



PALAMURU UNIVERSITY :: MAHABUBNAGAR :: 509 001

TENDER NOTICE NO.164/E-TENDERS/ADMN/WIFI/PU/2nd Call, DATED 14-09-2023.

E-TENDER NOTIFICATION FOR SUPPLY, INSTALLATION AND COMMISSIONING OF FIREWALL EQUIPMENT WITH 3 YEARS LICENSE FOR PALAMURU UNIVERSITY, MAHABUBNAGAR.

Online e-Procurement tenders are invited from Firms/Contractors for Supply, installation and commissioning of firewall equipment with 3 years license for Palamuru University Campus Mahabubnagar.. The online Tender shall consist of two parts (i) Technical bid (ii) Commercial bid. The details of tender conditions and terms can be downloaded from the electronic procurement platform of Government of Telangana i.e., <https://tender.telangana.gov.in>. The Bidders need to register on the electronic procurement marketplace of Government of Telangana i.e., <https://tender.telangana.gov.in>. On registration on the e-Procurement marketplace they will be provided with a *User Id and Password* by the system using which they can submit their bids online. The University will not accept any bid submitted in the paper form. The bidders who are desirous of participating in 'e' procurement shall submit their Technical Bids etc., in the standard formats prescribed in the Tender documents displayed at 'e' market place. The bidders should upload the scanned copies of all the relevant certificates, documents etc., in the 'e' market place in support of their Technical bids. The bidder shall sign on all the statements, documents, certificates uploaded by him/her owning responsibility for their correctness / authenticity. The Department shall carry out the Technical Bid evaluation solely based on the uploaded certificates / documents, DD towards EMD in the e-procurement system and open the price bids of the responsive bidders. The bidder is solely responsible for the correctness of the particulars furnished in the online bid form. The bid document can be downloaded from 15-09-2023 @ 10.00 AM to 22-09-2023 @ 03.00 PM Time and date of opening of tenders: (a) Technical Bid (PQ Stage) 22-09-2023 @ 03.01 PM followed by opening of commercial bid. Under no circumstances, they will be relaxed unless otherwise extended by an official notification. The Bidders need to contact Office of the Registrar, Administrative Building, Palamuru University Campus, Telangana State – 509001, for information on e-Procurement tender. Email: registrar@palamuruuniversity.ac.in , Contact No.: 7989731204

The detailed tender documents can also be downloaded from the University's website www.palamuruuniversity.ac.in Please note that the Application fee should be remitted through **Demand Drafts drawn in favour of the Registrar Palamuru University** and uploaded along with the e-tender bid. However original DD's must be handover to The Registrar, Palamuru University, on or before the last date and time. Bids not accompanied with the tender document fee are liable to be rejected. ***The EMD should be paid online in form of e-challan or net banking .***

**Sd/-
REGISTRAR,**



PALAMURU UNIVERSITY : MAHABUBNAGAR :: 509 001

TENDER NOTICE NO.164/E-TENDERS/ADMN/WIFI/PU, DATED 14-09-2023.

E-TENDER NOTIFICATION FOR SUPPLY, INSTALLATION AND COMMISSIONING OF FIREWALL EQUIPMENT WITH 3 YEARS LICENSE FOR PALAMURU UNIVERSITY, MAHABUBNAGAR

Sub: Palamuru University – Supply, Installation and commissioning of firewall equipment with 3 years license for Palamuru University - Tender Notification – Regarding.

Palamuru University hereby invites e-procurement tenders from resellers/firms for supply, installation and commissioning of firewall equipment with 3 years license at Palamuru University, Mahabubnagar - 509001.

