



**Institute for Development and Research in
Banking Technology**
(Established by Reserve Bank of India)

Tender No: IDRBT/SYS/VR/240/2022 – 2023 dated 15th December 2022

Request for Proposal (RFP)

For

**Supply, Installation and Maintenance of Perimeter Security Solution and Network Switches at
IDRBT**

**Institute for Development and Research in Banking Technology
IDRBT, Castle Hills,
Road No.1, Masab Tank, Hyderabad – 500057, TS.**

December 2022

NOTE: This document contains 47 pages

This document is the property of Institute for Development and Research in Banking Technology (IDRBT). It may not be copied, distributed or recorded on any medium, electronic or otherwise, without the IDRBT's written permission thereof, except for the purpose of responding to IDRBT for the said purpose. The use of the contents of this document, even by the authorized personnel / agencies for any purpose other than the purpose specified herein, is strictly prohibited and shall amount to copyright violation and thus, shall be punishable under the Indian Law.

Disclaimer

This Request for Proposal (RFP) is not an offer by the IDRBT, but an invitation to receive response from eligible interested bidders for **Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT**. No contractual obligation whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by IDRBT with the successful bidder. This document should be read in its entirety.

Any product name / function used in this document are meant to be generic and do not refer to the product of any particular company. In case such proprietary terms have been inadvertently mentioned then such terms should be taken to refer to the generic technology. Bidders with industry standard equivalent product name / function /feature under any other name will also be eligible to submit response to RFP.

Request for Proposal

IDRBT invites sealed tenders for **Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT**. IDRBT is looking for bidders from reputed companies having previous experience in handling successfully similar projects for Banks/FI/ Insurance companies in India.

1. Introduction

Institute for Development and Research in Banking Technology (IDRBT) is an autonomous body Established by Reserve Bank of India. The primary goal of the Institute is, as follows:

- 1.1. Development & Research on Banking Technology.
- 1.2. The systemic requirements of the banking system
- 1.3. Offer training in banking technologies for Indian Banking sector
- 1.4. Act as a CA (Certifying Authority) for Bankers.

2. Objective of the project

IDRBT has comprehensively employed technology over the years to efficiently discharge its duties in day to day functioning. IT applications are centrally hosted and providing high uptime of the application services on 24x7 basis to Member banks over INFINET & INTERNET network and IDRBT. The main objective of this RFP is to replace the existing perimeter security solution at IDRBT DC and DR locations for protecting entire IT Infrastructure from Cyber threats and vulnerabilities, secure access to IT Applications. The summary of the requirement is as under.

Sno	Description	Qty
1	Technical Specification for Gateway Security Appliance Type I	2+2
2	Technical Specification for Gateway Security Appliance Type II	2
3	Common Technical Specification for Security Gateway Appliance for Type – I & II.	-
4	Technical Specification for Centralized Management Appliance	1
5	Technical Specification for L3 – Network Switch	2+2
6	Technical Specification for L2 – Network Switch	2+1

3. Bid Schedule

Sr.No.	Subject	Date/time
1	RFP Ref. Number & Date	Tender No. IDRBT/SYS/VR/240/2022-2023 dated 15 th December 2022
2	Last Date for receipt of Queries	26 th December 2022

Sr.No.	Subject	Date/time
3	Pre bid meeting	26 th December 2022 (Online)
4	Last date for receipt of Bidding Documents	10 th January 2023
5	Venue / Address for Pre-bid meeting, submission of Bid & Place of opening of Bids	Institute for Development and Research in Banking Technology, Road No. 1, Castle Hills, Masab Tank, Hyderabad – 500057. Phone : 040 – 23294010
6	E-mail address for communication	itprocurement@idrbt.ac.in The participating bidders should mandatorily confirm their participation by email on or before 26 th December 2022 11:00 Hrs for attending to online pre-bid meeting

4. Bid Submission

The Technical and Commercial bids shall be submitted in separate sealed envelopes clearly super scribing on the envelope “**Technical Bid for Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT as per Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022**” and “**Commercial Bid for Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT as per Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022**” on or before 3:30 PM of 10th January 2023..

5. Bidders Eligibility Criteria

Bidders must meet the following eligibility requirements. Bids of non-compliant bidders will not be technically or financially evaluated.

Sr.No	Basic Requirement	Bidders Eligibility Criteria	Documentary evidence required
1	Legal Entity	The Bidder shall provide evidence that it is a current legal entity.	Attested copy of the Certificate of Incorporation/Registration of the Bidder
2	Duration of past experience	The Bidder should have experience in the following fields: Supply, Installation, Maintenance of Perimeter Security Solution for the organizations across India.	The Bidder should submit documentary evidence in support of minimum experience of 3 years (Copies of Purchase Order and Completion certificate to be attached)

Sr.No	Basic Requirement	Bidders Eligibility Criteria	Documentary evidence required
3	Annual Turnover	The OEM / Bidder should have a minimum annual turnover of at least Rs.5 Crores in each of the last three financial years (i.e. 2019-20,2020-2021 & 2021-2022).	Certificate from the statutory auditor
4	Net worth	The Bidder should have positive net worth in the last three financial years (i.e. 2019-20,2020-2021 & 2021-2022).	Certificate from the statutory auditor
5	Technical Capability	<p>Bidder must have successfully completed in the last five years at least the following numbers of similar IT infrastructure Implementation engagement(s) of value specified herein:</p> <ul style="list-style-type: none"> • One project of similar nature not less than the amount Rs.75 Lakhs <p>OR</p> <ul style="list-style-type: none"> • Two projects of similar nature not less than the amount equal Rs.60 Lakhs <p>OR</p> <ul style="list-style-type: none"> • Three projects of similar nature not less than the amount equal Rs.50 Lakhs 	Copies of POs and completion certificate from client
6	General / Legal Status	The company should not be blacklisted by any Government agency / Banks / Other Financial Institutions in India.	Self-declaration on the company letter head signed by Company Secretary or Board approved Authorized Signatory.
7	OEM's Authorization	Bidder should be a OEM Authorized partner/System Integrator/Representative.	Bidder has to provide an Ink Signed MAF for the quoting OEM along with Technical Bid
8	Support	Bidder should have a local entity in Hyderabad to provide better support during the warranty	Documentary proof to be enclosed.

5.2 Details regarding the fulfillment of the eligible criteria should be submitted as per **Annexure IV**.

5.3 The Bidder shall provide references (including Referee names and contact details) in respect of major projects of similar type completed in the last three (3) years.

6. Terms & Conditions

6.1 All bids and supporting documentation shall be submitted in English.

6.2 The cost of bidding and submission of tender documents is entirely the responsibility of

bidders, regardless of the conduct or outcome of the tendering process.

- 6.3 All costs and charges, related to the bid, shall be expressed in Indian Rupees only and the above total cost is inclusive of installation charges and customization charges.
- 6.4 IDRBT will not take into consideration, any variation in the \$ price.
- 6.5 IDRBT reserves right to change the Quantity of the Items and procure complete or part of the equipment/solution quoted by the vendor/OEM.
- 6.6 The Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT should be completed within 10 (Ten) weeks from the date of issue of purchase order.
- 6.7 **The participating bidder's bids will be evaluated Category Wise viz Category A– External Security Gateway Appliance and Category B – L2 & L3 Network Switches. IDRBT may place purchase orders with one or more successful bidders.**
- 6.8 IDRBT reserves the right to reject all or any of the quotations without assigning any reason thereof.
- 6.9 The bidder should work in close association with other vendors/service providers working for IDRBT.

7. Criteria for evaluation

- 7.1 The objective of the evaluation process is to evaluate the bids to select an effective and technically best fit solution at a competitive price. The decision of the IDRBT shall be final.

7.2 Two Stage evaluation process

- i. Bidder has to submit complete bid before the stipulated time given in the RFP document. For the purpose of the evaluation and selection of bidder for this project, a two-stage evaluation process will be as followed:
- ii. **Stage I** - Examination of bidders' eligibility –The IDRBT will evaluate the documents viz. eligibility criteria, Non-Disclosure Agreement (NDA) and other documents submitted along with Technical bid. In the first stage, only the 'Technical Bids' of those who fulfill the **Eligibility Criteria** will be evaluated. Bidders have to submit BoQ without prices and also indicating the compliance to specifications as the technical bid. Those bidders satisfying the technical requirements of **Annexure – IX to XIV** as determined by the IDRBT and as per the requirements / specifications and the terms and conditions of this document, shall be short-listed.
- iii. **Stage II** - Commercial Bids evaluation – In Second Stage, Commercial bids of the technically

qualified vendors will be opened. The commercial bids will be evaluated based on L1 criteria.

