



MAULANA AZAD NATIONAL URDU UNIVERSITY

(A Central University established by an Act of Parliament in 1998)

PURCHASE & STORES SECTION

INVITATION FOR ONLINE TENDER (TWO BIDS SYSTEM)

(Tender No:01/CIT/MANUU/F.73/FTS.24/2019), dt: 4th March 2020

Sub: MANUU – Purchase & Stores Sections – Supply and installation of UTM (Nest Gen Firewall) Centre under buyback of existing UTM for Information Technology – Online (through CPPP) Tender Enquiry – Reg.

The Maulana Azad National Urdu University (MANUU), Hyderabad (Central University established by an Act of Parliament in 1998) intends to procure UTM (Next Generation Firewall) for Centre for Information Technology, MANUU, Gachibowli, Hyderabad from the prospective bidders (under buyback of existing UTM). The intended bidders may furnish their quotations (as per the specifications mentioned below) online through Central Public Procurement Portal (CPPP) @ <https://eprocure.gov.in/eprocure>. The online bids along with **EMD for Rs. 75,000/-** drawn in favour of Finance Officer, MANUU, Hyderabad (Exemption as per GoI norms will only be considered on production of documentary proof in the concern category, failing which the bid will be rejected) shall be furnished as per the proforma prescribed (Annexure-2). The bid documents (both Technical bid and financial bid) along with the scanned copy of EMD proof must be uploaded online on CPP Portal on or before **17.03.2020** by **3.00 pm**. However, the original EMD document/DD shall be submitted at Purchase Section next day of closing date of submission of bids).

Terms and Conditions of the Tender:

1. Submission of Bids:

- 1.1 The technical and financial bids should be furnished in Annexure-1 and Annexure-2 respectively and both the bids should be submitted online @ <https://eprocure.gov.in/eprocure> only along with the requisite documents.
- 1.2 Conditional and incomplete bids will be rejected summarily
- 1.3 The bids must be submitted before due date and time.
- 1.4 **Modification and Withdrawal of Bids:** The bidder may modify or withdraw their bid through online before last date for submission of the Bids.
- 1.5 No tender will be accepted after the date of opening and time as specified in the tender enquiry for whatever reasons.
- 1.6 Bidders shall have to ascertain the exact percentage of GST applicable on each of the items while quoting the rates in the financial bid (ANNEXURE-2). In case of discrepancy / difference of opinion on GST rates, the University shall decide the lowest quotation on verification of the relevant provisions of GST Act vis-à-vis supporting documents provided by the bidders in respect of the claim for the GST. In case of ambiguity on percentage of GST applicable, the University will award the contract on the basic price i.e excluding GST quoted in the online price bid. The decision of the University shall be final and binding in this regard. The items procured are exclusively for the MANUU, Centre for Information Technology for education and research purpose only and not for commercial use.
- 1.7 The University reserves its right to award the contract to the firm quoting lowest (L-1) rates, i.e., Price of New Equipment less Buyback price of existing UTM.



2. Submission of EMD

- 2.1 The firms should submit EMD of Rs. 75,000/- in the form of Demand Draft / Bank Guarantee / Fixed Deposit drawn in favour of Finance Officer, MANUU payable at Hyderabad in original by post or by hand. Scanned copy of EMD should be uploaded along with Technical bid document. Exemption as per govt. norms will be considered on production of documentary proof.
- 2.2 The EMD of the unsuccessful bidders will be returned within 60 days after closing date of the bid or within 30 days after finalizing the bid without interest. The EMD of the successful bidder will be returned on submission of Performance Security.

3. Opening of Bids

- 3.1 Technical bid would be opened online only and scrutinized as per the eligibility criteria prescribed.
- 3.2 Financial bids of only technically qualified bidders will be opened by the authorized officers of the University.
- 3.3 The bidder must provide the services as per the specifications mentioned in the tender. The firms may also quote for higher / superior specifications. However, the criteria for requirement would be based on the actual specifications mentioned in this tender document.
- 3.4 The quotation should be valid for a minimum period of 75 days from the closing date of tender.

