover for last three years and include the copies of Balance Sheet in support of it	Year	Turnover	Profit/Loss(-)
		2020-21		
		2021-22		
		2022-23		

5. Commercial Bid Format : -

SRN	Particulars	Proposed Brand Name & Ver.	QTY	Unit Cost	Total Cost
1	Hub End Devices DC (HA)				
2	Hub End Devices DR (HA)				
3	Branch End Devices				
4	One time Cost of Implementation (IF)				

5	Support/AMC				
6	Licenses (if)				
7	Delivery terms				
8	Payment Terms				
9	Warrantee Terms				
10	Total Cost of Project One Year				
11	Total Cost of Project Three Year				
13	Total Cost of Project Five Year				

1.16 Rights to Accept/Reject any or all Bids

Notwithstanding anything contained in this TENDER, KUCB reserves the right to accept or reject any Application and to annul the Bidding Process and reject all Applications/ Bids, at any time without any liability or any obligation for such acceptance, rejection or annulment, and without assigning any reasons therefore. In the event that the Authority rejects or annuls all the Bids, it may, in its discretion, invite all eligible Bidders to submit fresh Bids hereunder.

KUCB reserves the right to reject any Application and/ or Bid if:

1.16.1 at any time, a misrepresentation is made or uncovered, or

1.16.2 the Applicant does not provide, within the time specified by the Authority, the supplemental information sought by the Authority for evaluation of the Application.

In case it is found during the evaluation or at any time before signing of the Agreement or after its execution and during the period of subsistence thereof including the concession thereby granted by KUCB, that one or more of the pre-qualification conditions have not been met by the Bidder, or the Bidder has made any misrepresentation or has given any incorrect or false information, the Bidder shall be disqualified forthwith if not yet appointed as the Successful Bidder either by issue of the LOA (Letter of Approval) or entering into of the Agreement, and if the Bidder has already been issued the LOA or has entered into the Concession Agreement, as the case may be, the same shall, notwithstanding anything to the contrary contained therein or in this TENDER, be liable to be terminated, by a communication in writing by KUCB to the Bidder, without Bidder being liable in any manner whatsoever to the Bidder and without prejudice to any other right or remedy which KUCB may have under this TENDER, the Bidding Documents, the Concession Agreement or under applicable law. KUCB reserves the right to verify all statements, information and documents submitted by the Bidder in response to the TENDER. Any such verification or lack of such verification by KUCB shall not relieve Bidder of its obligations or liabilities hereunder nor will it affect any rights of KUCB there under.

The bid shall be rejected if the bidder-

1.16.2.1 Stipulates own condition/conditions.

1.16.2.2 Does not fill and (digital) sign undertaking forms, which are incorporated, in the document.

1.17 Performance Bank Guarantee

1. The Bidder shall at his own expense, deposit with BANK, within thirty (30) working days of the notification of award of the contract an unconditional and irrevocable Performance Bank

Guarantee (PBG) from the list of approved banks (specified in the bid document) as per the format given in this bid, payable on demand, for the due performance and fulfilment of the contract by the Bidder.

2. This Performance Bank Guarantee will be for an amount equivalent to 10% of the total contract value. All charges whatsoever such as premium, commission, etc. with respect to the Performance Bank Guarantee shall be borne by the Bidder.

3. Details on validity of the performance bank guarantee are specified under Tender highlights of this document. The Performance Bank Guarantee letter format can be found in this document.

4. The Performance Bank Guarantee may be discharged/ returned by BANK upon being satisfied that there has been due performance of the obligations of the Bidder under the contract. However, no interest shall be payable on the Performance Bank Guarantee.

5. In the event of the Bidder being unable to service the contract for whatever reason, KUCB would evoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of KUCB under the Contract in the matter, the proceeds of the PBG shall be payable to KUCB as compensation for any loss resulting from the Bidder's failure to complete its obligations under the Contract. KUCB shall notify the Bidder in writing of the exercise of its right to receive such compensation within 14 days, indicating the contractual obligation(s) for which the Bidder is in default.

6. The 30 day notice period shall be considered as the 'Cure Period' to facilitate the Implementation Agency to cure the breach. The PBG shall be evoked only if the breach is solely attributable to the bidder and the bidder fails to rectify the breach within the 'Cure Period'.

7. KUCB shall also be entitled to make recoveries from the Bidder's bills, performance bank guarantee, or from any other amount due to the Bidder, the equivalent value of any payment made to the Bidder due to inadvertence, error, collusion, or misstatement.

2. Scope of Work

The below mention requirements under this RFP should be treated as the minimum requirement but not limited to

2.1 Project Objective

The KUCB wishes to engage an agency (hereafter referred to as "Service Provider", "Selected Agency", "Vendor", and "Bidder") for supply & Implementation of SDWAN Technology hardware appliance basis for KUCB offices for 5 years with warranty and 24x7x365 technical support.

Our objective to establish SDWAN is to get uninterrupted smooth connectivity, Bandwidth Aggregation, Network Security and Centralized Management and Centralised real time Monitoring of Network.

2.2 Present Architecture

Presently, all the Offices of KUCB are connected through a MPLS (WAN) technology. Primary connectivity is MPLS provided by BSNL. For Secondary connectivity we are using IPSEC VPN over internet broadband supplied by Airtail, BSNL and Vodaphone .All Branches are connected to Data Center and Disaster Recovery Site.

2.3 Summary of Scope

The supply for SD-WAN, integrated with AAA, Bandwidth Aggregator, Cyber Security. All in one Box with 3G/4G/5G, PPPoE, Dynamic/Static WAN links and minimum 4 ports of Ethernet LAN/WAN

Switchable port with multi-source Internet Connectivity (Internet/broadband/Dongle) and MPLS links. Utilization Report/Graph, Monitoring of link. All Servers including orchestration, Database Server will be on Premises from day one only. Supply of software and hardware for AAA, Bandwidth Aggregator, SD-WAN, Security, as single tightly integrated solution. All Orchestration software should be hosted in Datacenter and on other site/location as backup information will be shared by KUCB. OEM needs to provide the audit report for execution of completion of every purchase order. OEM to produce the certificate if the devices are installed as per best industry practice.