The bidder who quote the lowest price shall be considered as L1.

iv. IDRBT will notify the name of the Successful Bidder only.

7.3 Technical Bid

- i. The Technical Specifications of Perimeter Security Solution are to be submitted as per **Annexure – IX to XIV**.
- ii. The bidders are required to submit a Technical Bid indicating the specifications and compliance to the specifications.
- iii. The Bidder must warrant that key project personnel for implementation, should have minimum OEM certified engineers (certified in Networking and Security) on supplied Bill of Material, to be employed in this project and who have been sufficiently involved in similar past installation.
- iv. The Bidder has to submit the list of members of the project team and copies of their certifications.
- v. The Bid is liable to be rejected if any commercial details are found along with the technical bid.

7.4 The Commercial Bid:

- i. The Bidder must organize bids in accordance with the format specified in the RFP - Commercial Bid format at **Annexure XVI**.

8. List of Annexures:

Sno	Formats	Description	Qt	Submission
1	Annexure - I	Document Submission Checklist	-	Mandatory
2	Annexure - II	Bidder's application Form	-	Mandatory
3	Annexure – III	Bidders profile Form	-	Mandatory
4	Annexure – IV	Bidder Eligibility Criteria	-	Mandatory
5	Annexure – V	Bidders Queries Pro-forma	-	Mandatory
6	Annexure – VI	Bidder's Undertaking	-	Mandatory
7	Annexure VII	Manufacturer's Authorization Form (MAF)	-	Mandatory
8	Annexure VIII	Non-Disclosure Agreement	-	Mandatory
9	Annexure IX	Technical Specification for Gateway Security Appliance Type I	4	Mandatory
10	Annexure X	Technical Specification for Gateway Security Appliance Type II	2	Mandatory
11	Annexure XI	Common Technical Specification and Technical bid format for Security Gateway Appliance Type – I & II	-	Mandatory
12	Annexure XII	Technical Specification for Centralized Management Appliance	1	Mandatory
13	Annexure XIII	Technical Specification for L3 – Network Switch	2+	Mandatory

Sno	Formats	Description	Qt	Submission
14	Annexure XIV	Technical Specification for L2 – Network Switch	2+ 1	Mandatory
15	Annexure XV	Format for Deviations from Technical Specifications and Terms and Conditions of the RFP	-	Mandatory
16	Annexure XVI	Commercial Bid Format	-	Mandatory
17	Annexure XVII	Performance Bank Guarantee	-	Mandatory
18	Annexure XVIII	Buy back of old Security Gateway appliance on “as is where” basis)	-	Mandatory

The Bill of Material shall be hosted at IDRBT, Hyderabad and Navi Mumbai.

9. Scope of Work

The minimum specified scope of work to be under taken by the selected bidder is mentioned below:

- 9.1. The “Scope of Work” will include Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT at Hyderabad and Navi Mumbai locations.
- 9.2. The existing applications and IT infrastructure should be integrated with new devices and solution seamlessly.
- 9.3. The bidder should Supply, Install, integrate, test and operationalize the required components as part of the total solution as per technical specification mentioned in **Annexure – IX to XIV** of this RFP with Indicative Bill of Material stated in Annexures, while proposing for a solution.
- 9.4. The Bidder needs to provide complete end to end solution including hardware, software, necessary accessories, active and passive components for efficient functioning of the proposed solution.
- 9.5. The specifications given are minimum. Bidders can quote equivalent or higher technical specifications to meet the requirements of IDRBT. The RFP and annexes together constitute the overall requirements of the solution.
- 9.6. The bidder / System Integrator shall engage the services of respective OEMs for Plan & Design and post implementation audit, validation of the Solution. The System Integrator shall implement the solution as per the plan and design provided by the respective OEMs involved in the solution for their respective components.
- 9.7. Immediate to post deployment the bidder should demonstrate perimeter security solution in the live environment in IDRBT, demonstrate that the Memory and CPU average utilization of the security device doesn't exceed 55% of the total memory and CPU capacity during 30 days in live production environment i.e. after acceptance test to stabilization. In case this requirement is not met, then the OEM and System Integrator must replace the devices with a higher capacity box to meet this requirement without any additional cost implication to IDRBT.

9.8. The OEM and System Integrator must assure that all types of support including warranty, security, upgrade and maintenance support for hardware, software and any other component shall be available throughout the contract period. In case any of the components of the solution is declared end of support by the OEM, the same shall be replaced with an equivalent or higher component without any cost implication to IDRBT. Solution/upgrade for any newly emerged threat/vulnerabilities must be provided without any additional cost to IDRBT.

9.9. The Bidder has to ensure that the solution shall work as desired, and the Bidder is also responsible to supply and install any other components that is inadvertently missed out in BoM of the RFP but required for the overall solution to work. The Bidder must add such items by adding additional line, in the Bill of Material.

9.10. The Bidder shall procure the software license in the name of IDRBT.

9.11. The hardware and software to be supplied are:

9.11.1. Implementation of Perimeter Security Solution and Network Switches

- i. Should rack mount the devices and appliances in the rack identified by IDRBT
- ii. Should install and confirm the devices and appliances with latest and hardened IOS from OEM and create environment as per IDRBT requirements in the devices and appliances.
- iii. Integrate Network and Perimeter Security Solution with servers, applications, LAN and WAN networks (INFINET and INTERNET)
- iv. Should enable communication between the following environments.
 - a. LAN to Servers and Virtual Machines.
 - b. Between Virtual Machines
 - c. Server Virtual Machine to WAN Network - INFINET and INTERNET.
 - d. Virtual Machines in DMZ to Virtual Machines in Trusted Zone.
 - e. Enable security features to restrict access between Virtual Machine.
 - f. Must migrate existing active policies/rules from Security Gateway Appliances of IDRBT to the proposed PSS solution to ensure stability and continuity in policies.

9.12. A Letter of warranty and support from respective Original Equipment Manufacturer's (OEM) shall also be submitted in addition to a letter from respective Manufacturer's Authorization Form for the contract period.

9.13. The OEMs should also provide certificate that all Equipment's offered are not be declared End of Life and End of Support for a minimum of 7 years from the date of acceptance.

9.14. The bidder should fix all the technical problems, provide and implement upgrades, updates free

of cost to IDRBT, as and when released by the OEM during warranty.

9.15. The scope includes the dismantling and removal of all equipment, cables, etc. being replaced at no extra cost.

9.16. The bidder shall address statutory requirements, network and security audit recommendations suggested by IDRBT from time to time on regular basis without additional cost to IDRBT.

9.17. The successful bidder will be required to provide comprehensive warranty for a period of 7 years from the UAT/acceptance of the solution. The bidder at his own cost, including the cost of transport, shall replace defective hardware.

10. Delivery & Installation Period

The following time schedule for completion of the activities from the date of placement of orders should be strictly adhered to. Delay in delivery and installation may invite penalties for the vendors.

Sr.No	Description	Period
a	Delivery	≤ 6 Weeks
b	Installation and Operationalization	≤ 4 Week

11. Warranty

Seven year on-site comprehensive warranty covering all parts & labor from the date of acceptance of the systems by IDRBT. During the warranty period, the successful bidder will have to undertake comprehensive maintenance of the entire hardware, hardware components, systems software and accessories supplied by the vendor.

11.1. Seven years on-site comprehensive warranty should be provided for all devices proposed in this RFP.

11.2. The IDRBT shall promptly notify the successful bidder in writing of any claims arising under this warranty. Upon receipt of such notice, the bidder shall with all reasonable speed, repair or replace the defective products or part thereof without cost to the IDRBT.

12. System maintenance, Support and Preventive maintenance:

The successful bidder should provide free maintenance of the entire BoM proposed in this RFP, during the warranty period by deputing qualified maintenance engineer under the contract.

12.1. The successful bidder shall ensure that faults and failures intimated by IDRBT as above are set right within 24 hours of being informed of the same.