Part – I
TENDER SCHEDULE

- | | |
|--|---|
| 1. Name of the Tender | : Supply, installation, and commissioning of firewall equipment with 3 years license for Palamuru University |
| 2. Sale of Tender Schedule | : 15-09-2023 from 10:00 AM |
| 3. Closing date and time
(For receiving duly filled in tender bids) | : 22-09-2023 by 3.00 PM. |
| 4. Submission of Tender bids | : e-tenders in two parts (i) Technical bid (Annex-I) and (ii) Commercial bid (Annex-II) should be submitted at e-procurement tenders |
| 5. Date & Time of opening | : 22-09-2023 at 03.01 P.M on E-procurement Website |
| 6. Earnest Money Deposit (EMD) | : EMD of Rs. 1,00,000/- (Rupees One Lakh only)
Payable through online mode of payment in favour of Registrar, PU. The Tenders without accompanying EMD will not be considered and will be summarily rejected. |
| 7. Application Cost | : Application cost of Rs. 5,000/- (Five Thousand only) should be payable in favor of the Registrar, PU and should submit on or before last date and time |
| 8. Security Deposit | : 5 % of the total cost of the product in the Form of Bank Guarantee in favour of The Registrar, Palamuru University, payable at Mahabubnagar from any Nationalized Bank, after award of the contract for a period of 3 Years |
| 9. Warranty Period | : Onsite Warranty of the products installed should be 3 Yrs. |
| 10. Payment Terms | : No advance payment will be made. Payment will be arranged in accordance with the satisfactory completion installation of firewall equipment. |
| 11. Agreement | : Agreement should be executed by the successful bidder upon issue of work order. However, EMD will be retain till the submission of Bank Guarantee. |

Sd/-
Registrar, PU.

Annexure-I
TECHNICAL SPECIFICATIONS

Sl. No	Specification
	General
1	OS should be "IPv6 Phase II Ready" certified
	Hardware
2	The Firewall must be appliance based
3	Should support 8 or more gigabit RJ45 interfaces
4	Should support 8 or more 1G SFP Slots
5	Should have 4 no of 10G SFP+ slots populated with the transceivers
6	Should have 1 console port (RJ45) and 1 or more Number of USB ports
	Firewall Performance
7	Should have Firewall throughputs of minimum 30 Gbps or more
8	IPSec VPN throughput should be 10 Gbps or more
9	NGFW throughput should be 8 Gbps with enterprise mix traffic \ real world traffic
10	Threat protection throughput should be 6 Gbps with enterprise mix traffic \ real world traffic
11	Must support at least 70,00,000 or more concurrent connections
12	Must support at least 4,00,000 or more new sessions per second processing.
13	Should Support Virtualization (ie Virtual Systems / Virtual Domains). Should be having 10 or more virtual system license from day one
	Firewall Features
14	Should support both "bridge mode" or "transparent mode" apart from the standard NAT mode
15	Should provide NAT functionality, including PAT. Should support NAT 66, NAT 64, Static NAT IPv4 to IPv6 and vice versa and IPv6-IPv4 tunneling or dual stack.
16	Should support IPv4 & IPv6 policies
17	Provision to create secure zones / DMZ (ie Multi- Zone support)
18	Should support the standards based Multi-Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.
19	Should support VLAN tagging (IEEE 802.1q) in NAT/Route mode
20	Should support Static routing and Dynamic Routing (RIP, OSPF & BGP)
21	Should support Active-Active/ Clustering as well as Active- Passive redundancy.
22	Should support ISP Load balancing/ Link Sharing and Failover
23	Should support multi-path intelligence based on link quality criteria
24	Should support link performance check based on packet loss, latency & jitter
25	Should support application specific rules based on SLA strategy
26	Should support high performance deep packet inspection for application identification and control
	Authentication
27	Should support User-Group based Authentication (Identity based Firewalling) & Scheduling
28	Should support authentication servers – RADIUS, LDAP & Active Directory
29	Support for RSA Secure ID or other Token based Products