2.4 Project Management Plan

The success of the project depends on the proper project planning and management. At the onset, the System Integrator shall survey KUCB location and plan the project implementation in great details and should provide a micro level view of the tasks and activities required to be undertaken in consultation with KUCB. Initial list of planning related tasks and procedures (along with corresponding documentation) that the Service Provider should be submitted at the onset is as follows:

- Project Schedule: A detailed timeline indicating various activities to be performed along with completion dates and resources required for the same.
- Transition Plan: Bidder to provide the detailed approach & plan for replacement of the hardware.
- Progress Monitoring Plan: Detailed Daily, Weekly, Monthly Progress Report formats along with issue escalation format. The bidder has to take the approval of the report format before start of the project.
- Standard Operating Procedures: Detailed procedures for installation, configuration, and monitoring of KUCB network to be shared with the department.
- Risk Mitigation Plan: List of all possible risks and methods/procedure to mitigate them.
- Escalation Matrix & Incident Management: A detailed list of key contact persons with contact details with escalation hierarchy for resolution of issues and problems. This has to be via an Incident Management system
- The bidder shall be responsible for documenting configuration of all devices and proper Network diagram files, so as to enable quick recovery in case of failure of devices.
- The selected bidder shall document all the installation and commissioning procedures and provide the same to KUCB within 15 days of the commissioning.
- The bidder shall also be responsible for maintenance and updation of all the policy documents including but not limited to security policy, configuration policy etc.
- To finalize the different type of report in coordination with IT department. The report format is required to submit under plan. Various report like Daily, Monthly, Quarterly etc.
- OEMs of disparate solutions should be involved in this phase. Specifically, all the OEMs should certify and endorse the final design document

2.5 Bandwidth Aggregation

The solution should be able to combine bandwidth from sources like Internet Leased Lines (ILL), MPLS, Broadband as well as 3G/4G/5G LTE. The Bandwidth aggregation should support aggregation of links irrespective of its types. IT should support following configuration at minimum.

- combine multiple Internet links, such as broadband, MPLS, 4G/5G, or satellite connections, to increase bandwidth, reliability, and overall network performance.
- For ILL, MPLS , broadband connection and 3G/4G/5G (Aggregation must be link independent)

- required ports to aggregate at least three links
- Load balancing Algorithms and method for support

2.6 ROUND ROBIN

Bandwidth Algorithm Round Robin should forward each request to each WAN link from the available links, in linear order. Once it reaches the last WAN link, the loop should return to the first WAN link and starts over again. Weighted round robin scheduling can allow different applications to get a fair share of the bandwidth while strict priority queuing can minimize jitter and latency for time-sensitive applications.

2.7 PERSISTENCE

Should directs traffic through the same connection persistently, based on its source and/or destination IP addresses. Traffic should continue to move on the same connection until the end of the session.

2.8 PRIORITIZATION

Should enable routing of traffic by setting an order of connectivity priority, where traffic is redirected via prioritized healthy links and only use lower-priority links when current active connections fail.

2.9 ENFORCED MODEL

Under this option, Bandwidth Aggregation should direct a fixed volume of traffic through a pre-determined connection, allowing users from specific IP addresses to access servers and restricting outbound traffic to a specified connection.

2.10 FASTEST RESPONSE TIME

The load balancer should choose the WAN link with the lowest response time—which means the load balancer picks the quickest responding WAN link to process a request.

2.11 SD WAN Architecture

Software Defined Wide Area Network (SD-WAN) should be integral part of the entire solution, providing a centrally hosted solution for management, enabling our IT staff to remotely program edge devices and make changes in network policies centrally, in real time. The SD-WAN has to be compatible with the current technology being used at KUCB and must be capable of upgradable in terms of technology, functionality and scalability.

2.12 True SD-WAN architecture

True SD-WAN architectures aim to enhance network agility, improve application performance, and simplify network management through centralized control, dynamic traffic routing, and security integration. By decoupling network control from physical hardware, KUCB be able to achieve greater flexibility, scalability, and cost-efficiency in managing the wide area networks.

The true SD-WAN Architecture typically consists of the following components:

Edge Devices: Appliances deployed at each branch office or site. They form the endpoints of the SD-WAN network and are responsible for handling network traffic.

Centralized Controller: The controller is a centralized management system that should oversees the entire SD-WAN infrastructure. It should provides a single point of control for configuring and managing the network, including policies, security settings, and traffic routing.

Overlay Network: SD-WAN uses an overlay network, which is a logical network abstraction that operates on top of the underlying physical network infrastructure. This overlay network allows for the creation of virtual networks and the routing of traffic across different paths based on network conditions.

Dynamic Path Selection: SD-WAN architectures employ dynamic path selection mechanisms to optimize network traffic based on real-time conditions. This includes monitoring link performance, such as latency, packet loss, and bandwidth, and dynamically routing traffic over the most suitable path.

Traffic Segmentation: SD-WAN allows for the segmentation of network traffic into different classes or categories based on policies. This enables organizations to prioritize critical applications, ensure better performance for specific traffic types, and apply security measures accordingly.

Security Integration: True SD-WAN architectures incorporate security features into the network design. This can include encryption, firewall capabilities, intrusion prevention systems (IPS), and secure web gateways (SWG). Security policies can be centrally managed and enforced across all network sites.

Orchestrator: An orchestrator is a higher-level software layer that integrates with the SD-WAN controller and provides additional management and automation capabilities. It enables organizations to streamline network operations, configure policies, and gain visibility into network performance through a centralized interface.

The SD-WAN solution should include all the below mentioned functionality and features.