13. Penalty for Delay:

For any delay in installation and commissioning of the equipment beyond the specific period, IDRBT will charge penalty @ 0.5% of the order per week or part thereof, subject to a maximum of 6%. In case, the amount equal to 6% of the order value is deductible as penalty and the vendor is still unable to complete successful Installation, the Institute reserves the right to cancel the order and no payment will be made to the vendor.

14. Penalty for downtime

Any equipment viz (Perimeter Security Solution) that is reported to be down should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within 1 working days. In case vendor fails to meet the above standards of maintenance, there will be a penalty chargeable as specified in the table below.

SI.No	Item	Penalty chargeable per day (Rs)	Response Time
1	Security Gateway	1,000/-	>6 Hrs and ≤ 1 day
	Appliances, L2 & L3	2,000/-	>1 and ≤ 4 days
	Network Switches	5,000/-	≥ 4 days

15. Repeated failure

15.1. During the warranty period if any system as a whole or any subsystem has any failure on two or more occasions in a period of 3 months, it shall be replaced by equivalent new equipment or any alternative steps are to be taken which would serve the purpose to the Institute. Every quarter engineer has to visit and check the Network and Security devices performance or any corrective maintenance or patch updates required for smoother operation and also as and when desired by the institute for technical help or installation help.

15.2. The bidders are required to adhere to tendering norms and no undue explanation, request for change in due date of bid submission, etc. will be offered by the Institute. Any request of any kind from the bidder before the bid submission due date must be forwarded to the undersigned in writing. The Institute reserves the right to accept or reject the bidder request without offering any explanation or reason for the acceptance or rejection. However, in case of any change/amendment in the tender content, all bidders participating in the tendering process would be informed in writing and sufficient time would be provided to adhere to such change/amendment

16. Training

16.1. A Comprehensive training shall be the key to successful Operations and Maintenance; hence, the successful bidder is required to provide training (for three days) to IDRBT nominated Officials at IDRBT, Hyderabad. The training documents, including Operating Manuals, Standard Operating Procedures (SOP) for the proposed solution shall be prepared and shared by the successful bidder with IDRBT. The successful Bidder is free to propose the training plan. However, at a minimum, the plan shall include the following:

Sr No	Training Description
1	Overview of the components Installed
2	Technical Architecture
3	Operating procedure Hardware and Software
4	Technical and Operational Manuals
5	Handling worst case scenarios

16.2. The above plan is only indicative; the final training plan shall be finalized between the successful bidder and IDRBT.

16.3. No separate charges will be paid for training.

17. User Acceptance Test

17.1. IDRBT, prior to the initiation of the Operationalization phase, shall undertake a detailed UAT process.

17.2. The User acceptance test will be carried out as per mutually agreed Acceptance Test Plan (ATP) against the systems requirements.

17.3. The system will be considered accepted (supplied, installed and operationalized) only after ATP is completed as per the agreed plan and is duly signed/certified by the IDRBT and the successful bidder.

18. Period of Validity

All the prices and other terms and conditions of the offer proposed by the bidder should be **Valid** for a **minimum** period of **Six months**.

19. Correction of Errors

Arithmetic errors in bids will be treated as follows:

19.1. Where there is a discrepancy between the amounts in figures and in words, the amount in

words shall govern.

19.2. Where there is a discrepancy between the unit rate and the line item total resulting from multiplying the unit rate by the quantity, the unit rate will govern unless, in the opinion of IDRBT, there is obviously a gross error such as misplacement of a decimal point, in which case the line item total will govern.

19.3. Where there is a discrepancy between the amount mentioned in the bid and the line item total present in the Bill of Quantity, the amount obtained on totaling the line items in the Bill of Materials will govern.

19.4. The amount stated in the tender form, adjusted in accordance with the above procedure, shall be considered as binding, unless it causes the overall tender price to rise, in which case the bid price shall govern.

20. Confidentiality

Bidder agrees that all mails, data, financial, mail, security architecture and personnel data relating to IDRBT's business and other information identified as confidential by IDRBT, the same shall be kept confidential and shall not be shared with any third party without prior written approval from IDRBT.

21. Right to Verification

The IDRBT reserves the right to verify any or all statements made by the bidder in the tender documents and to inspect the bidder's facility, if necessary, to establish to its satisfaction about the bidder's capacity to perform the job.

22. Insurance

22.1. Insurance for all the hardware components supplied under the contract shall be arranged by the Bidder at his own risk and cost throughout the period of delivery, implementation and final acceptance process.

22.2. IDRBT will not be responsible for any loss/damage/theft of any systems/goods due to any reasons whatsoever, claims etc., if the Bidder himself will deal any. Evidence of the insurance policy shall be submitted to IDRBT.

23. Payment Terms:

23.1. Hardware items: A payment of 90 percent (90%) of the contracted sum would be payable on successful installation, integration and issue of acceptance certificate by the Institute.

23.2. 10 percent (10%), would be payable after successful warranty period is over from the date of acceptance or payable against PBG valid for 7 years.

23.3. All payments will be released based on the invoices submitted to Institute by the vendor.

24. Obligations of Successful Bidder

24.1. The successful bidder has to supply all the components, services and licenses to make solution complete and operational.

24.2. The successful bidder shall handover the complete and operational solution to IDRBT for monitoring, maintenance and management.

24.3. The successful bidder shall deploy their own computing resources, trained and experienced engineers for implementing, managing and maintaining the system.

24.4. Whenever any new threats / vulnerabilities become public, the successful bidder shall bring this to the notice of IDRBT immediately and help/guide IDRBT in plugging the same. Once the call has been attended, successful bidder engineers shall put their maximum efforts and deploy their best resources to resolve all calls at the earliest possible time frame at both locations and ensure appropriate uptime.

24.5. The successful bidder to ensure that during the implementation, the critical services hosted at IDRBT, Hyderabad shall not face any downtime due to improper configuration.

25. Order Cancellation:

IDRBT reserves its right to cancel the order in the event of delay in delivery and installation beyond the stipulated time.

26. Resolution of Disputes

IDRBT and the bidder shall make every effort to resolve amicably, by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the contract. If after thirty days from the commencement of such informal negotiations, IDRBT and the bidder have been unable to resolve amicably a contract dispute, either party may require that the dispute be referred for resolution by formal arbitration.

27. Indemnification

27.1. The bidder/ successful bidder at its own cost and expenses defend and indemnify the Institute against all third-party claims including those of the infringement of Intellectual Property

Rights, including patent, trademark, copyright, trade secret or industrial design rights, arising from use of the Products or any part thereof in India.

- 27.2. The bidder shall expeditiously meet any such claims and shall have full rights to defend itself there from. If the Institute is required to pay compensation to a third party resulting from such infringement, the bidder shall be fully responsible therefore, including all expenses and court and legal fees.
- 27.3. The Institute will give notice to the Bidder of any such claim and shall provide reasonable assistance to the bidder disposing of the claim.
- 27.4. The bidder shall also be liable to indemnify the Institute, at its own cost and expenses, against all losses/damages, which the Institute may suffer on account of violation by the bidder/successful bidder of any or all national/international trade laws, norms, standards, procedures, etc.

28. Liquidated Damages

The liquidated damages is an estimate of the loss or damage that the Institute may have suffered due to delay in performance or non-performance of any or all the obligations (under the terms and conditions of the purchase contract relating to supply, installation, operationalisation, implementation, training, support/services, acceptance, maintenance, etc., by the bidder/successful bidder and the bidder/successful bidder shall be liable to pay the Institute a fixed amount for each day of delay / non-performance of the obligations by way of liquidated damages, details of which will be specified in the RFP. Without any prejudice to the Institute's other rights under the law, the Institute shall recover the liquidated damages, if any, accruing to the Institute, as above, from any amount payable to the Bidder either as per the RFP, executed between the parties or under any other purchase agreement / contract, the Institute may have executed / shall be executing with the bidder/successful bidder.

29. Force Majeure

The bidder/successful bidder or the Institute shall not be responsible for delays or non-performance of any or all contractual obligations, caused by war, revolution, insurrection, civil commotion, riots, mobilizations, strikes, blockade, acts of God, Plague or other epidemics, fire, flood, obstructions of gation by ice of Port of dispatch, acts of government or public enemy or any other event beyond the control of either party, which directly, materially and adversely affect the

performance of any or all such contractual obligations.