4. Pre-qualification (eligibility) criteria:

- 4.1 The bidder should be a registered firm / supplier / authorized dealer with GSTIN.
- 4.2 The firm should submit an EMD of Rs. 75,000/-
- 4.3 The firm should submit the OEM Certificate or OEM Authorization of dealer or authorization of distributor from OEM's or manufacture's authorization certificate specific to this tender.
- 4.4 The firm should submit bid showing item wise compliance as per Annexure – 4 with respect to specification and warranty etc., any deviation of quality will be summarily rejected.
- 4.5 The bidder must upload Annexure – 1 duly filled in.
- 4.6 The bidder must have achieved the minimum average annual turnover of **Rs.12,00,000/-** during the last three financial years. (To be supported by the documents mentioned at S. No. 7 of Annexure 1)



PURCHASE & STORES SECTION

- B. In addition to the above, the bidder must have supplied the;
- Network Security Related Equipment's on three Purchase Orders worth **Rs. 6,00,000/-** each (or)
 - Network Security Related Equipment's on two Purchase Orders worth **Rs. 7,50,000/-** each (or)
 - Network Security Related Equipment's on one Purchase Order worth **Rs.12,00,000/-** During the last 5 years period.
- C. In support of the above (tender clause 4.6. B), the bidders are required to upload the copy(ies) of Purchase Order or any certificate indicating the details of amount of work along with Work Order / Award of Contract / Purchase Order with quantities and date. Consolidated quantities and amount against different orders/contract cannot be considered.

5. Job Requirement

- 5.1 Supply and Installation of **UTM(Next Generation Firewall) under buyback of existing UTM Fortigate 3040b for Centre for Information Technology as per specification and quantity mentioned below.**

S.no	Particulars	Quantity
1.	Supply, Installation, Configuration and Commissioning of UTM Firewall with 3 Years Subscription of (Antivirus, Antispam, Web & Application Filter, Intrusion Detection & Prevention plus 24 X 7 Support) as per the specification below	01 set
2.	Buy back of existing running UTM Model: Fortigate 3040b S.No: FG3K0B3I13700055 <i>(The prospective bidders are requested to visit the site and check the condition/location of the items during any working hours/days on their own cost)</i>	01 set

- 5.2 Specifications of S.no 1 of tender clause 5.1 (new UTM equipment)

S.No	Specification
General Features	
1	Network security appliance should support "Stateful" policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc. Proposed NGFW solution should have WAF(Web Application Firewall) capability.
2	OEM should be positioned in Gartner's Report – in Magic Quadrant in the leaders/challengers for UTM as per the report for the year 2018-2019.
3	OEM should have technical support centre in India
4	Should have 3 years 24X7 support warranty & gateway anti-malware,anti spam,anti bot,web & apps protection, Anti-Virus, IPS/IDS, sandboxing from day 1.



PURCHASE & STORES SECTION

5	Proposed UTM/NGFW should be NSS lab recommended.
Hardware & Interface for each Firewall Unit/Appliance	
6	The platform must be supplied with minimum 8 x GE RJ45 inbuilt interfaces, 6 x 1GE SFP interface Slots populated with 5x 1GE SFP Single Mode Transceivers & 2 x 10GE SFP+ interface slots.
7	Minimum 240 GB SSD local storage
8	The Appliance should have separate USB & Console Ports
Performance for each Firewall Unit/Appliance	
9	A Minimum NGFW throughput in real world/production environment (by enabling and measured with application visibility and control utilizing HTTP transactions and traffic mix such as HTTPS, SMTP and other protocols and logging enabled) – 9 Gbps.
10	Concurrent Connection(TCP) – 6 Million
11	New Connections per Sec - 2 Million
12	Minimum NG Threat prevention throughput in real world/production environment (by enabling and measured with application visibility and control, NGIPS, Anti-Virus, Anti-Spyware, Anti-Bot and all other security threat prevention features enabled with HTTP transactions and traffic mix such as HTTPS, SMTP and other protocols and logging enabled)– 7 Gbps. The bidder shall submit the performance test report from Global Product Engineering department / Global Testing Department/ Global POC team of OEM to certify the mentioned performance.
13	Minimum IPsec VPN throughput – 9 Gbps
14	Simultaneous Client-to-Site IPsec VPN tunnels: 1000
Routing Protocols	
15	Static Routing
16	Policy Based Routing
17	The Firewall should support dynamic routing protocol like RIP, OSPF, BGP
Firewall	
18	Firewall should provide application inspection for LDAP, SIP, H.323, SNMP, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC, IMAP, NFS etc
19	The firewall should support transparent (Layer 2) firewall or routed (Layer 3) firewall Operation
20	The Firewall setup should support ISP link load balancing : multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing and granular multipath rule (or) ECMP (Equal cost multipath)
21	Firewall should support link aggregation functionality to group multiple ports as single port.
22	Firewall should support static NAT, policy based NAT and PAT
23	Firewall should support IPsec data encryption