- Orchestrator
- Orchestrator should be hosted on custom domain (URL) provided during implementation.
- Centralized monitoring dashboard
- Hardware monitoring (Load Average, RAM /HDD /CPU Utilization)Threshold based alerts and notifications
- Network WAN/LAN/SDWAN monitoring with alerts and notifications

2.13 Orchestrator (Centralized Policy Management and SDWAN Controller)

- All network-wide configuration & application routing policies shall be from the Centralized policy management and SDWAN controller.
- All configurations of the Edge / Gateway following successful installation shall be conducted via the SDWAN controller.
- The Centralized policy management and SD-WAN controller must have web-based GUI.
- All communications between the Edge / Gateway and SD-WAN controller shall be encrypted with industry standard strong encryption.
- When using multiple underlays with different WAN addressing, the solution must support management over any WAN address. If any or multiple of the WAN links fail, it must be possible to operate / manage the solution over any remaining interface(s)
- Application-wise and Tunnel-wise priority

2.14 Basic Routing: Gateway & Edges shall support:

- The overlay paths established amongst the edge devices must support the ability to run routing protocols: OSPF/BGP for IPv4.
- 802.1Q on LAN and WAN interfaces should be applicable.
- BGP on both LAN (for learning customer addresses) and WAN (for learning underlay addresses) interfaces
- BGP peer from access to WAN over underlay
- Local IP breakout to underlay network, be it Internet or IPVPN
- SDWAN Edges shall support configurable IPv4 NAPT for traffic breaking out to the underlay on WAN interfaces
- Edges shall support configurable IPv4 1:1 and 1:N NAT on WAN interfaces for traffic breaking in / out to the underlay on WAN interfaces
- It shall be possible for users to define 'applications' based multiple priorities (source prefixes, destination prefixes, IP protocol number, tcp source ports, tcp destination ports) for use in application monitoring and application policies.
- The edge devices shall support shaping of WAN/LAN egress traffic.
- The edge devices shall support policing and packet filtering of ingress/egress traffic
- Ability to translate between different packets and exchange reachability information across different protocols
- SDWAN Gateway will have to appropriately distribute routing information between domains authorizing the creation of the forwarding path.
- To support Internet Breakout supporting NAT and Native IP Routing

2.15 Network Services

- Multi-Hybrid WAN Connectivity (ILL, PPPoE , DHCP, 4G, 5G LTE, 5G)
- SD-WAN should offer an extensive list of capabilities including sub-second packet steering across multiple WAN interface, packet loss reduction through services such as FEC, packet replication, and poor performing link avoidance.
- Route exchange should be with SDN controller, stateful high-availability, link aggregation, hierarchical QoS, per tunnel QoS, and overlay encapsulation options (VXLAN, IPSec).
- Should be available as software to deploy in on-premises hardware including appliances, , hypervisors, or containers.
- L3 VPN - Should support multi-VRFs on SDWAN remote Device
- L3 VPN - Seamless Interop with Existing L3 VPN Services
- Application aware traffic redirect capability
- Full-mesh, hub-and-spoke, and hybrid connectivity models
- Static/Dynamic routes
- Ingress QoS with configurable rate limiting parameters
- Enterprises use private IP numbers; hence IP conflict has to be supported by solution, as per case.

2.16 Service Topologies to be supported by same instance of SDWAN core components

- SDWAN solution should support all remote offices on internet or local break-out.
- However, it should support few Remote offices on MPLS as well as on Internet

2.17 Transport Independent Overlay Network

- Each edge device must dynamically establish fully meshed encrypted overlay paths to every other edge device, across multiple different WAN services: L3VPN, Internet and Cellular Data connectivity (3G/4G /5G LTE etc.)
- Each edge device must dynamically establish fully meshed encrypted overlay paths to every other edge device, across multiple different WAN services: L3VPN, Internet and Cellular Data connectivity (3G/4G/5G LTE etc.).
- The solution must support site-to-site remote routing via WAN aggregation; hub & spoke model and/or any-to-any
- The solution must support dynamic optimal direct site-to-site remote routing (spoke- to-spoke model)

2.18 Overlays & Network

- The overlay paths established amongst the edge devices must support Transport of unicast and IP based traffic
- The overlay services shall support both encrypted and non-encrypted modes of operation for all overlay types
- The solution shall support Multiple independent overlay services per Edge, with independent routing tables (allowing overlapping addressing) separated on the LAN side via different ports
- The solution should support Controller Less operations
- The overlay shall support Micro-VPN services (IP routing contexts) that are local to the box, for example to support guest wifi LANs
- The solution must be capable of advertising and withdrawing user routes to the LAN VPN PE, if the Edge / Gateway can establish a data-plane connection (tunnel) to the target Edge / Gateway.
- The solution shall allow to dynamically add and remove services as required
- The system must support local internet break out i.e. local users in each of the remote offices must be able to access Internet directly without going through the Hub location.
- The system must support local internet breakout for specific Application/applications e.g. remote offices locations must be able to access Office 365 over local Internet directly (local breakout) without going through the centralized Internet Gateway of DC and/or DR.
- Local Internet breakout must be configurable per remote offices per application or combination of the two, as the case may be
- The solution shall support multiple Tenant networks isolated from one another
- The solution shall support a set of distinct networks for a single Tenant
- When using multiple underlays with different WAN addressing, the solution must support management over any WAN address. If any or multiple of the WAN links fail, it must be possible to operate / manage the solution over any remaining interface(s)

2.19 Dynamic Load Sharing of Traffic Based on defined Business logic and/or application policies

- Edge devices must be able to load balance traffic across multiple WAN paths based on load balancing algorithms efficiently using all available WAN bandwidth

- The solution shall support a mechanism to load balance traffic across multiple underlays / tunnels on a per flow basis based on policy and the detected performance of the underlay / tunnel
- The solution must be able to make decisions to forward critical applications over the best-performing path based on the defined application policy based network performance— packet loss and delay by offered solution
- The solution must respond to measured performance changes (degradation) in addition to link and node state changes (up/down) and adjust application forwarding accordingly
- The solution must be able to prioritize time sensitive traffic over other traffic

2.20 Application Management

Edge devices must be able to identify and classify applications. Identification and classification of at least the following classes of application types must be supported by the solution:

- Mailing solutions /Office 365
- Web based applications
- Video Conferencing
- Solution to alert if the application is receiving an acceptable service from the underlay
- The solution must be able to dynamically control data packet forwarding decisions by looking at application type, performance, policies, and path status

2.21 Remote location Enablement - Self- installation and Activation (auto configuration)

The solution shall support remote offices which have 3G/4G/5G connection to the internet.