If a Force Majeure situation arises, the bidder/successful bidder shall promptly notify the Institute in writing of such conditions and any change thereof. Unless otherwise directed by the Organization in writing, the bidder/successful bidder shall continue to perform his obligations under the contract as far as possible, and shall seek all means for performance of all other obligations, not prevented by the Force Majeure event.

30. Jurisdiction

The jurisdiction of the courts shall be Hyderabad.

For any questions/clarifications mail us at itprocurement@idrbit.ac.in

Document Submission Checklist

The bidder has to ensure that the following have been submitted as a part of the RFP submission process. Failure to provide any of the documents as detailed below could lead to the disqualification of the bidder from the bid.

The following documents/items need to be submitted:

Sr.No	Description	Submitted (Bidder)	Verified (IDRBT)
1	Bidder's application Form	<input type="checkbox"/>	<input type="checkbox"/>
2	Bidders profile Form	<input type="checkbox"/>	<input type="checkbox"/>
3	Bidders Eligibility Format	<input type="checkbox"/>	<input type="checkbox"/>
4	Technical Bid Forms - BILL OF MATERIAL WITHOUT PRICES	<input type="checkbox"/>	<input type="checkbox"/>
5	Deviations from Technical Specifications and Terms and Conditions of the RFP	<input type="checkbox"/>	<input type="checkbox"/>
6	Bidders Queries Pro-forma	<input type="checkbox"/>	<input type="checkbox"/>
7	Bidder's Undertaking	<input type="checkbox"/>	<input type="checkbox"/>
8	Manufacturers' Authorization Form	<input type="checkbox"/>	<input type="checkbox"/>
9	Non-Disclosure Agreement	<input type="checkbox"/>	<input type="checkbox"/>
10	Commercial Bid	<input type="checkbox"/>	<input type="checkbox"/>
11	Performance Bank Guarantee	<input type="checkbox"/>	<input type="checkbox"/>

Bidder's application Form

[On the Letterhead of the Applicant]

Place:

Date:

To,

The Director,
Institute for Development and
Research in Banking Technology,
Road No. 1, Castle Hills, Masab Tank,
Hyderabad 500057

Dear Sir,

Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022

Request for Proposal (RFP) for Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT

Being duly authorized to represent and act on behalf of (hereinafter referred to as "the Applicant"), and having reviewed and fully understood all of the qualification requirements and information provided, the undersigned hereby apply **Request for Proposal (RFP) for Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT.** The details as per the requirements of the RFP enquiry are enclosed for your consideration.

Yours faithfully,

(Signature of Authorized Signatory)
<NAME, TITLE AND ADDRESS>

FOR AND ON BEHALF OF
<NAME OF THE APPLICANT ORGANISATION>

Bidders profile Form

Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022

BIDDER DETAILS	
1	The registered name of the bidding company
2	Business address for correspondence
	Location
	Street
	Locality
	City
	Pin Code
	Country
	Telephone
	Facsimile
	Email
Other	
3	Name of the Bidder's Contact Person
4	Contact's position with Bidder
5	Contact addresses if different from above
	Location
	Street
	Locality
	City
	Pin Code
	Country
	Telephone
	Facsimile
	Email
Other	
6	Business structure
7	Bid Company's registered address
8	Details of company registration
9	Names of Directors
10	Include a structure chart reflecting the organization
	Experience in Similar Projects: (Give details with respect to Perimeter Security Solution and Network devices – a minimum of two projects.)

11	Project Name:		
12	Project Location:		
13	Client Name:		
14	Client address:		
15	Client contact/reference person(s):	Name	
		Address – if different from above	
		Telephone Facsimile	
		Mobile Phone	
		Email address	
16	Project started (month/year):		
17	Project elapsed time – months- vis-à-vis Project schedule:		
19	Name of senior project staff:		
		Project Director	
		Project Manager	
	Other		
20	Nature of the Project:		

Bidder Eligibility Criteria

Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022

Sno	Basic Requirement	Bidders Eligibility Criteria	Documentary evidence required	Compliance (Y/N)
1	Legal Entity	The Bidder shall provide evidence that it is a current legal entity.	Attested copy of the Certificate of Incorporation/Registration of the Bidder	
2	Duration of past experience	The Bidder should have experience in the following fields: Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches for the organizations across India.	The Bidder should submit documentary evidence in support of minimum experience of 3 years (Copies of Purchase Order and Completion certificate to be attached)	
3	Annual Turnover	The OEM / Bidder should have a minimum annual turnover of at least Rs.5 Crores in each of the last three financial years (i.e. 2019-20,2020-2021 & 2021-2022).	Certificate from the statutory auditor	
4	Net worth	The Bidder should have positive net worth in the last three financial years (i.e. 2019-20,2020-2021 & 2021-2022).	Certificate from the statutory auditor	
5	Technical Capability	<p>Bidder must have successfully completed in the last five years at least the following numbers of similar IT infrastructure Implementation engagement(s) of value specified herein:</p> <ul style="list-style-type: none"> • One project of similar nature not less than the amount Rs.75 Lakhs <p>OR</p> <ul style="list-style-type: none"> • Two projects of similar nature not less than the amount equal Rs.60 Lakhs <p>OR</p> <ul style="list-style-type: none"> • Three projects of similar nature not less than the amount equal Rs.50 Lakhs 	Copies of POs and completion certificate from client	

Sno	Basic Requirement	Bidders Eligibility Criteria	Documentary evidence required	Compliance (Y/N)
6	General / Legal Status	The company should not be blacklisted by any Government agency / Banks / Other Financial Institutions in India.	Self-declaration on the company letter head signed by Company Secretary or Board approved Authorized Signatory.	
7	OEM's Authorization	Bidder should be a OEM Authorized partner/System Integrator/Representative.	Bidder has to provide an Ink Signed MAF for the quoting OEM along with Technical Bid	
8	Support	Bidder should have a local entity in Hyderabad to provide better support during the warranty	Documentary proof to be enclosed.	

**Bidder's Undertaking
(On letterhead of the Bidder)**

Date:

To,

The Director,
Institute for Development and
Research in Banking Technology,
Road No. 1, Castle Hills, Masab Tank,
Hyderabad 500057

Dear Sir,

Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022.

We, the undersigned, as bidder, having examined the complete RFP for **Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT** in full conformity of your requirements as elaborated in above said RFP for the amounts mentioned by us in the Commercial Bid or such other sums as may be agreed to between us.

We hereby agree to all the terms and conditions stipulated in the RFP except for the variations and deviations of requirements as mentioned by us in the Compliance Statement, submitted along with our Technical Proposal.

We agree to abide by our Offer for a period of **180 days** from the date of last day of Bid submission and it shall remain binding on us for acceptance at any time before the expiration of this period.

We understand that you are not bound to accept the lowest or any bid you may receive.

We undertake, if our Bid is accepted, to provide Performance Bank Guarantee as per the prescribed format within the times stipulated in the RFP.

We undertake as a part of this contract for successful operation of the **Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT** during the warranty period (if contracted).

Yours faithfully,

(Authorized Signatory)

In the capacity of _____

Duly authorized to sign the Bid for and on behalf of _____

Manufacturer's Authorisation Form (MAF)

Tender No. _____ Dated _____

To

Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022 for Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT

We _____ who are established and reputable manufactures of _____ having offices at _____ and _____ do hereby authorize

M/s _____ (Name and address of Agent /Dealer) to offer their quotation, negotiate and conclude the contract with you against the above invitation for tender offer.

We hereby extend our full guarantee and warranty as per the terms and conditions of the tender and the contract for the equipment and services offered against this invitation for tender offer by the above firm.

Yours faithfully,

(Name) for and on behalf of M/s _____ (Name of manufacturers)

Note: This letter of authority should be on the letterhead of the manufacturing concern and should be signed by a competent person of the manufacturer.