PURCHASE & STORES SECTION

24	It should support the IPSec VPN for both site-site and remote access VPN
25	Firewall should support IPSec NAT traversal.
26	Support for standard access lists and extended access lists to provide supervision and control
27	Firewall system should support virtual tunnel interfaces to provision route-based IPSec VPN
28	Firewall system should support Quality of service (QoS)/bandwidth management functionalities.
29	The Firewall should have integrated solution for SSL VPN
30	Should support LDAP(OpenLDAP), RADIUS(Freeradius), Windows AD, PKI based Authentication
Integrated Intrusion Prevention System(IPS)	
31	IPS should have DDoS and DoS anomaly detection and protection mechanism with threshold configuration, Deep packet Inspection and IPS signature-tuning for false positives.
32	Support SYN detection and protection for both targets and IPS devices.
33	The device shall allow administrators to create Custom IPS signatures
34	Should have a built-in Signature and Anomaly based IPS engine on the same unit
35	Signature based detection using real time updated database & should have minimum 8000+ IPS signature database from day one
36	Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)
37	Signature updates do not require reboot of the unit.
38	Configurable IPS filters to selectively implement signatures based on severity, target (client/server) and operating systems
39	IPS Actions: Default, monitor, block, reset, or quarantine
40	Should support packet capture option
41	IP(s) exemption from specified IPS signatures
42	Should support IDS sniffer mode
43	Firewall should support antimalware capabilities , including antivirus, botnet traffic filter, antispysware and sandboxing technology. The solution should have an inbuild Advanced Malware Protection Licence which should be able to protect from zero-day threats like ransomware.
44	Solution should be able to detect and prevent unique communication patterns used by BOTs i.e. information about botnet family
45	The solution should support sandboxing for prevention from zero day threats (Proposed unknown malware analysis service with guaranteed protection signature delivery time not more than 10 minutes. Solution must have capabilities to prevent unknown threats)



PURCHASE & STORES SECTION

46	Should have antivirus protection for protocols like HTTP, HTTPS, IMAPS, POP3S, SMTPS protocols etc.
47	Solution should have an option of packet capture for further analysis of the incident
48	Solution should uncover threats hidden in SSL links and communications Including SSL Decryption and SSH Inspection
49	The AV should scan files that are passing on CIFS protocol
50	The proposed system shall provide ability to allow, block attachments or downloads according to file extensions and/or file types
51	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.
Other Support	
52	Should support features like Web-Filtering, Application-Control & Gateway level DLP from day one
53	The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should support over 120 Million URLs without external solution, devices or hardware modules.
54	Should support detection over 3,500+ applications in multiple Categories: Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)
55	The solution should have the flexibility to write security policies based on IP Address & User Name
56	QoS features like traffic prioritization, differentiated services,. Should support for QoS features for defining the QoS policies.
57	It should support the VOIP traffic filtering
58	Appliance should have identity awareness capabilities
59	Protection against Reverse proxy, SQL injection protection, Cross-site scripting protection
60	Solution must support VRRP clustering protocol or equivalent.
61	Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI.
62	Support accessible through variety of methods, including console port, Telnet, and SSH
63	Support for both SNMPv2 and SNMPv2c, providing in-depth visibility into the status of appliances.
64	Should have capability to import configuration and software files for rapid provisioning and deployment using Trivial File Transfer Protocol (TFTP), HTTP, HTTPS
65	The proposed solution should have feature for logging & reporting with minimum 1TB of total Log Storing capacity.
66	The reporting platform must provide option for creating customized reports.