	VPN
30	Should support protocols such as DES & 3DES, MD5, SHA-1, SHA-256 authentication, Diffie- Hellman Group 1, Group 2, Group 5, Group 14, Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm, The new encryption standard AES 128, 192 & 256
31	Should support minimum 200 IPSec Site-to-Site and 1000 no of IPSec Site-to- Client VPN tunnels.
32	Should have integrated SSL VPN with license for 1000 concurrent SSL VPN users from day one
33	Support for Client based VPN is mandatory and support for SSL Web VPN is preferable.
34	Should support Windows, Linux and MAC OS for SSL-VPN
35	Should support NAT within IPSec/SSL VPN tunnels
36	Should support Stateful failover for both Firewall and VPN sessions.
	IPS
37	Should have a built-in Signature and Anomaly based IPS engine on the same unit
38	Should have protection for 7000+ signatures
39	Able to prevent denial of service and distributed Denial of Service attacks.
40	Supports user-defined signatures (i.e., Custom Signatures) with Regular Expressions.
	Application Control
41	Should have Application control feature with 3000 or more application signatures
42	Should perform Traffic Shaping based on applications
43	Should control popular IM/P2P, proxy applications regardless of port/protocol
	Gateway Antivirus
44	The appliance should facilitate embedded anti-virus/ anti-malware support
45	Gateway AV/ Anti-malware should be supported for real-time detection of viruses and malicious code for HTTP, HTTPS, FTP, SMTP, SMTPS, POP3 and IMAP protocols
46	should also include Botnet filtering and detecting and preventing Botnet command and control traffic
47	Should have configurable policy options. Possible to select traffic to scan for viruses
48	Should support on-premise/cloud APT solution for unknown malware analysis protection.
49	Should support advanced anti-malware detection system for identifying and mitigating Advanced Persistent Threats. Together with superior, industry-validated AV signatures, which identifies standard AV threats, and uses advanced heuristics and on-premise sandboxing to determine malicious behavior.
	Web Filtering
50	The appliance should facilitate embedded Web Content and URL Filtering feature
51	Web content and URL filtering solution should work independently without the need to integrate with External proxy server.
52	URL database should have 200 million or more URLs under more than 70 categories
53	Should be able to block different categories/sites based on User Authentication.
	Management, Log & Reporting
54	Firewall should support management either through GUI/CLI
55	Firewall should support logging to multiple syslog servers.
56	Log & Reporting should be a dedicated appliance solution out of the Firewall
57	The log & reporting platform must have a minimum storage of 2 TB
58	The solution should provide comprehensive security event logging, reporting
	Preferred Make: CISCO/ Palo Alto / Fortinet

PART – III
TERMS & CONDITIONS

1. The Firms should submit their tenders duly enclosing Demand Drafts towards Non-refundable application cost of **Rs. 5,000/- (Rupees five Thousand only)** in the name of Registrar Palamuru University after going through the conditions laid down.
2. The Bidder shall strictly adhere to all the terms and conditions stipulated in the tender with regard to Supply, Installation and Commissioning of firewall equipment for Palamuru University Campus.
3. The University shall invite the L-1 bidder for negotiation if the University observe the price quoted by L-1 bidder are on higher side
4. *Time is the essence of the contract and the bidder should supply and install firewall equipment within **45 Days** of issue of work order or Letter of Intent on war foot basis.*
5. The following information has to be filled by the tenderer with evidence (Documentary proof to be enclosed). Mandatory Conditions
 - a. Registration Certificate
 - b. GST Registration No.
 - c. Past Experience orders related to IT/ITES/Networking.
 - d. Pan Card Copy.
 - e. Tender Specific OEM Authorization for the mentioned Product on Bidder Name and Address.
 - f. Telangana GST Address and Office Address
 - g. Annual Turn over of Rs. 30 Lakhs per year in last three Financial Year
 - h. Detail Profile of the Firm
 - i. IT Returns of the last 3 (three) years.
 - j. The bidder should Submit MAF from OEM, Data sheet of product, specified certification and other necessary technical literature.
6. The offers must be in English. The rates should be indicated both in figures and in words against each item exclusive of taxes as applicable as per government norms.
7. The rates shall be fixed and constant throughout the entire period of the Contract and will not be modified under any circumstances.
8. Offers received after the bid closing date/time shall not be considered.
9. Telex / Tele fax / E-Mail Tenders will not be accepted and the University takes no responsibility for delay / loss or non-receipt of tenders by post / couriers, online e tender only
10. Any offer containing incorrect statement and incomplete information will be summarily rejected and no unsolicited correspondence shall be entertained.
11. PRICE BID / FINANCIAL BID of only those bidders shall be opened who qualify in the technical evaluation.
12. Palamuru University reserves the right to accept / reject any offer in full or in part or accept any offer other than the lowest without assigning any reasons thereof.
13. All disputes or differences whatsoever arising between the parties relating to the contract shall be settled by the arbitration in accordance with the rules of arbitration of Indian Council of Arbitration and the Award made in pursuance thereof shall be binding on the parties. The venue of arbitration

shall be Mahabubnagar, and the Registrar, Palamuru University, Mahabubnagar – 509001, will make the appointment of the arbitrator on behalf of the University.