Non - Disclosure Agreement (On ₹ 100 stamp paper)

Date:

To,

The Director,
Institute for Development and
Research in Banking Technology,
Road No. 1, Castle Hills, Masab Tank,
Hyderabad 500057

[Salutation]

Confidentiality Undertaking

We acknowledge that during the course of bidding for Request for Proposal (RFP) floated for **Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022 for Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT.** we may have access to and be entrusted with Confidential Information. In this letter, the phrase "Confidential Information" shall mean information (whether of a commercial, technical, scientific, operational, administrative, financial, marketing, business, or intellectual property nature or otherwise), whether oral or written, relating to IDRBT and its business that is provided to us pursuant this Agreement. In consideration of you making Confidential Information available to us, we agree to the terms set out below:

1. We shall treat all Confidential Information as strictly private and confidential and take all steps necessary (including but not limited to those required by this Agreement) to preserve such confidentiality.
2. We shall use the Confidential Information solely for the preparation of our response to the RFP and not for any other purpose.
3. We shall not disclose any Confidential Information to any other person or firm, other than as permitted by item 5 below.
4. We shall not disclose or divulge any of the Confidential Information to any other client of [name of product vendor / implementation partner]
5. This Agreement shall not prohibit disclosure of Confidential Information:
 - To our partners/directors and employees who need to know such Confidential Information to assist with the bidding for RFP floated for **Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT**
 - With your prior written consent, such consent not to be unreasonably withheld;
 - To the extent that such disclosure is required by law;
 - To the extent that such disclosure is required by any rule or requirement of any regulatory authority with which we are bound to comply; and
 - To our professional advisers for the purposes of our seeking advice. Such professional advisers will be informed of the need to keep the information confidential.
6. Upon your request we shall arrange delivery to you of all Confidential Information, and copies thereof, that is in documentary or other tangible form, except:

-
- For the purpose of a disclosure permitted by item 5 above; and
 - To the extent that we reasonably require to retain sufficient documentation that is necessary to support any advice, reports, or opinions that we may provide.
7. This Agreement shall not apply to Confidential Information that:
 - Is in the public domain at the time it is acquired by us; Enters the public domain after that, otherwise than as a result of unauthorized disclosure by us;
 - Is already in our possession prior to its disclosure to us; and
 - Is independently developed by us.
 8. This Agreement shall continue perpetually unless and to the extent that you may release it in writing.
 9. We acknowledge that the Confidential Information will not form the basis of any contract between you and us
 10. We warrant that we are acting as principal in this matter and not as agent or broker for any person, company, or firm.
 11. We acknowledge that no failure or delay by you in exercising any right, power or privilege under this Agreement shall operate as a waiver thereof nor shall any single or partial exercise thereof or the exercise of any other right, power, or privilege.
 12. This Agreement shall be governed by and construed in accordance with Indian law and any dispute arising from it shall be subject to the exclusive jurisdiction of the Mumbai courts.

We have read this Agreement fully and confirm our agreement with its terms

Yours sincerely

Signature and Stamp of Company

[Authorized Signatory (same as signing the proposal) – Implementation
Partner] Name:

Position :

Date :

Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022**Technical Specification and Technical bid format for Security Gateway Appliance Type - I**

Sr.No	Parameters	Technical Specifications of Type I Security Appliances	Compliance Y/N	Comments/ Supporting Documents
1	Product Details	Bidder to mention Make, Model No. and Part Code of the appliance		
2	Qty	2+2		
3	Hardware	The proposed security gateway solution should be appliance based.		
4	Form Factor	1U/2U – Rack mountable		
5	Concurrent TCP/HTTP Connection Capacity	2 Millions		
6	TCP/HTTP Connections Per Second	Connections per second should be minimum of 40000 or more		
7	HTTP Throughput	2 Gbps		
8	CPU & IOS	The appliance hardware should have multi-core CPU with a hardened 64 bit IOS to support higher memory.		
9	Memory	The firewall must have a minimum of 16GB memory upgradable to 32GB.		
10	Storage	The storage provided in the security gateway appliance must be Flash/SSD type storage with local in-build storage.		
11	Network Ports	The security gateway appliance should have maximum capacity of 8 X 1G and 4 x 10G ports (Copper)		
12	Dedicated Additional Port	The security gateway appliance should have High availability, Sync & Management ports. (As part of maximum no of available ports)		
13	USB Ports	2x USB 3.0 ports		
14	Power Supply	The proposed security gateway appliance should have dual Redundant and Hot swappable power supply and Redundant Hot swappable fan for high availability of hardware.		

Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022

Technical Specification and Technical bid format for Security Gateway Appliance Type - II

Sr.No	Parameters	Technical Specifications of Type II Security Appliances	Compliance Y/N	Comments/ Supporting Documents
1	Product Details	Bidder to mention Make, Model No. and Part Code of the appliance		
2	Qty	2		
3	Hardware	The proposed security gateway solution should be appliance based.		
4	Form Factor	1U/2U – Rack mountable		
5	Concurrent TCP/HTTP Connection Capacity	25000 or more		
6	TCP/HTTP Connections Per Second	Connections per second should be minimum of 15,000 or more		
7	HTTP Throughput	750 Mbps		
8	CPU & IOS	The appliance hardware should have multi-core CPU with a hardened 64 bit IOS to support higher memory.		
9	Memory	The firewall must have a minimum of 8GB memory upgradable to 16GB.		
10	Storage	The storage provided in the security gateway appliance must be Flash/SSD type storage with local in-build storage.		
11	Network Ports	The security gateway appliance should have maximum capacity of 8 X 1G and 4 x 10G ports (Copper)		
12	Dedicated Additional Port	The security gateway appliance should have High availability, Sync & Management ports. (As part of maximum no of available ports)		
13	USB Ports	2x USB 3.0 ports		
	Power Supply	The proposed security gateway appliance should dual redundant power supply for high availability of hardware.		

Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022**Common Technical Specification and Technical bid format for Security Gateway Appliance Type – I & II**

Sr.No	Technical Specifications of Type I & II Security Gateway Appliances	Compliance Y/N	Comments/ Supporting Documents
A	Common Features of Security Gateway Appliances		
1	The Security Gateway Appliance OEM should be in leaders Quadrant in latest Gartner Magic Quadrant Report for Enterprise Firewalls for atleast 5 years		
2	The Security Gateway Appliance OEM should be ICSA labs certified for firewall.		
3	The OEM should be having recommended rating from NSS labs next generation Security Gateway Appliance from past 2 years.		
4	The proposed Security Gateway Appliance IOS should be IPv6 Phase II ready and certified. The proposed solution must support Configuration of dual stack gateway on a bond interface, OR on a sub-interface of a bond interface		
5	The solution must support NAT66, NAT64 and NAT46		
6	The solution shall support all types of IPv6 R's.		
7	The Security Gateway Appliance should support "Stateful" policy inspection. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc., capabilities in a single appliance from day one.		
8	The above-mentioned technical parameters for the proposed Security Gateway Appliance model needs to be validated by the OEM on their letter head & signed by authorised signatory.(The test methodology and result should be compliant to the benchmark testing methodology).		
9	The test report which is attested by the authorised signatory of the OEM shall be submitted as a supporting document for compliance to this requirement.		
10	The proposed OEM product should hardened and not having any critical vulnerabilities, backdoor entries, not been compromised by external cyber security threats reported in the product IOS in last two years.		
B	The following are the general technical features must be available and enabled from day of the Security Gateway Appliances mentioned below:		
1	SSL inspection-must be supported for 10% of the total throughput/traffic. The next generation Security Gateway Appliance must provide SSL inspection feature for specific or selective traffic based on source/destination IP & application, SSL Inspection (Inbound/Outbound), HTTPS Inspection, HTTP/2,TLS Inspection and Advanced routing facilities.		
2	IDS & IPS		
3	Anti-Spyware		
4	Anti-Botnet		

Sr.No	Technical Specifications of Type I & II Security Gateway Appliances	Compliance Y/N	Comments/ Supporting Documents
5	Anti-malware		
6	Monitoring, Event logging & reporting		
7	Application Identification		
8	Packet capture utility with support for IPV4 & IPV6		
9	QoS Marking		
10	Policy based forwarding		
11	User Identity Acquisition		
12	Application Control and URL filtering		
13	Threat Emulation (Sandboxing)		
14	Threat Extraction (Scrubbing)		
15	HTTPS Inspection		
16	Identity Awareness		
17	IPSec VPN		
18	Mobile Access		
19	Security Policy Management		
20	Logging and Status		
21	Event Correlation and Reporting		
22	Networking & Clustering		
23	Virtual Systems		
24	The proposed solution must provide a mechanism to constantly educate end users of the security policy in real time.		
25	The proposed solution must have the capability to provide a solution to mitigate Distributed Denial of Service attacks.		
26	The proposed security gateway appliance must use Stateful Inspection based on granular analysis, communication and application state to track and control the network flow.		
27	The proposed solution must support access control for at least 150 predefined /services/protocols		
28	Firewall should support IPSec NAT traversal.		
29	Secure communications between site-to-site and remote users with IPSec & SSL VPN.		
30	Should provide NAT functionality including PAT. Should support NAT 66,NAT 64,DNS 64,Static NAT IPv4 to IPv6 and vice versa,IPv6-IPv4 tunnelling or dual stack.		
31	Should support IPv4 & IPv6 policies.		
32	It should support the IPSec VPN for both site-site and remote access VPN.		
33	Antivirus, Anti-bot, IPS, App Control, URL Filtering, SSL VPN, etc., licenses to be provided as a bundle along with the Firewall appliance.		
34	Following latest protocols must be supported--IPSec/GRE,DES,3DES,AES(128,192,256),MD5,SHA-1,SHA-2,Diffie-Hellman Groups, IKE v1,v2 algorithms.		
35	FTP,HTTP,HTTPS,SNMP,SMTP,DHCP,DNS.		
36	The firewall should support transparent(Layer 2) firewall or routed (Layer 3) firewall Operation.		