- The solution must support zero-touch provisioning/plug-n-play for new remote offices, which entails on- site remote offices personnel having to make physical (i.e., cabling) changes only and administrators not having to make configuration changes to bring new remote offices online
- The Remote offices would terminate multiple transport media viz., links (from multiple service providers), Internet link (broadband), LTE etc on the EDGE SERVER(s).
- The Edge WAN link will be provided with an IP address, netmask, default gateway and DNS server via DHCP, PPPoE, 4G/5G LTE or Static configuration
- The solution shall not require any off-site customer specific pre-staging / pre-configuration
- The auto configuration system shall require secure mutual authentication of the SDWAN controller and specific SDWAN Edge
- Individual SDWAN Edges shall be identified by a unique key / certificate which is installed on to the Edge by the trusted installer at installation time by some simple but secure method requiring no or minimal manual data input
- The URL of the SDWAN controller shall not be pre-installed in the Edge and shall be provided at installation time by the trusted installer
- The solution shall allow for one (1) and two (2) factor of activation of SDWAN Edge and Gateway devices
- The solution shall operate when the Edge devices are behind NAT (NAT-T)
- The solution shall support hybrid remote offices which have a WAN connection and a second WAN connection to the internet
- When deployed with a mix of hybrid Edges, IP VPN connect Edges and Internet connected Edges, Edges will continue to be able to communicate under asymmetric break conditions as long as all sites have at least one active connection
- In case of failover of any transport media or EDGE SERVER, the connectivity should be automatically established with the alternate transport media on EDGE SERVER

- Remote offices should be able to aggregate / use bandwidth from all the transport media terminating on single EDGE SERVER or multiple Edge server at the location

2.22 Centralized Management, Monitoring and Configuration of WAN

- The solution should support TLS 1.2 or higher for management web GUI SSL access for better security.
- The solution must provide unified platform for Service Assurance, Change and Compliance management
- The solution to offer Auto Discovery of SDWAN network consisting of SDWAN controller, gateway, orchestrator, Edge server, EDGE SERVER interfaces etc
- Auto discovery should be supported
- The Centralized management solution must provide GUI based Platform for real time alerts monitoring, assurance and reporting
- The system must provide state full alarms/alerts for entire lifecycle of alarms/alerts
- The solution must offer topology based real time monitoring for Up/down status, Application accessibility alerts, EDGE SERVER alerts etc
- The solution must offer real time dashboards of status of network , Edge server and interfaces including trending to facilitate operations of entire solution and impact on users (if any)
- The solution must offer near real time dashboards of application experience including trending to facilitate management of impact on users (if any)
- Network Performance Measurement to monitor overlay performance (round trip delay & packet loss) and make an intelligent forwarding decision based on application based SLA requirements
- Visualization using charts, real-time views, maps, grids
- The solution must be able to monitor the network performance—packet loss and delay to aid policy formulation for automatic routing based on defined thresholds
- The solution must respond to link and node state changes (up/down) and adjust application forwarding accordingly
- The solution shall provide information / metrics on the current and historic overall traffic utilization (total egress, ingress bandwidth)
- The solution to syslog based collection of statistics from Edge server
- The centralized management solution must have web-based GUI (HTTP) / (HTTPS)
- The solution must provide user guide for deployment and management of SDWAN infrastructure
- All network-wide configurations shall be from the centralized management appliance
- All application forwarding policies shall be configured from the centralized management appliance
- The centralized management solution shall have NMS capabilities and must support network wide device and network visibility for all the devices in the scope of the solution
- The NMS should be configured to monitor all the links terminated on the devices irrespective of the type of link (broadband, LTE, Internet etc).
- Wherever Internet is terminated locally on the EDGE SERVER, it must be feasible to remotely configure the EDGE SERVER for local breakout to access Internet
- The remote offices Edge server should also be configurable to access centralized Internet DC and DR for internet, in case local internet fails, automatically without any manual intervention

- The solution must support automatic upgrades of Updates/Patches/Versions of all software components including operating systems, firmware, management software, security software or any other software, which would be part of the the remote offices Edge server

2.23 Monitoring, Reports and Analytics

- The solution must be able to collect and aggregate traffic statistics for all WAN paths. Traffic statistics include path utilization, application specific utilization and path performance
- The solution must support device health monitoring for all the devices within the solution scope
- The solution must store historical traffic and performance information for at least one year to assist with trouble analysis, traffic forecasting and SLA compliance
- The platform shall monitor WAN routes and raises alarm in case of WAN route instability or outage, as per the case
- The solution shall provide tools to do Configuration Audit
- The solution must support email-based alarm to notify the administrators when any device/link fault or network performance degradation happens
- The solution must offer module for detailed reporting of various Use Cases for managing entire solution
- Solution should offer Real & historical time series log event reporting
- Solution should offer Reporting of Traffic usage detection
- Solution should offer Uptime reports - Application availability, Remote offices uptime, Network uptime, Uptime SLA reports wrt Network Service provider (Internet/LTE)
- Traffic reports per site: bandwidth usage per access circuit, bandwidth usage per application, latency,packet loss, QoS per access circuit etc.
- Solution should offer reporting, both
- Solution should offer integration with email system
- The solution shall provide graphical dashboard with following KPIs
- Hardware Device, Traffic & Network Health Monitoring on Daily, Weekly, Monthly & Yearly basis for
- Device Memory Usage (graphical)
- Load Average(graphical)
- CPU Temperature / Utilization
- Hard Disk Utilization
- Physical Interface Monitoring like LAN& WAN Ports
- Tunnel Status:
- System should have facility to export report in following formats
- CSV
- PDF
- XLS / XLSX
- Should have facility for Predefined and custom report templates
- Application reports should have : Top Applications usages, Top URLs, Top Bandwidth Consuming Applications
- Should support Site based Application usage analysis report
- The Reporting solution must have web-based GUI (HTTPS)
- Solution should offer individual real-time dashboards for respective remote offices
- Following reports shall be essential part of the solution
    a) Traffic Throughput reports
    b) Application bandwidth reports
    c) Application SLA Violations reports

d) Network Performance (NPM)
e) Security Audit report

2.24 Architecture of Core Components

- The Centralized policy management and SDWAN controller to be installed at Mumbai Location, depending on requirements
- The solution has to facilitate multi tenancy of Enterprise customers, from same instances of SDWAN core components
- The solution must be modular wherein segregation of Control Plane & Management Plane should be possible
- It should be possible to segregate control plane & management plane so that control plane can be hosted at remote offices, if required
- SDWAN Controller, Policy Engine, Service Provisioning & Assurance (including reporting module) applications shall be deployed in HA configurations (Active-Hot standby)
- The auto switchover from Active to Hot standby should happen within 3 minutes
- The Centralized policy management and SDWAN controller should have web based GUI.
- The solution shall support multiple Tenant networks isolated from one another
- The centralized internet access or local break out policies must be customizable dependent on remote offices requirement