14. The E.M.D of the unsuccessful tenderers will be refunded without any interest.
15. The firm must have valid TSGST/CST/CGST Registration Certificate. (Please attach copies of valid certificates).
16. The security deposit shall be liable to be forfeited wholly or partly at the sole discretion of the University, if the tenderer either fails to execute the work as per the tender terms, or fails to fulfill the contractual obligations or fails to settle in full his dues to the Palamuru University.
17. In case of premature termination of the contract, the Security Deposit will be forfeited and the Palamuru University will be at liberty to recover the loss suffered by it & if additional cost is to be paid, the same shall be recovered from the tenderer.
18. The University is empowered to recover from the Security Deposit for any sum due and for any other sum that may be fixed by the University as being the amount or loss / losses / damages suffered by it due to delay in performance and / or non-performance and / or partial performance of any of the conditions of the contract and / or non-performance of guarantee obligations.
19. Failure to comply with the terms of security deposit shall result into cancellation of work order and termination of the contract without any further reference to the tenderer and the EMD shall be forfeited.
20. The University reserves the right to cancel the tender or terminate the contract with L-1 vendor without assigning any reasons thereof.
21. **Warranty:** All items supplied by the tenderer shall be guaranteed against any defects and the tenderer should provide time-to-time operational maintenance support for a period of 3 years (On Site comprehensive Warranty). The said warranty should cover all Hardware products & Software. The warranty and service shall be provided directly from the manufacturer. Necessary guarantee certificates shall accompany the supplies. The tenderer shall be liable to rectify any defects that may be found in the equipment supplied free of cost
22. Response Time: The Response time of the bidder to attend any complaint upon receipt of the complaint/information from the user should not be more than 24 hours for minor breakdown and not more than 72 hours for major breakdown
23. The bidders should submit Documents in support of Technical Specifications of the items mentioned in Part-II.
24. Make / Brand of items offered shall be specified failing which offers are liable to be rejected. It shall be appreciated if one copy of detailed descriptive literature / pamphlets is enclosed along with the offer which may help technical evaluation. In case material offered is ISI marked / tested at any Govt. recognized test house copies of relevant certificates shall be furnished along with the offer.
25. Bidders can seek clarifications, raise technical queries, etc., related to tender by 13-04-2023 via e-mail to registrar@palamuruuniversity.ac.in
26. 100% payment will be released only on satisfactory installation/services as per the scope of work as certified by the officer in charge of the Institute and after producing the GST invoice. Bidder does not agree to the above payment terms is requested not to submit their Bid.

REGISTRAR, PALAMURU UNIVERSITY

Annexure - II
TECHNICAL BID

1. Name of Tendering Company/Dealer with :
Registration No. & Date issued by appropriate
authorities (Please enclose copy of certificate of
registration)
2. Name of Chairman/Managing Director/Manager :
3. Furnish following particulars of the Registered Office :
 - a. Complete Postal Address :
 - b. Telephone No. :
 - c. Fax. No. :
 - d. E-Mail Address :
4. Furnish following particulars of Registered office if :
different from Sl.No.4.
 - a. Complete Postal Address :
 - b. Telephone No. :
 - c. Fax. No. :
 - d. E-Mail Address :
5. PAN No. (Attach Attested Copy) :
6. GST No. (Attach Attested Copy) :
7. Service Tax Regn. No. (Attach Attested Copy) :
8. Financial turnover for the last three Consecutive financial :
Years Please attach copies of audited balance sheet and
IT returns for (2018-19, 2019-2020 and 2020-21), (Attach
separate sheet if space provided is insufficient)
9. Give details of the major clients – Govt. Departments, :
PSUs, Research Organizations (Copies of the Purchase
Orders / Indents should be attached for proof).
 - a. Sl. No :
 - b. Name& address of the client with details :
 - c. Name of the contact person, :
 - d. telephone no., Fax no., :
 - e. e-mail id :
10. Details of Earnest Money Deposit D.D. No. and Date &
Name of the Bank