PURCHASE & STORES SECTION

67	The reporting platform must provide multiple report output types or formats, such as PDF, HTML, and CSV
68	Should capable to provide a convenient method for alerting administrators when critical events are encountered, by sending e-mail alert messages to administrator defined e-mail addresses
Others / Miscellaneous	
70	The bidder/OEM must provide onsite and remote support as and when required
71	Training of required duration to be provided to corresponding staffs of CIT, MANUU for day to day handling and configuration of the appliances. At least 2 days separate admin level training post installation is mandatory
72	The buyback cost for the existing device Fortigate 3040b to be adjusted in the price bid
73	Licence: All the licensing required for the functionalities asked in the tender specification should be included in the offerings.
74	All the devices should be upgraded to the recent OS free of cost.
75	SLA: 1. The Initial configuration must be done by OEM Certified Engineer on-site. 2. Onsite as well as remote support as and when required. 3. OEM Warranty for the Entire system along with 24/7 support. 4. In case of Hardware breakdown the damaged hardware components must be replaced within 5 days after initiation of the service request. 5. Hardware should be updated now and then with latest firmware throughout the warranty period. 6. Above item should carry Three years onsite full comprehensive free warranty. 7. Proposed Product Firewall UTM should be supportable back to back warranty/AMC from OEM for at least 3 years after completion of 3 years warranty period.

6. Delivery & Payment:

- 6.1 The supply and installation of the said items should to be made within a period of **30days** from the date of award of contract (AOC) **or** on or before 30.03.2020 **whichever is earlier.**
- i) Failure to supply the material as per the prescribed specifications within the stipulated period shall entitle the Procuring Entity (MANUU) for imposition of penalty @ 1/2% (half percent) **per day** on the quantity undelivered covered in the award of contract, subject to a maximum of 5% (five percent) after expiry of the stipulated time period of the supply unless extension is obtained in writing from the office on valid ground before expiry of delivery period.
- ii) If the deliveries are not made by the specific date and Procuring Entity is forced to buy the material at your risk and cost from elsewhere, the loss or damage that may be sustained thereby would be recovered from the defaulting supplier.
- 6.2 **The selected firms should submit 10% of value of Award of Contract (AOC) as Performance Security in the form of D.D / Fixed Deposit Receipt / Bank Guarantee** in favour of MANUU payable at Hyderabad which would be released (without interest) after supply of material as per specifications and after fulfilling of all tender obligations. In case, the goods supplied are under warranty, the **10% Performance Security will be released after 60 days of completion of warranty period without any interest.** The



PURCHASE & STORES SECTION

account details are as follows;

A/c. Name : Maulana Azad National Urdu University
A/c. Number : 187901000000001
Bank : Indian Overseas Bank
Branch : Gachibowli, Hyderabad-500 032
IFSC Code : IOBA0001879

- 6.3 **Payment:** 100% payment after receipt of the goods, inspection, installation (if any) at concerned office site in good condition and acceptance by the consignee, within 30 (thirty) days provided the successful bidder should have been furnished the 10% Performance Guarantee.
- 6.4 No advance/part payment will be made.

7. Miscellaneous

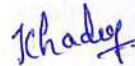
- 7.1 **MANU University GSTIN:** 36HYDM03116B1DT. MANUU does not claim / registered with Dept. of Science and Technology or any other Government Dept for exemption / discount on GST
- 7.2 The items procured are exclusively for the MANUU Centre for Information Technology for education and research purpose only and not for commercial use.

8. Termination of the contract:

- 8.1 If the information provided by the firm during the process of contract is found false at later stage, the University reserves the right to cancel the Purchase Order and / or blacklist the firm.
- 8.2 Sub-letting of this contract is not permissible.
- 8.3 This Request for Proposal (RFP) is issued with no financial commitment and the Buyer (MANUU) reserves the right to change or vary any part thereof or foreclose the procurement process at any stage. The Buyer also reserves the right to disqualify any vendor, should it be necessary, at any stage.
- 8.4 In case of any dispute, Hyderabad will be the Jurisdiction. The Registrar, Maulana Azad National Urdu University, Hyderabad shall decide the issue and his decision will be final and shall be binding on the both parties.


Registrar

Maulana Azad National Urdu University
Gachibowli, Hyderabad- 500032





PURCHASE & STORES SECTION

Instructions for filling up BOQ (Online Only)

Name of the Bidder/ Bidding Firm / Company :									
PRICE SCHEDULE									
(DOMESTIC TENDERS – RATES ARE TO GIVEN IN RUPEES (INR) ONLY)									
(This BOQ template must not be modified/replaced by the bidder and the same should be uploaded after filling the relevant columns, else the bidder is liable to be rejected for this tender. Bidders are allowed to enter the Bidder Name and Values only)									
NUMBER #	TEXT #	NUMBER #	TEXT #	NUMBER #	NUMBER #	NUMBER #	NUMBER #	NUMBER #	TEXT #
Sl. No.	Item Description	Quantity	Units	BASIC RATE In Figures To be entered by the Bidder in Rs. P	GST Amount on Item Qty x Basic Rate in INR Rs. P	TOTAL AMOUNT Without Taxes col (13) = (4) x (7) in Rs. P	TOTAL AMOUNT With Taxes col (14) = sum (8) to (13) in Rs. P	TOTAL AMOUNT In Words	
1	2	4	5	7	9	13	14	15	