2.25 Legacy and Migration

- Ability to provide a gateway function between the legacy, non-SD-WAN brownfield network and the new SD-WAN network
- To provide temporary connectivity between IPVPN and SDWAN architectures, for the duration of a customer migration to SDWAN
- Monitors and implement application traffic identification and steering functions to & from the legacy world
- Solution shall support creation of Multi-Hybrid WAN by providing permanent connectivity between legacy topologies and new SDWAN architecture

The in-built solution for Authentication, Authorization & Accounting (AAA) and Bandwidth management should support following functionalities and features.

2.26 User Management

- Local Authentication as well as external AAA supported
- PAP/CHAP/MSCHAP v-1/2
- IPoE/PPPoE/MAC/Captive Portal /VLAN Type Local/Radius Authentication
- Local/Radius - Pool/Authentication
- Static IP via Radius and Local authentication
- Access based on Time and Date time restriction
- Data transfer based Quota allocation per Rate-limit per QoS
- Schedule based Rate-limit and burst
- Real time QoS User/Group Policy update
- QoS via Radius and Local authentication
- Per User Online Traffic Monitor Accounting/Session /Graph
- Error Handling Redirect to Expired/Disabled/unauthorised
- Limited/unlimited/Fair Usage support

QoS

- User/IP/Subscriber wise
- Group wise
- Application based
- Real time Dynamic Bandwidth
- Destination Based IP address/Pool

2.27 Administration

- Role-based administration
- Multiple administrators and user levels Per interface
- Upgrades & changes via Web UI
- Department/Branch/Franchise/Operator Management
- Backup/Restore configuration
- Universal Time Zone Settings
- Config/access log with rollbacks
- All services and Remote Radius SMS, Service alerts
- Multilingual UI

2.28 Security And Encryption

- All remote site traffic must be encrypted when transported over WAN transport links: ILL/PPPoE/ 4G/5G LTE and/or Internet protecting Data Confidentiality and Integrity
- Should be capable of continuously detect software vulnerabilities with the most comprehensive signature database, across the widest range of asset categories.
- Should be capable of Detecting and inventory of all known and unknown assets that connect to global hybrid-IT environment.
- Should be capable of Vulnerability Management, Detection, and Response.
- Prevent security incidents by minimizing the attack surface with software-defined micro segmentation and policy enforcement
- Alerts you in real time about network irregularities. Identifies threats and monitors unexpected network changes before they turn into breaches.
- The solution shall support scalable IPSec for full mesh networking
- Should be capable of Passive Scanning Sensor (PS) continuously monitors of all network traffic and flags any asset activity. It identifies and profiles devices the moment they connect to the network.
- The solution should Pinpoint your most critical threats and prioritize patching. Using real-time threat intelligence and machine learning, take control of evolving threats, and identify what to remediate first.
- The solution should be able to do continuously monitoring of all network traffic and flags any asset activity. Identify and profile devices the moment they connect to the network, including those difficult to scan, corporate owned, brought by employees, and rogue IT.
- Should be capable of proactively address potential threats. Whenever new vulnerabilities and threats, attacks or suspicious activities appear, real-time alerts notify immediately.
- Encryption shall be supported for all overlay services to support L3
- The encryption must be done as per IPSec standards using AES with 256bit keys
- The use of encryption should not limit the performance or availability of remote site applications and should be transparent to end users
- The solution must support traffic filtering based on following criteria
    - Country
    - Domain

- O Content
- O IP / IP Pool
- O Pre-defined URLs

- The solution shall support following features
  - User IP Address Tracking
  - Duplicate Address Detection
  - SPAM Control filter
  - Basic DDOS control
- The solution shall support Whitelisting of IP range/subnets
- Complete isolation of Edge server & SDWAN solution from Public Cloud hosted applications
- The proposed SDWAN solution should support DDoS Protection
- The solution shall support multiple user accounts per enterprise with individual user logins
- The solution shall support multiple levels of user permission, specifically a read only
- Communications between network elements and systems must be capable of strong, mutual authentication
- The solution shall support configuration history and change control
- The solution shall support rollback of configuration changes
- The logs of devices should be able to be integrated with Syslog for co-relation and analysis, if required

The hardware should have provision to subscribe threat Protection in future that includes:

- ZERO DAY – Vulnerabilities for which there is no vendor patch available and for which an active attack has been observed in the wild
  Sites/Domains that initiates such attacks should be blocked.
- PUBLIC EXPLOIT – Vulnerabilities(Sites/Domains) whose exploit knowledge is well known and for which exploit code exists and is publicly available
- URL Filtering – L7 access controlled for users restricted their access to unwanted sites / Domains
- ACTIVELY ATTACKED – Vulnerabilities that are being actively attacked in the wild
- HIGH LATERAL MOVEMENT – Vulnerabilities that, if compromised, let the attacker propagate the attack broadly throughout the breached network
- EASY EXPLOIT – Vulnerabilities that can be exploited easily, requiring few skills and little knowledge
- HIGH DATA LOSS – Vulnerabilities whose exploit will yield massive data loss
- DENIAL OF SERVICE – Vulnerabilities whose payload could overload or crash the compromised systems so that they become permanently or temporarily unavailable
- NO PATCH – Vulnerabilities for which there isn't a fix from the vendor
- MALWARE – Vulnerabilities (sites/Domains) associated with malware infection
- EXPLOIT KIT – Vulnerabilities for which an exploit kit is available. Sites / Domain that injects an exploit kit.