TECHNICAL COMPLIANCE

Sl. No	Specification	Compliance YES / NO
	Make	
	Model No.	
	General	
1	OS should be "IPv6 Phase II Ready" certified	
	Hardware	
2	The Firewall must be appliance based	
3	Should support 8 or more gigabit RJ45 interfaces	
4	Should support 8 or more 1G SFP Slots	
5	Should have 4 no of 10G SFP+ slots populated with the transceivers	
6	Should have 1 console port (RJ45) and 1 or more Number of USB ports	
	Firewall Performance	
7	Should have Firewall throughputs of minimum 30 Gbps or more	
8	IPSec VPN throughput should be 10 Gbps or more	
9	NGFW throughput should be 8 Gbps with enterprise mix traffic \ real world traffic	
10	Threat protection throughput should be 6 Gbps with enterprise mix traffic \ real world traffic	
11	Must support at least 7,000,000 or more concurrent connections	
12	Must support at least 400,000 or more new sessions per second processing.	
13	Should Support Virtualization (ie Virtual Systems / Virtual Domains). Should be having 10 or more virtual system license from day one	
	Firewall Features	
14	Should support both "bridge mode" or "transparent mode" apart from the standard NAT mode	
15	Should provide NAT functionality, including PAT. Should support NAT 66, NAT 64, Static NAT IPv4 to IPv6 and vice versa and IPv6-IPv4 tunneling or dual stack.	
16	Should support IPv4 & IPv6 policies	
17	Provision to create secure zones / DMZ (ie Multi- Zone support)	
18	Should support the standards based Multi-Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.	
19	Should support VLAN tagging (IEEE 802.1q) in NAT/Route mode	
20	Should support Static routing and Dynamic Routing (RIP, OSPF & BGP)	
21	Should support Active-Active/ Clustering as well as Active- Passive redundancy.	
22	Should support ISP Load balancing/ Link Sharing and Failover	
23	Should support multi-path intelligence based on link quality criteria	
24	Should support link performance check based on packet loss, latency & jitter	
25	Should support application specific rules based on SLA strategy	
26	Should support high performance deep packet inspection for application identification and control	
	Authentication	
27	Should support User-Group based Authentication (Identity based Firewalling) & Scheduling	
28	Should support authentication servers – RADIUS, LDAP & Active Directory	
29	Support for RSA Secure ID or other Token based Products	
	VPN	

30	Should support protocols such as DES & 3DES, MD5, SHA-1, SHA-256 authentication, Diffie- Hellman Group 1, Group 2, Group 5, Group 14, Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm, The new encryption standard AES 128, 192 & 256	
31	Should support minimum 200 IPSec Site-to-Site and 1000 no of IPSec Site-to- Client VPN tunnels.	
32	Should have integrated SSL VPN with license for 1000 concurrent SSL VPN users from day one	
33	Support for Client based VPN is mandatory and support for SSL Web VPN is preferable.	
34	Should support Windows, Linux and MAC OS for SSL-VPN	
35	Should support NAT within IPSec/SSL VPN tunnels	
36	Should support Stateful failover for both Firewall and VPN sessions.	
	IPS	
37	Should have a built-in Signature and Anomaly based IPS engine on the same unit	
38	Should have protection for 7000+ signatures	
39	Able to prevent denial of service and distributed Denial of Service attacks.	
40	Supports user-defined signatures (i.e., Custom Signatures) with Regular Expressions.	
	Application Control	
41	Should have Application control feature with 3000 or more application signatures	
42	Should perform Traffic Shaping based on applications	
43	Should control popular IM/P2P, proxy applications regardless of port/protocol	
	Gateway Antivirus	
44	The appliance should facilitate embedded anti-virus/ anti-malware support	
45	Gateway AV/ Anti-malware should be supported for real-time detection of viruses and malicious code for HTTP, HTTPS, FTP, SMTP, SMTPS, POP3 and IMAP protocols	
46	should also include Botnet filtering and detecting and preventing Botnet command and control traffic	
47	Should have configurable policy options. Possible to select traffic to scan for viruses	
48	Should support on-premise/cloud APT solution for unknown malware analysis protection.	
49	Should support advanced anti-malware detection system for identifying and mitigating Advanced Persistent Threats. Together with superior, industry-validated AV signatures, which identifies standard AV threats, and uses advanced heuristics and on-premise sandboxing to determine malicious behavior.	
	Web Filtering	
50	The appliance should facilitate embedded Web Content and URL Filtering feature	
51	Web content and URL filtering solution should work independently without the need to integrate with External proxy server.	
52	URL database should have 200 million or more URLs under more than 70 categories	
53	Should be able to block different categories/sites based on User Authentication.	
	Management, Log & Reporting	
54	Firewall should support management either through GUI/CLI	
55	Firewall should support logging to multiple syslog servers.	
56	Log & Reporting should be a dedicated appliance solution out of the Firewall	
57	The log & reporting platform must have a minimum storage of 2 TB	
58	The solution should provide comprehensive security event logging, reporting	
	Preferred Make: CISCO/ Palo Alto / Fortinet	