Name of the firm

Unit Price (in Rupees) without GST

Total GST amount (in Rupees) i.e. Qty. x unit price x GST%



PURCHASE & STORES SECTION

Annexure-1 (Technical Bid)

1.	Name of the Firm	M/s.
	Postal Address	
	Contact No (s)	
	E-mail ID	
	Account Number	
	Name of the Account Holder / Firm / Agency	
	Bank Name	
	Branch Name & Details	
	IFSC Code	
2.	Details of EMD of Rs. 75,000/- (Exemption for registering with MSME NSIC etc as per Gol norms will only be considered on production of documentary proof in the concerned category, failing which the bid will be rejected) The EMD shall be submitted at Purchase & Stores Section before closing date.	D.D. No. _____ dated: _____ Bank _____ (upload documentary proof if exemption is claimed)
3.	Firm Registration Details	(Yes / No) (upload Firm registration certificate)
4.	GST Registration Details	(Yes / No) (upload GST registration certificate)
5.	OEM Certificate / authorized dealer / authorized distributor / manufacture's authorization certificate specific to this tender	(Yes / No) (upload Documentary proof)
6.	Compliance report of each items	(Yes / No) (upload compliance report of each item)
7.	Average Annual Turnover of Rs. 12,00,000/- during the preceding three years (Attach scanned copy of audited balance sheet and Profit & Loss Account for these years, Certificate Certified by CA) [as per tender clause 4.6 (A)]	(Yes / No) (upload Documentary proof)
8.	Value of Purchase Orders of UTM (Firewall) / Network security related equipment carried out during the preceding five years, (Attach scanned copy of Purchase Orders indicating amount, date etc.,) [as per tender clause 4.6 (B) & (C)]	(Yes / No) (upload Documentary proof)
9.	Annexure –1 duly filled in	(Yes / No) (upload document)

Declaration:

- That we have not been debarred by any Government Department/Under taking.
- It is hereby declared that the firm have carefully read and understood the tender document and **agreed with all the terms and conditions** of the tender, Hyderabad jurisdiction etc., and agreed that the decision of the University shall be final in all respect.

Place :
Date :2020

Signature of the authorized
Dealer/signatory of the firm



Annexure-2 (Financial Bid)

(To be filled Online as per the CPPP format only)

Name of the Bidder/ Bidding Firm / Company :								
PRICE SCHEDULE								
(DOMESTIC TENDERS – RATES ARE TO GIVEN IN RUPEES (INR) ONLY)								
(This BOQ template must not be modified/replaced by the bidder and the same should be updated after filling the relevant columns, else the bidder is liable to be rejected for this tender. Bidders are allowed to enter the Bidder Name and Values only)								
NUM BER #	TEXT #	NUM BER #	TEXT #	NUMBER #	NUMBER	NUMBER #	NUMBER #	TEXT #
Sl. No.	Item Description	Quantity	Units	BASIC RATE In Figures To be entered by the Bidder in Rs. P	GST Amount on Item Qty x Basic Rate in INR Rs. P	TOTAL AMOUNT Without Taxes col (13) = (4) x (7) in Rs. P	TOTAL AMOUNT With Taxes col (14) = sum (8) to (13) in Rs. P	TOTAL AMOUNT in Words
1	2	4	5	7	9	13	14	15
1	Supply, Installation, Configuration and Commissioning of UTM Firewall with 3 Years Subscription of (Antivirus, Antispam, Web & Application Filter, Intrusion Detection & Prevention plus 24 X 7 Support)	01	Set			0.00	0.00	INR Zero Only
2	Total Price of buyback value of existing running UTM device along with all taxes, duties Model: Fortigate 3040b S.No: FG3K0B3I13700055	01	Set			0.00	0.00	INR Zero Only
Total in Figures (1-2)						0.00	0.00	INR Zero Only
Quoted Rate in Words								



PURCHASE & STORES SECTION

Annexure-3 (Bank Guarantee)

EARNEST MONEY DEPOSIT (EMD) SUBMISSION FORM
(THROUGH BANK GUARANTEE)

(To be executed on non-judicial stamped paper of an appropriate value)