2.29 Hub End Device

- The proposed SDWAN Gateway appliance should have a minimum of 4 Nos or above 1G Base T interface port with 2 x 10GSFP+ slots & minimum 2 X USB.

- The hub gateway appliance should be hosted in HA from day 1
- The solution should support on the number of users it can support and the throughput of the device.
- The SDWAN appliance must support universal ports with the ability to configure any port as LAN/WAN in the field
- NAT support: static NAT, dynamic NAT, PAT
- IPv6 Support: Management over IPv6, IPv6 routing protocols, IPv6 tunnelling, IPv6 IPsec VPN
- IPv6 SDWAN Support: Ping6 link monitor, IPv6 source and destination objects
- Needs to support minimum one RJ45 console port for OOB management.
- The proposed SDWAN Gateway Hub Router should support throughput of minimum 10 Gbps.
- The proposed SDWAN Gateway Hub Router should support throughput of minimum 2 Gbps aggregated VPN throughput.
- Should not impose license-based limitation on number of remote access VPN users. Should support upto 1000 site- to- site secured VPN Tunnels.
- Should support dynamic routing protocols like BGP & OSPF etc.
- Should support IPV6 from day one.
- Should support the IPsec VPN deployment modes: Gateway-to- gateway, hub-and-spoke, full mesh, redundant-tunnel.

2.30 Branch Device

- Proposed SDWAN appliance must be of desktop form factor with minimum of 4 Universal ports that can be configured as WAN, LAN (100/1000 RJ-45) Ports and 2 USB ports for 4G/5G LTE Dongle.
- The appliance should support HA for future without any additional license requirements for SD-WAN
- The appliance should be preferably desk mount, energy friendly with fan less design
- The SDWAN appliance must support universal ports with the ability to configure any port as LAN/WAN in the field
- SDWAN appliance must be capable of terminating broadband, ILL, MPLS, 3G/4G/5G, PPPoE connectivity
- SDWAN solution must be able to use minimum 2 WAN links together at same time
- SDWAN appliance must be able to support minimum of 200 IPSEC VPN tunnels
- The appliance should support minimum 1 Gbps SDWAN throughput
- Proposed SDWAN Gateway Hub Router should throughput of minimum 300 Mbps of L7 NGFW throughput
- Proposed SDWAN Gateway Hub Router should throughput of minimum 600 Mbps of aggregated VPN throughput
- Should include the dynamic routing protocols like BGP & OSPF etc.
- Should be able to support VoIP traffic
- Should support IPV6 from day one
- Should support the IPsec VPN deployment modes: Gateway-to- gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode
- Should include IPsec Configuration Wizard for termination with popular third-party devices
- Should support Built-in DHCP

- The operating temperature of the appliance should be supported upto 65C

2.31 Other General

- On detection of change of WAN IP/ISP of the device, there should be an alarm functionality to lock the device & OTP based SMS to activate the device
- The SDWAN solution should be software based capable of running on any X86 hardware with support for VNF and therefore should not any OEM specific ASIC-based offering
- X86 provides better scalability, protection against vendor lock in on hardware and also deploy third party gateway functions like firewall, server load balancer reducing the inventory and its related management overhead
- Proposed Solution should allow user to choose custom Security associations with all available encryption algorithms, DH Groups etc. as per the standards
- **The solution should be implemented as true software defined WAN network architecture. SDWAN network architecture should have clear separation of management/ control, and data plane functions.**
- True SD-WAN solution which can give the full functionality and flexibility of SD-WAN with no halfway measures or look alike functionalities
- The solution needs to be flexible enough to support customization in case of any unique requirements with the availability of the OEM engineering and support team in India
- Proposed SD-WAN solution may be Make in India but should be Class -1 MII with all the Technology IP ownership within India under Make in India policy of Govt. of India subject to satisfy all the requirement and performance of true SDWAN solution.
- Solution needs to provide real-time analytics on the CPE health status, WAN links status, application wise bandwidth utilization status with minimum CPE resource utilization
  (Only real time analytics can support real time decisions and pro-active problem identification and resolution. Near real time solutions give 5 – 10 mins old statistics which may not be as effective as real time analytics)
- Solution should have the capability to use Standard IPSEC with AES256 encryption and other standard encryptions like Poly1305 and Chacha20
  (Poly1305 and Chacha20 are the most updated security algorithms used to ensure better security that the traditional IKEv1 and IKEv2)
- The SDWAN should support Mobile Application based zero touch deployment.
- The solution should be using advanced protocol for analytics and WAN monitoring instead of SNMP which is resource intensive for real time applications.

2. 31 Support & AMC

All the hardware, software products supplied should carry a minimum warranty of 5 (3+2) years from the date of operationalization of the system to the satisfaction of KUCB. On-site, comprehensive, back-to-back from Original Equipment Manufacturer (OEM) for a period of 5 (3+2) years from the date of installation (if applicable). The warranty also includes all software subscriptions (critical hot fixes, service packs, and major upgrades). Remote access to Installed systems will be provided from our head office

The AMC shall be:

- On-site/Remote, comprehensive, back-to-back from OEM for all hardware and software products as a part of RFP till the end of contract i.e. for 5 year.
- Software updates and upgrades at no extra cost to KUCB

- Replacement of failed hardware (if applicable) within N e x t b u s i n e s s d a y from the time call is lodged for critical location.
- Comprehensive on-site support from bidder for operational issues as and when arises.
- Any other hardware / software required to complete the solution / achieve functionality to be provided by the bidder, without any additional cost
- All the hardware supplied should be appliance based, RACK mountable and must be supplied with all related accessories, power cables, mounting kit, console cable etc.
- All the software and licenses required to meet the tender specifications must be provided from day-one
- The SD-WAN Edge server should support atleast 4 WAN ports and 2 USB for 4G & 5G LTE
- Entire solution (AAA, Bandwidth Aggregator, SD-WAN, Security) should be integrated into a single hardware at each location to ensure integrity of system, operating system and confidentiality of management & data plane encryption
- It should be possible to have 1+1 Edge device at critical locations.
- Operating Temperature of hardware shall be 0~50 degree Celsius or better
- Operating relative humidity of the hardware shall be 5%-80% or better
- Input power supply shall be 160~240 V, 100W max

2. 32 Coordination with existing FMS Service provider of KUCB

1 During the project, the Agency shall have coordination and full cooperation with the existing FMS service provider /vendor of KUCB. Since the project infrastructure has to be fully integrated with the KUCB IT Environment, the Implementation agency will require support from existing FMS and vice versa.