Annexure – II
COMMERCIAL BID

S.No.	Description of items	Qty	Rate	Total Amount
1.	Firewall equipment with 3 years license subscription and 3 years warranty for 3000 Users	01		
	NET TOTAL			
	GST @ 18%			
	TOTAL (Incl. of taxes)			

CERTIFICATE OF ETHICAL PRACTICES

I / We assure the Institute/University that neither I / We nor any of my / our workers will do any act/s which is improper / illegal during the execution in case the tender is awarded to us. Neither I / We nor anybody on my / our behalf will indulge in any corrupt activities / practices in my / our dealing with the Institute. I / We will have no conflict of interest in any of our works / contracts at the University.

Date:

SIGNATURE OF THE
TENDERER

ANNEXURE-III

PERFORMANCE BANK GUARANTEE ON SECURITY DEPOSIT

This deed of Guarantee made on..... day of Month & Year by Name & Address of the bank (hereinafter called the "GUARANTOR") on the one part, on behalf of M/s Name & address of the Firm (hereinafter called the "FIRM") in favour of The Registrar, Palamuru University, Mahabubnagar, on the following terms and conditions.

Whereas the FIRM is entering into an agreement with PALAMURU UNIVERSITY for providing and fixing of Wi-Fi Access Points and networking in Palamuru University Campus and this guarantee is being made for the purpose of submission of Security money required to be deposited at the time of signing of the agreement between Palamuru University and FIRM.

Know all people by these presents that the GUARANTOR, hereby undertake to indemnify and keep Palamuru University indemnified up to the extent of Rs...../- Rupees in words..... only) during the validity of this bank guarantee and authorize Palamuru University to recover the same directly from the GUARANTOR. This bank guarantee herein contained shall remain in full force and effect till the expiry of its validity or till any extended period (if extended by the bank on receiving instructions from FIRM.). The liability under the guarantee shall be binding on the GUARANTOR or its successors.

Whereas the GUARANTOR further agrees that their liability under this guarantee shall not be affected by any reason of any change in the offer or its terms and conditions between the FIRM and Palamuru University with or without the consent or knowledge of the GUARANTOR.

Whereas the GUARANTOR further agrees to pay guaranteed amount hereby under or part thereof, on receipt of first written demand whenever placed by Palamuru University during the current period of this guarantee. The GUARANTOR shall pay Palamuru University immediately without any question, demure, reservation or correspondence.

Whereas the GUARANTOR hereby agrees not to revoke this guarantee bond during its currency period except with the previous consent of Palamuru University in writing.

Notwithstanding anything contained herein

- Our liability under this bank guarantee shall not exceed Rs..... (Rupees in words only)
- This Bank guarantee shall be valid up to Rs...../- (Rs. In words.....only).
- We are liable to pay the guaranteed amount or any part thereof under this bank guarantee only and only against the written claim or demand on or before

Sealed with the common seal of the bank on thisday of (Month) and (Year).

Witness:

1.....

2.....

(Signature and seal of the bank)

SIGNATURE AND STAMP OF THE TENDERER