Date :

Bank Guarantee No :

Amount of Guarantee :

Guarantee Period : From to

Guarantee Expiry Date :

Last date of Lodgement :

WHEREAS Maulana Azad National Urdu University, Gachibowli, Hyderabad 500032 (hereinafter referred to as "**The Owner**") which expression shall unless repugnant to the context includes their legal representatives, successors and assigns) has executed a binding to the contract on [insert date of acceptance of the letter of acceptance(LOA)] with [insert name of the Successful Bidder](hereinafter referred to as the "**Contractor**") which expression shall unless repugnant to the context include its legal representatives, successors and permitted assigns) for the EMD for supply and installation of major UTM(Firewall) for Centre for Information Technology shall have the meaning ascribed to it in the Contract] based on the terms & conditions set out in the Tender Documents number [insert reference number of the Tender Documents] dated [insert date of issue of Tender Documents].....and various other documents forming part thereof.

AND WHEREAS one of the conditions of the Contract is that the Contractor shall furnish to the Owner a Bank Guarantee from a commercial bank in India having a branch at Hyderabad for a sum of R...../- (the amount guaranteed under this bank guarantee shall hereinafter be referred to as the "**Guaranteed Amount**") against due and faithful performance of the Contract including the performance bank guarantee obligation and other obligations of the Contractor for the supplies made and the services being provided and executed by under the Contract. This bank guarantee shall be valid from the date hereof up to the expiry of the Contract Period including any extension thereof.

AND WHEREAS the Contractor has approached [insert the name of the commercial bank] (here in after referred to as the "**Bank**") having its registered office at [insert the address].....and at the request of the Contractor and in consideration of the promises made by the Contractor, the Bank has agreed to give such guarantee as hereunder:

- (i) The Bank hereby undertakes to pay under this guarantee, the Guaranteed Amount claimed by the Owner without any further proof or conditions and without demur, reservation, contest, recourse or protest and without any enquiry or notification to the Contractor merely on a demand raised by the Owner stating that the amount claimed is due to the Owner under the Contract. Any such demand made on the Bank by the Owner shall be conclusive as regards the amount due and payable by the Bank under this bank guarantee and the Bank shall pay without any deductions or set offs or counterclaims whatsoever, the total sum claimed by the Owner in such Demand. The Owner shall have the right to make an unlimited number of Demands under this bank guarantee provided that the aggregate of all sums paid to the Owner



PURCHASE & STORES SECTION

- by the Bank under this bank guarantee shall not exceed the Guaranteed Amount. In each case of demand, resulting to change of PBG values, the Owner shall surrender the current PGB to the bank for amendment in price.
- (ii) However, the Bank's liability under this bank guarantee shall be restricted to an amount not exceeding Rs...../-[Rupees..... only].
- (iii) The Owner will have the full liberty without reference to the Bank and without affecting the bank guarantee to postpone for any time or from time to time the exercise of any powers and rights conferred on the Owner under the Contract and to enforce or to forbear endorsing any powers or rights or by reasons of time being given to the contractor which under law relating the Surety would but for the provisions have the effect of releasing the surety.
- (iv) The rights of the Owner to recover the Guaranteed Amount from the Bank in the manner aforesaid will not be affected or suspended by reasons of the fact that any dispute or disputes have been raised by the Contractor and / or that any dispute(s) are pending before any office, tribunal or court in respect of such Guaranteed Amount and/ or the Contract.
- (v) The guarantee herein contained shall not be affected by the liquidation or winding up, dissolution, change of constitution or insolvency of the Contractor but shall in all respects and for all purposes be binding and operative until payment of all money due to the Owner in respect of such liability or liabilities is effected.
- (vi) This bank guarantee shall be governed by and construed in accordance with the laws of the Republic of India and the parties to this bank guarantee hereby submit to the jurisdiction of the Courts of Hyderabad for the purposes of settling any disputes or differences which may arise out of or in connection with this bank guarantee and for the purposes of enforcement under this bank guarantee.
- (vii) All capitalized words used but not defined herein shall have the meanings assigned to them under the Contract.
- (viii) NOTWITHSTANDING anything stated above, the liability of the Bank under this bank guarantee is restricted to the Guaranteed Amount and this bank guarantee shall expire on the expiry of the Warranty Period under the Contract.
- (ix) Unless a Demand under this bank guarantee is filed against the Bank within six (6) months from the date of expiry of this bank guarantee all the rights of the Owner under this bank guarantee shall be forfeited and the Bank shall be relieved and discharged from all liabilities hereunder.
- (x) However, in the opinion of the Owner, if the Contractor's obligations against which this bank guarantee is given are not completed or fully performed by the Contractor within the period prescribed under the Contract, on request of the Contractor, the Bank hereby agrees to further extend the bank guarantee, till the Contractor fulfills its obligations under the Contract.
- (xi) We have the power to issue this bank guarantee in your favour under Memorandum and Article of Association and the Undersigned has full power to do so under the Power of Attorney dated [date of power of attorney to be inserted] granted to him by the Bank.