2 KUCB shall ensure that existing FMS service provider shall cooperate with the implementation agency and provide all necessary support, configuration settings, access to requisite and necessary IT assets.

3 KUCB/FMS shall provide the raw power to the required location for installing network components. However, it will be bidder's responsibility to connect respective power cable /hardware as per requirement of KUCB environment.

4 Provisioning of power cable (as per KUCB condition) to connect the supplied hardware is under bidder's scope without any extra cost to KUCB.

3.1 Evaluation methodology

1. The objective of this evaluation methodology is to facilitate the selection of one Service Provider (SP) fulfilling selection criteria and providing professional services at optimal cost. The successful bidder/service provider will be playing the role for Implementation of SD-WAN Technology for the period of 5 (3+2) years .

3.2 Evaluation process

3. 3 Objective – evaluation

1. The objective of this evaluation methodology is to facilitate the selection of bidder for implementing and managing SD-WAN at optimal cost.

2. The project is based on SD-WAN implementation cost and Services and the selected bidder has to deliver the goods and services as per scope of the project.

3. 4 Evaluation steps

1. The Bank has adopted a two (2) bid processes in which the Bidder has to submit following bids in separate envelopes at the time of submission of bids as stipulated in this document.
   a) Technical Bid
   b) Commercial Bids

2. The Bank shall evaluate first the 'Minimum Eligibility/ Pre-Qualification Criteria' and based on its evaluation, 'Technical Bids' shall be undertaken for evaluation at the second stage. 'Commercial bids' shall be opened for only the shortlisted bidders out of technical evaluation. The final selection will be done based on **Techno-commercial evaluation**.

3. Evaluation criteria proposed to be adopted will be Quality cum Cost Based System (QCBS) where Technical Bid Score will get a weightage of 70% and Commercial Bid Score a weightage of 30%.

4. The evaluation by the Bank will be undertaken by a Committee of officials or/and representatives formed by the Bank and its decision will be final.

5. Techno –commercial evaluation steps includes DEMO's, POC and TheNegotiations. It involves analysing the technological capabilities and feasibility of a product or service, as well as evaluating its potential economic viability and market opportunities.

6. This involves assessing the technical features, functionalities, and performance of the technology or solution. It includes evaluating factors such as compatibility, scalability, reliability, security, ease of integration, and maintenance requirements. The aim is to determine if the technology meets the desired technical standards and requirements.

7. A techno-commercial evaluation also involves identifying and assessing potential risks and challenges associated with the technology. This includes evaluating factors such as technical risks, market risks, regulatory compliance, intellectual property considerations, and any other potential obstacles that may impact the successful implementation and adoption of the solution.

3. 5 Technical Bid

3.6 Preliminary Examinations

1. The Bank will examine the Bids to determine whether they are complete, the documents have been properly signed, supporting papers/ documents attached and the bids are generally in order.

2. The Bank may, at its sole discretion, waive any minor infirmity, nonconformity or irregularity in a Bid which does not constitute a material deviation, provided such a waiver does not prejudice or affect the relative ranking of any Bidder.

3. Prior to the detailed evaluation, the Bank will determine the substantial responsiveness of each Bid to the Bidding document. For the purpose of this clause, a substantially responsive Bid is one, which conforms to all the essential and mandatory requirements and / or contains reservations with regard to the critical and essential terms and conditions of the Bidding Document without material deviations.

4. Deviations from or objections or reservations to critical provisions, such as those concerning Bid security, performance security, qualification criteria, Force Majeure etc. will be deemed to be a material deviation.

5. If a Bid is not substantially responsive, it will be rejected by the Bank and may not subsequently be made responsive by the Bidder by correction of the nonconformity.

6. The Bidder is expected to examine all instructions, forms, terms and specification in the Bidding Document. Failure to furnish all information required by the Bidding Document or to submit a Bid not substantially responsive to the Bidding Document in every respect will be at the Bidder's risk and may result in the rejection of its Bid.

7 Hardware specifications should be as per the specifications mentioned in this bid. The quantity required may vary by +20% during the course of execution of the project. The unit rate quoted in the financial bid will be used to calculate the price of the varied component.

Hub end gateway appliances at both DC and DR should be in HA (High availability)

Sr. No.	Discription	Unit	Quantity	Make & Model
1	SD-WAN Controller, Manager, orchestrator, Analytics or any other component to be placedat DC & DR	Nos	2	
2	SD-WAN CPE hardware supporting 300 Mbps inclusive of all IO pluggable and power modules withWI-FI Disabled, User/IP authentication, QoS, Firewall (Next Gen) ,WAN Bandwith Aggregation - 4G -5G- LTE, PPPoE, V.35, Static/Dynamic	Nos	34	