Sr.No	Technical Specifications of Type I & II Security Gateway Appliances	Compliance Y/N	Comments/ Supporting Documents
37	Firewall should support minimum VLANS 1024.		
38	Firewall should support static NAT, Policy based NAT and PAT		
39	Solution must block threats/malwares in real-time & should not allow any zero day threat/vulnerability in network		
40	The gateway security appliance should acquire User Identities from AD/LDAP, Server Health Monitoring system, client probing, etc., and should have ability to identity/isolate rouge machines in the networks by Integrating with existing AD solution.		
41	Dynamic/Retrospective Analysis in network to observe files and assess the current status of the threat as they execute in a purpose-built, evasion-resistant virtual environment , enabling detection of previous unknown malware using behavioural characteristics.		
42	The gateway security appliance should block the traffic based on geo location (country wise).		
43	The geo location based configuration should be supported granularly for per policy and per application wise as per the business requirement		
44	The gateway security appliance solution architecture should have Control Plane separated from the Data Plane whereby Control Plane should handle Management functions and Data Plane should handle security processing and network processing functions		
C	IoT Security		
1	Collect IoT devices and traffic attributes from certified IoT discovery engines.		
2	Configure a new IoT dedicated Policy Layer in policy management.		
3	Configure and manage security rules that are based on the IoT devices' attributes.		
4	The gateway security appliance should support Authentication with the following features and not limited to :		
5	Should support User-Group based authentication(Identity based Firewalling) & Scheduling.		
6	Should support authentication servers- RADIUS,LDAP and Active Directory		
7	Support for RSA Secure ID or other Token based products.		
8	The gateway security appliance should support Application Control with the following features and not limited to :		
9	Web site access control with application control. Must Identify ,allow, block or limit the use of thousands of applications, including Web 2.0 and social networking, regardless of port, protocol or evasive technique used to traverse the network.		
10	Should have application control features for 5000 or more applications.		
11	Should perform traffic shaping of popularP2P applications.		
12	Should control popular IM/P2P applications regardless of port/protocols.		
13	The solution should provide the protection from zero day attacks, known & unknown attacks.		
14	The proposed solution shall support DNS proxy.		

Sr.No	Technical Specifications of Type I & II Security Gateway Appliances	Compliance Y/N	Comments/ Supporting Documents
15	The proposed appliance should have rich security management features for managing, monitoring and maintenance of the appliance.		
D	The gateway security appliance solution should provide QoS Marking and Policy based Forwarding with the following and not limited to :		
1	QoS Marking		
i.	by source address		
ii.	by destination address		
iii.	by application (such as Webex, Social Media)		
iv.	By static or dynamic application groups (such as Instant Messaging or P2P groups)		
v.	by port		
vi.	by services		
2	Policy based Forwarding		
i.	Based on Zone		
ii.	Source or Destination Address		
iii.	Source or destination port		
iv.	Application (not port based)		
v.	AD/LDAP user or User Group		
vi.	Services		
E	The internet link load balancing & Auto Failover should support technical features and not limited to the following:		
1	The security appliance should support balanced round robin-equal load on the INTERNET links and weighted round robin- differential loads on INTERNET links based on weights.		
2	ii. Network Path Monitoring: The gateway security appliance should have the feature of Network Path Monitoring. i.e track the health & availability of entire path including Internet Router LAN Port, WAN Port, ISP Next Hop Router IP, ISP Cloud Service & Internet Service. In case of any component failure, gateway security appliance should detect it immediately & provide complete information about which component has failed along the path such as Internet Router WAN port OR ISP service etc.,		
3	The gateway security appliance should support Symmetric Return to cause return packets to egress out the same interface on which the associated ingress packets arrived.		
4	The gateway security appliance solution must provide for load balancing and Auto Failover of minimum four (4) internet links. The load balancing and automatic failover must be seamless and automatic without manual Intervention.		
F	High Availability Configuration		
1	The gateway security appliance must be deployed in High Availability pairs in active -Passive configuration and must support high availability for both IPV4 & IPV6 traffic. The failover between the HA pairs must be seamless and automatic without requirement for manual intervention.		

Sr.No	Technical Specifications of Type I & II Security Gateway Appliances	Compliance Y/N	Comments/ Supporting Documents
G	Migration of Policies or rules & Integration with LAN/WAN Network		
1	The system integrator should plan Migration existing policies to new solution and Integration with IDRBT network and other devices with minimum downtime.		
2	The solution must provide seamless approach to migrate existing L3/L4 policies to L7 Application based policies without any disruption. The solution must integrate with the existing security and monitoring solutions in IDRBT.		
H	The features of proposed Sandbox need to handle all the Security appliances, not limited to the following:		
1	Sandbox to provide on - premise threat analysis -environment, detonation , and automated orchestration of prevention for highly evasive zero-day exploits and malware.		
2	Mitre-ATT&CK based reporting to provide malware tactics and techniques		
3	Payload analysis-		
4	* Classification of custom-malware, unknown, targeted and advanced threats. Creates signatures for use by IPS.		
5	Sniffer mode, API or integrated.		
6	The proposed solution should provide zero day exploit protection and detection for file analysis to Prevent multi-stage, multi-hop attacks.		
7	Type of Files to be handled		
8	* Productivity (Word, Excel, PDF etc.,)		
9	* Archives (.rar, .zip, .tar.gz, .cab etc.,)		
10	* Executables (.exe, .dll, .msi etc.,)		
11	* Media (.avi, mpeg, .mp3, .mp4 etc.,)		
12	Protocols		
13	* HTTP, FTP, POP3, IMAP, SMTP, SMB, IM etc.,		
14	* SSL equivalent versions		
15	7-year onsite warranty should carry direct warranty from OEM 24X7 call logging with 6 hours call to resolution cycle) and the same should be substantiated by necessary supporting document.		

Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022**Technical Specification and Technical bid format for Central Management Appliance for Monitoring Security Gateway Appliance Type I & II**

Sr.No	Technical Specifications of Central Management Appliance for Monitoring Type I & II Security Gateway Appliances	Compliance Y/N	Comments/ Supporting Documents
A	The Central Management console must have the following features from day one:		
i.	The security gateway appliance must provide a common central management console for all security gateways (firewalls).		
ii.	The Central Management Appliance must support 3TB Storage from day 1		
iii.	The OEM must provide 1 Central Management Appliance at DC capable to manage all its Security Gateway Appliances deployed at DC and DR locations.		
iv	The management solution should provide customisable Management Dashboard to provide quick insight about i) Applications , ii) Users , iii) Files, iv) Top Rule Usage, v) Content, vi) Threat classification/category		
v	It should indicate automatically where improvements in the firewall policies are required based on ongoing continuous assessment.		
vi	It should support deployment of versions/ patches/fixes on managed devices directly from the central management console.		
v	Risk Analysis of Firewall Rules should be based on Zone to Zone, Subnet to Subnet or IP to IP etc.		
B	Security Rules optimisation:		
i.	Unused Rules Calculation for specific time period based on Firewall Traffic Logs		
ii.	Analysis on Covered/Shadow/Hidden Rules		
iii.	Analysis on Rules Consolidation (Merging of similar kind of rules)		
iv.	Analysis on Redundant Rules		
v.	Tightening of Overly Permissive Rules (Any-Any)		
vi.	Analysis on Unattached/Unused Objects to simplify objects management		
vii	Analysis on Rule-Reordering to improve the performance of the Firewall		
viii	Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets.		
C	Integrate with existing Vulnerability Assessment tool to correlate Firewall Risky Rules & Vulnerability data to assess the attack surface		