Date:

Bank
(Corporate Seal of the Bank)
Signature of the person duly authorized
to sign on behalf of the Bank



PURCHASE & STORES SECTION

Annexure-4 (Compliance Report)

S.No	Specification	Compliance (Y/N)	Deviation if any
General Features			
1	Network security appliance should support "Stateful" policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc. Proposed NGFW solution should have WAF(Web Application Firewall) capability.		
2	OEM should be positioned in Gartner's Report – in Magic Quadrant in the leaders/challengers for UTM as per the report for the year 2018-2019		
3	OEM should have technical support centre in India		
4	Should have 3 years 24X7 support warranty & gateway anti-malware, anti spam, anti bot, web & apps protection, Anti-Virus, IPS/IDS, Sandboxing subscription from day 1.		
5	Proposed UTM/NGFW should be NSS lab recommended.		
Hardware & Interface for each Firewall Unit/Appliance			
6	The platform must be supplied with minimum 8 x GE RJ45 inbuilt interfaces, 6 x 1GE SFP interface Slots populated with 5x 1GE SFP Single Mode Transceivers & 2 x 10GE SFP+ interface slots.		
7	Minimum 240 GB SSD local storage		
8	The Appliance should have separate USB & Console Ports		
Performance for each Firewall Unit/Appliance			
9	A Minimum NGFW throughput in real world/production environment (by enabling and measured with application visibility and control utilizing HTTP transactions and traffic mix such as HTTPS, SMTP and other protocols and logging enabled) – 9 Gbps. The bidder shall submit the performance test report from Global Product Engineering department / Global Testing Department/ Global POC team of OEM to certify the mentioned performance.		
10	Concurrent Connection(TCP) – 6 Million		
11	New Connections per Sec - 2 Million		
12	Minimum NG Threat prevention throughput in real world/production environment (by enabling and measured with application visibility and control, NGIPS, Anti-Virus, Anti-Spyware, Anti-Bot and all other security threat prevention features enabled with HTTP transactions and traffic mix such as HTTPS, SMTP and other protocols and logging enabled)– 7 Gbps. The bidder shall submit the performance test report from Global Product Engineering department / Global Testing Department/ Global POC team of OEM to certify the mentioned performance		



PURCHASE & STORES SECTION

13	Minimum IPsec VPN throughput – 9 Gbps		
14	Simultaneous Client-to-Site IPsec VPN tunnels: 1000		
Routing Protocols			
15	Static Routing		
16	Policy Based Routing		
17	The Firewall should support dynamic routing protocol like RIP, OSPF, BGP		
Firewall			
18	Firewall should provide application inspection for LDAP, SIP, H.323, SNMP, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC, IMAP, NFS etc		
19	The firewall should support transparent (Layer 2) firewall or routed (Layer 3) firewall Operation		
20	The Firewall setup should support ISP link load balancing : multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing and granular multipath rule (or) ECMP (Equal cost multipath)		
21	Firewall should support link aggregation functionality to group multiple ports as single port.		
22	Firewall should support static NAT, policy based NAT and PAT		
23	Firewall should support IPsec data encryption		
24	It should support the IPsec VPN for both site-site and remote access VPN		
25	Firewall should support IPsec NAT traversal.		
26	Support for standard access lists and extended access lists to provide supervision and control		
27	Firewall system should support virtual tunnel interfaces to provision route-based IPsec VPN		
28	Firewall system should support Quality of service (QoS)/bandwidth management functionalities.		
29	The Firewall should have integrated solution for SSL VPN		
30	Should support LDAP(OpenLDAP), RADIUS(Freeradius), Windows AD, PKI based Authentication		
Integrated Intrusion Prevention System(IPS)			
31	IPS should have DDoS and DoS anomaly detection and protection mechanism with threshold configuration, Deep packet Inspection and IPS signature-tuning for false positives.		
32	Support SYN detection and protection for both targets and IPS devices.		
33	The device shall allow administrators to create Custom IPS signatures		