Branch List with contacts, existing users and Primary bandwidth

Sr. No	Name of Branch	Branch Address	B/W	Users	Geo Location
1	Head Office	Dhanwardhini, Shriram Shaligram Plot, Near A.K. National Highschool Khamgaon, Tq-Khamgaon Dist-Buldhana, 444303	64 Mbps	85	20.707368, 76.564133
2	M.I.D.C.	Yashwardhini, M.I.D.C. Plot No C-9, Khamgaon, Tq-Khamgaon. Dist-Buldhana, 444303	2 Mbps	5	20.726940, 76.5433670
3	Cotton Market Kmn.	A.P.M.C.Complex, Cotton Market, Akola Road Khamgaon, Tq-Khamgaon Dist-Buldhana, 444303	2 Mbps	9	20.7046660, 76.5734900
4	Mahila	Jalamb Naka, Near Didwani Super Bazar, Nandura Road, Khamgaon,Tq-Khamgaon Dist-Buldhana, 444303	2 Mbps	6	20.7176940, 76.5636770
5	Shegaon	Shnehwardhini, Main road, Near Bus Stand. Shegaon, Tq-Shegaon Dist-Buldhana, 444203	2 Mbps	9	20.796974, 76.694069
6	Pimpal gaon Raja	Main Road, P.H.C. Centre, Near SBI, Pimpalgaon Raja, Tq-Khamgaon Dist-Buldhana, 444306	2 Mbps	4	20.723299, 76.4362390
7	Buldhana	Snehwardhini, Karanja Chowk, Infront of Buldhana Urban Co. Op. Bank, Buldhana, Tq-Dist-Buldhana, 443003	2 Mbps	9	20.536278, 76.1836260
8	Undri	Main Road, Near Bus Stand, Undri, Tq-Chikhali Dist-Buldana, 444307	2 Mbps	5	20.457419, 76.4612960
9	Janefal	C/o Dr Kulkarni's House,near Bus Stand, Janefal, Tq-Mehkar Dist-Buldana, 444304	2 Mbps	4	20.29624182, 76.573816
10	Lonar	Dhar Road, In front of Bus stand, Lonar, Tq-Lonar Dist-Buldana, 443302	2 Mbps	8	19.9867030, 76.5216570
11	Sonala	Main Road, Shivaji Chowk, Sonala, Tq-Sangrampur Dist-Buldana, 444204	2 Mbps	4	21.125030, 76.7407660
12	Warwat Bakal	Near Bus Stand, Sangrampur Road, Warwat Bakal, Tq-Sangrampur Dist-Buldana, 444202	2 Mbps	5	21.0201470, 76.7144460
13	Railway Station Amt.	Ralies Plot Agrawal Complax, Near Sati Dham Temple, Amravati, Tq-Dist-Amravati, 444603	2 Mbps	6	20.928655, 77.7565840
14	Badnera Road Amt.	Badnera Road Nawathe Plot, Near Mansarovar Hotel Amravati, Tq-Dist-Amravati, 444605	2 Mbps	6	20.9075940, 77.7507150
15	Itwara Amravati	Main Road,Laddha Complex, Near Chitra Takies, Amravati, Tq-Dist-Amravati, 444601	2 Mbps	12	20.934121, 77.753104
16	I.T.I. Colony Amt.	Sahakar Complex Kanta Nagar, Near DDR Office, Amravati, Tq-Dist-Amravati, 444602	2 Mbps	5	20.9454076, 77.77998
17	Cotton Market Amt.	New Cotton Market Yard, Cotton Market, Amravati, Tq-Dist-Amravati, 444604	2 Mbps	5	20.9474090, 77.7580090
18	Paratwada	Gujari bazar, Pared Ground, Main Road, Paratwada, Tq-Paratwada Dist-Amravati, 444805	2 Mbps	9	21.3029920, 77.5174780
19	Achalpur	Devdi, Near HDFC Bank ATM, Achalpur, Tq-Achalpur Dist-Amravati, 444806	2 Mbps	8	21.256747, 77.512593
20	Warud	Approch Road, Yavalkar Wadi, Warud, Tq-Warud Dist-Amravati, 444906	2 Mbps	6	21.474636, 78.269781

21	Morshi	Jaistambh Chowk, Morshi, Tq-Morshi Dist-Amravati, 444905	2 Mbps	5	21.3369600, 78.0098520
22	Daryapur	Main Road, Behind Sharma Petrol Pump, Banosa, Daryapur, Tq-Daryapur Dist-Amravati, 444803	2 Mbps	10	20.925624, 77.324414
23	Yeoda	Main Road, Near Dr.Rathi Hospital, Yeoda, Tq-Daryapur Dist-Amravati, 444706	2 Mbps	3	20.9975670, 77.2361120
24	Anjangaon Surji	Antodkar Complex , Daryapur Road , Anjangaon Surji -444705 Dist Amravati.	2 Mbps	6	21.1645420, 77.3171880
25	Dhaman gaon	Vir Bhagat Singh Squre, Near Rly Station, Dhamangaon Rly, Tq-Dhamangaon Rly Dist-Amravati, 444709	2 Mbps	5	20.784503, 78.138759
26	Pathrot	Dr.Kavitkar Complex, Paratwada Road, Pathrot, Tq-Achalpur Dist-Amravati, 444808	2 Mbps	4	21.2159730, 77.3665150
27	Akola	Tilak Road, Opp Uday Takies, Akola, Tq-Dist-Akola, 444005	2 Mbps	7	20.7121370, 76.9962740
28	Nagpur	Plot No 31, Gandhi Grain Market, Near Jaimal Suzuki Showroom, Telephone Exchange Square, Central Ave, Nagpur, Tq-Dist-Nagpur, 440008	64 Mbps	6	21.1485410, 79.1216750
29	Auranga bad	Apana Bazar, Building No.2, Jalna Road, Aurangabad, Tq-Dist-Aurangabad, 431001	2 Mbps	7	19.876120, 75.3471080
30	Jalgaon	Dr. J. J. Pandit Complex, Navi Peth, Near Shamrao Vitthal Co. op. Bank, Jalgaon, Tq-Dist-Jalgaon, 425001	2 Mbps	6	21.012978, 75.5566569
31	Bhusawal	Jamner Road, Behind Ashtabhuja Temple,Kanhaiyalal plot Bhusawal-425201	2 Mbps	6	21.0391970, 75.7802040
32	Burhanpur	Saniwara, Jaistamb Chowk, Burhanpur, Tq-Dist-Burhanpur, 450231	2 Mbps	6	21.312478, 76.229126
33	Ex.Counter Amravati	Bhaji Bazar, Near Vir Wamanrao Highschool, Amravati, Tq-Dist-Amravati, 444601	2 Mbps	3	20.933857, 77.7434050
34	Ex.Counter Buldhana	Jatkar Complex, Sangam Chowk, Near Bus Stand, Buldhana, Tq-Dist-Buldhana, 443003	2 Mbps	2	20.535285, 76.177045
				286	

----------End of RFP----------