Sr.No	Technical Specifications of Central Management Appliance for Monitoring Type I & II Security Gateway Appliances	Compliance Y/N	Comments/ Supporting Documents
D	Should support Security Management features		
E	Should support Logging & Monitoring features		
F	Should support Event Correlation and Reporting features		
G	View of Events and reports		
1	Export logs filtered according to field values.		
2	Generate SIEM compatible Threat Emulation and Forensics reports		
H	Reporting consolidated information		
1	The volume of connections that were blocked by security rule.		
2	Top sources of blocked connections, their destinations and services		
3	Top Rules used by the security policy		
4	Top security attacks detected by enforcement point (perimeter) determining their the top sources and destinations		
5	Number of installed and uninstalled policies in the enforcement point		
6	Top networking services		
7	Web activity by user detailing the top visited sites and top web users		
8	Top services that created most load for encrypted traffic		
9	Top VPN users performing the longest duration connections		
10	Centralised Management should be quoted with TAC Support and Warranty for 7 years with NBD Hardware Replacement.		
11	Printed technical catalogs /brochures/ User manual / Release notes for the quoted model containing technical specifications, features along with bid.		

Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022**Technical Specification and Technical bid format for Layer 3 Network Switch**

Sl. No	Specification Required	Compliance Yes / No	Remarks
1	Product details		
1.1	Bidder to mention Make, Model No. and Part Code		
1.2	Qty – 2+2		
2	Port Details and Features		
2.1	The Switch should offer Wire-Speed Non-Blocking Switching & Routing Performance at Layer 2 & Layer 3.		
2.2	The Switch should have Twenty Four (24x10GBASE-T) and 4x 10 Gbe populated with SFP+ Fibre Connectivity for uplinks from day one.		
2.3	Switch must support buffer of 10MB or more		
2.4	Must support dual internal, redundant power supplies that are hot-swappable.		
2.5	The Switch should support Active-Active or equivalent Switch Clustering feature.		
3	Performance		
3.1	Switching Bandwidth: Non-Blocking switch fabric capacity of 250 Gbps or more.		
3.2	Forwarding Capacity: wire-speed packet forwarding of 200 Mpps or more.		
4	Layer 2 features		
4.1	Should support 4K active VLANs, 160K MAC addresses or more, IP multicast snooping		
4.2	Should support Jumbo Frames (up to 9K bytes)		
5	Layer 3 features		
5.1	Should support minimum 10K IPv4 routes or more and 4K IPv6 routes or more		
5.2	Should support IPv4 and IPv6 Static Routing, ECMP, Virtual Interfaces, Routed Interfaces from day 1.		
5.3	Should support Dynamic IPv4 Routing protocols and features like VRRP v2/v3 , OSPFv2/v3, BGPv4 , VRF Lite and Multi-VRF, Graceful restart, Proxy ARP etc., or equivalent.		
5.4	Should support IPv6 Routing protocols and features like ICMPv6, BFD, RA Guard, Stateless auto config ,BGP, OSPF, IPv6 Neighbor Discovery , etc.,		
6	Security		
6.1	Switch should support RADIUS, TACACS/TACACS+ and username/password for Authentication, Authorization and Accounting (AAA)		
6.1a	Port-based Network Access Control 802.1X		

Sl. No	Specification Required	Compliance Yes / No	Remarks
6.1b	Port Security, Control Plane Policing (CPP) ,TLS, SFTP		
6.2	Should support secure communications to the management interface and system through SSL, Secure Shell (SSHv2), Secure Copy and SNMPv3		
6.3	Should support IPv4 and IPv6 ACLs with minimum of 2K rules per system		
6.4	Should support Byte and packet based broadcast, multicast, and unknown-unicast limits with suppression port dampening.		
6.5	Should support Flexible Authentication with 802.1x Authentication and MAC Authentication.		
7	Manageability		
7.1	Should support manageability using Network Management Software tools using SNMP		
7.1a	Solution should provide ecosystem integration with VMWARE, Hyper-V, Openstack etc.		
7.1b	Solution should support performance management and analytics capability for applications such as Wireshark, Perfsonar, Docker, TCP Dump, etc with On box functionality or External Server to be supplied by OEM.		
7.1c	Integrated Standard based Command Line Interface (CLI),		
7.2	Should support Monitoring of critical network parameters or equivalent		
7.2a	Qos Features		
7.2b	ACL-based QoS		
7.2c	Class of Service (CoS) IEEE 802.1p		
7.2d	Per-port QoS configuration		
8	All categories of Switches, Transceivers , Switch OS should be from same OEM		
9	Switch should be quoted with TAC Support and Warranty for 7 years with NBD Hardware Replacement.		
10	Printed technical catalogs /brochures/ User manual / Release notes for the quoted model containing technical specifications, features along with bid.		

Tender No: IDRBT/SYS/VR/240/2022 – 2023 dated 15th December 2022**Technical Specification and Technical bid format for Layer 2 Network Switch**

Sl. No	Specification Required	Compliance Yes / No	Remarks
1	Product details		
1.1	Bidder to mention Make, Model No. and Part Code		
1.2	Qty – 2+1		
2	Port Details and Features		
2.1	Should offer Wire-Speed Non-Blocking Switching & Routing Performance at Layer 2.		
2.2	24-Port 10/100/1000 Mbps, 4 x10G Populated SFP Copper Connectivity		
2.3	Switch must support buffer of 8MB or more		
2.4	The Switch should support stack or equivalent Switch Clustering feature.		
2.5	Stacking bandwidth: 30 Gbps or more		
3	Performance		
3.1	Should provide Non-Blocking switch fabric capacity of 90 Gbps or more.		
3.2	Forwarding Capacity: wire-speed packet forwarding of 75 Mpps or more.		
4	Layer 2 features		
4.1	Should support 2K active VLANs, 10K MAC addresses or more, IP multicast snooping		
4.2	Should support Jumbo Frames (up to 4K bytes)		
4.3	All Functionalities of Switch shall be IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software.		
4.4	Switch Should support IEEE standards:-IEEE 802.3ab,IEEE 802.3z,IEEE 802.3ae,IEEE 802.1ba,IEEE 802.3ad,IEEE 802.1ab,IEEE 802.1v		
4.5	Switch should support IEEE 802.1d Spanning tree protocol		
4.6	Switch should support 802.1s MSTP (Multiple instances of STP)		
4.7	Switch should support 802.1w RSTP (Rapid spanning tree), Should support ITU G.8032/IP FRR/IRF or equivalent for ring resiliency for fast/better convergence from day 1		
4.8	Switch should support Port mirroring in same hardware		
4.9	Switch should support out-of-band management Port, Console Port and USB port.		
5.0	Switch should support network management via SNMPv1/v2/v3		

Sl. No	Specification Required	Compliance Yes / No	Remarks
5.1	Switch should support for Config/image upload and download from TFTP/FTP servers.		
5.2	Operating temperature: 0°C to 50°C		
5.3	Relative Humidity: 10% to 95% Non-condensing		
5.4	All the switches, the fiber modules should be from the same OEM		
6	Security		
6.1	Switch should support RADIUS, TACACS/TACACS+ and username/password for Authentication, Authorization and Accounting (AAA)		
6.1a	Port-based Network Access Control 802.1X		
6.1b	Port Security, Control Plane Policing (CPP) ,TLS, SFTP		
6.2	Should support secure communications to the management interface and system through SSL, Secure Shell (SSHv2), Secure Copy and SNMPv3		
6.3	Should support IPv4 and IPv6 ACLs with minimum of 2K rules per system		
6.4	Should support Byte and packet based broadcast, multicast, and unknown-unicast limits with suppression port dampening.		
6.5	Should support Flexible Authentication with 802.1x Authentication and MAC Authentication.		
7	Manageability		
7.1	Should support manageability using Network Management Software tools using SNMP		
7.1a	Solution should support performance management and analytics capability for applications such as Wireshark, Docker, etc		
7.1b	Integrated Standard based Command Line Interface (CLI),		
7.2	Should support Monitoring of critical network parameters or equivalent		
7.2a	Qos Features		
7.2b	ACL-based QoS		
7.2c	Class of Service (CoS) IEEE 802.1p		
7.2d	Per-port QoS configuration		
8	All categories of Switches, Transceivers , Switch OS should be from same OEM		
9	Switch should be quoted with TAC Support and Warranty for 7 years with NBD Hardware Replacement.		
10	Printed technical catalogs/brochures/ User manual / Release notes for the quoted model containing technical specifications, features along with bid.		

Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022 for Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT

Format for Deviations from Technical Specifications and Terms and Conditions of the RFP

S.No.	RFP Clause	Technical Specification or terms and conditions in the Tender document	Deviation offered	Reasons and whether deviation adds to the operational efficiency in case of the systems
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Note:

- i. Above information in detail should be furnished in case of each system offered separately.
- ii. Also in case of deviations from any of the terms and conditions of the tender document should be specified.
- iii. If any deviations from the technical specifications are warranted, reasons for such variations should be specified and
- iv. Whether such variations add to improvement of the overall performance of the systems, if any, should be specifically mentioned and supported by relevant technical documentation as required above

Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022 for Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT

Commercial Bid Format

(Amount in Rs.)

Sno	Description	Qty (a)	Unit Price (b)	Total Amount (c) = a*b	Taxes in % (d)	Taxes (e) =d*c	Total Amount (f)= e+c
Category – A Security Gateway Appliances							
1	Type – I - Security Gateway Appliances Firewalls with 7 year warranty.	4					
2	Type – II - Security Gateway Appliances Firewalls with 7 year warranty.	2					
3	Centralized Management System for Firewalls with 7 year warranty for-Sr.No 1 to 2	1					
4	Total Amount in Rs – A	-					
5	Buy back of old Security Gateway appliances	4					
Category – B – L2 & L3 Network Switches							
1	L3 Network Switches	2+2					
2	L2 Network Switches (24 Port)	2+1					
3	Total Amount in Rs – B						
4	Grand Total in Rs - A+B						

PERFORMANCE BANK GUARANTEE

The Director,

Institute for Development and Research in Banking Technology,
Road No. 1, Castle Hills,
Masab Tank, Hyderabad –500057

Dear Sirs,

PERFORMANCE BANK GUARANTEE – for Tender No: IDRBT/SYS/VR/240/2022-2023 dated 15th December 2022 for Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT.

WHEREAS

M/s. (name of System Integrator), a company registered under the Companies Act, 1956, having its registered and corporate office at (address of the System Integrator), (hereinafter referred to as “our constituent”, which expression, unless excluded or repugnant to the context or meaning thereof, includes its successors and assigns), entered into a Purchase Agreement dated..... (hereinafter, referred to as “the said Agreement”) with you (IDRBT) for **Supply, Installation, Maintenance of Perimeter Security Solution and Network Switches at IDRBT** as detailed in the said Agreement.

We are aware of the fact that in terms of sub-para (...), Section (...), Chapter (...) of the said Agreement, our constituent is required to furnish a Bank Guarantee for an amount Rs..... (in words and figures), being 10% of the Contract Price of Rs. ... (in words and figures), as per the said Agreement, as security against breach/default of the said Agreement by our Constituent.

In consideration of the fact that our constituent is our valued customer and the fact that he has entered into the said Agreement with you, we, (name and address of the bank), have agreed to issue this Performance Bank Guarantee.

Therefore, we (name and address of the bank) hereby unconditionally and irrevocably guarantee you as under :

- I. In the event of our constituent committing any breach/default of the said Agreement, which

breach/default has not been rectified within a period of thirty (30) days after receipt of written notice from you, we hereby agree to pay you forthwith on demand such sum/s not exceeding the sum of Rs..... (in words and figures) without any demur.

- II. Notwithstanding anything to the contrary, as contained in the said Agreement, we agree that your decision as to whether our constituent has made any such default/s / breach/es, as afore-said and the amount or amounts to which you are entitled by reasons thereof, subject to the terms and conditions of the said Agreement, will be binding on us and we shall not be entitled to ask you to establish your claim or claims under this Performance Bank Guarantee, but will pay the same forthwith on your demand without any protest or demur.
- III. This Performance Bank Guarantee shall continue and hold good till the completion of the contracted period for the 'Total Solution' i.e. (date), subject to the terms and conditions in the said Agreement.
- IV. We bind ourselves to pay the above said amount at any point of time commencing from the date of the said Purchase Agreement until the completion of the contracted period for the Total Solution as per said Agreement.
- V. We further agree that the termination of the said Agreement, for reasons solely attributable to our constituent, virtually empowers you to demand for the payment of the above said amount under this guarantee and we have an obligation to honour the same without demur.
- VI. In order to give full effect to the guarantee contained herein, we (name and address of the bank), agree that you shall be entitled to act as if we were your principal debtors in respect of your claims against our constituent. We hereby expressly waive all our rights of surety ship and other rights, if any, which are in any way inconsistent with any of the provisions of this Performance Bank Guarantee.
- VII. We confirm that this Performance Bank Guarantee will cover your claim/s against our constituent made in accordance with this Guarantee from time to time, arising out of or in relation to the said Agreement and in respect of which your claim is lodged with us on or before the date of expiry of this Performance Guarantee, irrespective of your entitlement to other claims, charges, rights and relief's, as provided in the said Agreement.
- VIII. Any notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax, registered post or other electronic media to our address, as aforesaid and if sent by post, it shall be deemed to have been given to us after the expiry of 48 hours when the same has been posted.
- IX. If it is necessary to extend this guarantee on account of any reason whatsoever, we undertake to extend the period of this guarantee on the request of our constituent under intimation to you

(IDRBT)

- X. This Performance Bank Guarantee shall not be affected by any change in the constitution of our constituent nor shall it be affected by any change in our constitution or by any amalgamation or absorption thereof or therewith or reconstruction or winding up, but will ensure to the benefit of you and be available to and be enforceable by you.
- XI. Notwithstanding anything contained hereinabove, our liability under this Performance Guarantee is restricted to Rs..... (in words and figures) and shall continue to exist, subject to the terms and conditions contained herein, unless a written claim is lodged on us on or before the afore-said date of expiry of this guarantee.
- XII. We hereby confirm that we have the power/s to issue this Guarantee in your favour under the Memorandum and Articles of Association/ Constitution of our bank and the undersigned is/are the recipient of authority by express delegation of power/s and has/have full power/s to execute this guarantee under the Power of Attorney issued by the bank in his/their favour.
2. We further agree that the exercise of any of your rights against our constituent to enforce or forbear to enforce or any other indulgence or facility, extended to our constituent to carry out the contractual obligations as per the said Agreement, would not release our liability under this guarantee and that your right against us shall remain in full force and effect, notwithstanding any arrangement that may be entered into between you and our constituent, during the entire currency of this guarantee.

Notwithstanding anything contained herein:

- I. Our liability under this Performance Bank Guarantee shall not exceed Rs. (in words and figure) ;
- II. this Performance Bank Guarantee shall be valid only up to (date, i.e., completion of contracted period for the Total Solution) ; and
- III. we are liable to pay the guaranteed amount or part thereof under this Performance Bank Guarantee only and only if we receive a written claim or demand on or before (date i.e. completion of the contracted period for the Total Solution).

This Performance Bank Guarantee must be returned to the bank upon its expiry. If the Performance Bank Guarantee is not received by the bank within the above-mentioned period, subject to the terms and conditions contained herein, it shall be deemed to be automatically cancelled.

Dated this day 2022.

Yours faithfully,

For and on behalf of the Bank,

(Signature)

Designation

(Address of the Bank)

Note:

- a) This guarantee will attract stamp duty as a security bond under Article 54(b) of the Mumbai Stamp Act, 1958.
- b) A duly certified copy of the requisite authority conferred on the official/s to execute the guarantee on behalf of the bank should be annexed to this guarantee for verification and retention thereof as documentary evidence in the matter.

Buy back of old Security Gateway appliance on “as is where” basis.

FIREWALLS			
S.L.No	Location	Model	Serial Nos
1	Hyderabad DC - FW 1	4800	1340B00745
2	Hyderabad DC - FW 2	4800	1345B00519
3	Belapur DR - FW 1	4800	1345B00516
4	Belapur DR - FW 2	4800	1345B00484