PURCHASE & STORES SECTION

34	Should have a built-in Signature and Anomaly based IPS engine on the same unit		
35	Signature based detection using real time updated database & should have minimum 8000+ IPS signature database from day one		
36	Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)		
37	Signature updates do not require reboot of the unit.		
38	Configurable IPS filters to selectively implement signatures based on severity, target (client/server) and operating systems		
39	IPS Actions: Default, monitor, block, reset, or quarantine		
40	Should support packet capture option		
41	IP(s) exemption from specified IPS signatures		
42	Should support IDS sniffer mode		
43	Firewall should support antimalware capabilities , including antivirus, botnet traffic filter, antispysware and sandboxing technology. The solution should have an inbuild Advanced Malware Protection Licence which should be able to protect from zero-day threats like ransomware.		
44	Solution should be able to detect and prevent unique communication patterns used by BOTs i.e. information about botnet family		
45	The solution should support sandboxing for prevention from zero day threats (Proposed unknown malware analysis service with guaranteed protection signature delivery time not more than 10 minutes. Solution must have capabilities to prevent unknown threats)		
46	Should have antivirus protection for protocols like HTTP, HTTPS, IMAPS, POP3S, SMTPS protocols etc.		
47	Solution should have an option of packet capture for further analysis of the incident		
48	Solution should uncover threats hidden in SSL links and communications Including SSL Decryption and SSH Inspection		
49	The AV should scan files that are passing on CIFS protocol		
50	The proposed system shall provide ability to allow, block attachments or downloads according to file extensions and/or file types		
51	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.		
Other Support			
52	Should support features like Web-Filtering, Application-Control & Gateway level DLP from day one		
53	The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should support over 120 Million URLs without external solution, devices or hardware modules.		



PURCHASE & STORES SECTION

54	Should support detection over 3,500+ applications in multiple Categories: Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)		
55	The solution should have the flexibility to write security policies based on IP Address & User Name		
56	QoS features like traffic prioritization, differentiated services,. Should support for QoS features for defining the QoS policies.		
57	It should support the VOIP traffic filtering		
58	Appliance should have identity awareness capabilities		
59	Protection against Reverse proxy,SQL injection protection,Cross-site scripting protection		
60	Solution must support VRRP clustering protocol or equivalent.		
61	Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI.		
62	Support accessible through variety of methods, including console port, Telnet, and SSH		
63	Support for both SNMPv2 and SNMPv2c, providing in-depth visibility into the status of appliances.		
64	Should have capability to import configuration and software files for rapid provisioning and deployment using Trivial File Transfer Protocol (TFTP), HTTP, HTTPS		
65	The proposed solution should have feature for logging & reporting with minimum 1TB of total Log Storing capacity.		
66	The reporting platform must provide option for creating customized reports.		
67	The reporting platform must provide multiple report output types or formats, such as PDF, HTML, and CSV		
68	Should capable to provide a convenient method for alerting administrators when critical events are encountered, by sending e-mail alert messages to administrator defined e-mail addresses		
Others			
70	The bidder/OEM must provide onsite and remote support as and when required		
71	Training of required duration to be provided to corresponding staffs of CIT,MANUU for day to day handling and configuration of the appliances. At least 2 days separate admin level training post installation is mandatory		
72	The buyback cost for the existing device Fortigate 3040b to be adjusted in the price bid		
73	Licence: All the licensing required for the functionalities asked in the tender specification should be included in the offerings.		
74	All the devices should be upgraded to the recent OS free of cost.		



PURCHASE & STORES SECTION

75	SLA: 1. The Initial configuration must be done by OEM Certified Engineer on-site. 2. Onsite as well as remote support as and when required. 3. OEM Warranty for the Entire system along with 24/7 support. 4. In case of Hardware breakdown the damaged hardware components must be replaced within 5 days after initiation of the service request. 5. Hardware should be updated now and then with latest firmware throughout the warranty period. 6. Above item should carry Three years onsite full comprehensive free warranty. 7. Proposed Product Firewall UTM should be supportable back to back warranty/AMC from OEM for at least 3 years after completion of 3 years warranty period.		
----	---	--	--

Place :

Date :2020

Signature of the authorized
Dealer/signatory of the firm