TAMIL NADU OPEN UNIVERSITY

No. 577, Anna Salai, Saidapet, Chennai - 600 015.
Phone: (91-44) 2430 6645 / 6600 Fax: (91-44) 2430 6640
Email : registrar@tnou.ac.in ; website : www.tnou.ac.in

Dr.S.Vijayan
Registrar

File No.TNOU/FIREWALL/LT/2018
Date: 19.01.2018

Sub: TNOU- Admin- Purchase and Installation of Firewall at TNOU - Limited sealed quotations - Invited - Reg.

*****

I am, by direction, to invite limited sealed quotations for purchase and Installation of Firewall as per the specification of work is as per Annexure - I enclosed herewith.

Sl.No	Description of items	Rate Quoted
1	Annexure -I	

In this context, I am to inform that the Tenderer shall enclose the following documents as proof to determine the eligibility criteria :(Application form enclosed as Annexure - II)

i) The Registration Certificate issued by the Government Department concerned.

ii) Proof of experience in this field.

iii) Copy of PAN Card, Proof of Annual Turnover for minimum past 3 years and copy of latest Income-Tax Clearance Certificate/Return.

iv) Interest Free Earnest Money Deposit [EMD] amount of Rs.5,000/- by means of Demand Draft/Bankers Cheque, drawn in favour of 'The Registrar, Tamil Nadu Open University', payable at Chennai.

The successful Tenderer shall remit **5%** of the total cost of the tender amount or **Rs.50,000/-** whichever is higher, towards **INTEREST FREE REFUNDABLE SECURITY DEPOSIT** by means of Demand Draft/Bankers Cheque drawn in favour of **'THE REGISTRAR, TAMIL NADU OPEN UNIVERSITY'**, payable at Chennai, [i.e.] in addition to the Earnest Money Deposit. Both Earnest Money Deposit and Security Deposit are refundable after successful completion of the work done and other tender formalities.

In this context, I am to inform that the last date for submission of the Tender application along with the all requirements on **08.02.2018** upto **3.00 pm**. at the Registrar's Office, Tamil Nadu Open University, Saidapet, Chennai - 600 015.

Pre-bid Meeting is Scheduled on **02.02.2018 at 3.00** PM

The Tender will be opened in the Chamber of the Registrar at **4.00 pm on 08.02.2018** in the presence of the Tenderers or their authorized representatives.

The cost of Tender Form is Rs.590 (Rs.500+ GST 18%). It can be downloaded from our University Website www.tnou.ac.in.

REGISTRAR

ANNEXURE - I

SL.	Specifications	Compliance Yes/NO
1	Integrated Security Appliance which is capable of supporting Firewall, VPN, IPS, Web filtering etc	
2	The device should be IPv6 ready, and should support multi-core architecture.	
4	The device should be appliance based firewall, with ICSA labs (International Computer Security Association) Firewall & Anti virus certification and preferably VPNC (Virtual Network Consortium) featured.	
5	Product Support should be 24x7 and advanced replacement in case of hardware failure.	
6	Vendor & OEM should support the appliance with all necessary upgrade for at least 3 years from the date of purchase installation	
7	Number of network interfaces supported by the device should be mentioned exactly in the Bid. The product should have minimum of 2 x 10-GbE SFP+,4 x 1-GbE SFP, (12) 10/100/1000 copper gigabit, 1 USB, 1 console interface available	
8	Appliance should support Advance threat protection services from day one & there should be unrestricted user licensing with minimum 2 engines.	
9	Appliances should have dedicated management interface	
10	Firewall inspection throughput at least 5.0 Gbps or higher	
11	VPN throughput at least 2.5 Gbps or higher	
12	The Firewall should support at least 1 million concurrent sessions and at least 30,000 new sessions per second.	
13	The devices should not have license restriction on number of users	
14	Should support at least 3000 IPSec Site-to-Site VPN tunnels and 500 or more no of IPSec Client Remote access VPN	
15	Should support at least 500 concurrent SSL VPN users	
16	The firewall should be able to support dynamic load balanacing for outbound data passing through the firewall, if external firewall load balances are required same is to be mentioned.	
17	Dual WAN/ISP Support : Should support automatic ISP failover as well as Isp load sharing and laod balancing for outbound traffic	
18	Traffic management: Option to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy.	
19	Should not have 2nd gen proxy inbuilt on to the appliance to avoid latency	
20	Should support 300 or more VLAN interfaces (802.1P)	
21	Appliance should support IPSec NAT traversal.	
22	Should support OSPF, RIP V1 and V2 routing protocol.	
23	Bandwidth Control/ Restriction per IP Address group & per Policy should be available.	
24	Should support NAT without degrading the performance of the firewall.	
25	Should support authentication using XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, Internal user database, terminal Services, Citrix or TACACS +	

26	Should have Layer 2 bridge or transparent mode	
27	The Firewall should have atleast 1.5 Gbps of IPS throughput or higher.	
28	IPS shall be able to detect incidents that originate from inside the netowrk perimeter as well as from outside the network perimeter and shall be able to take action on the basis of configured policies.	
29	Appliance should have support for DOS & DDOS scanning attacks and attack protection.	
30	The proposed firewall should work in High Availbility Mode and support active/active and active passive	
31	Should do real time scanning or proxy based scanning of all the traffic passing through the appliance.	
32	Signatures should have a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (eg. For severity level: high, medium, low)	
33	Should be able to generate graphical reports on top attacks, source for attack etc.	
34	Should have the option to schdeule reports for automatic generation & email it to admin.	
35	The OEM should have regular update of its attack signature database and the same should be configuarble to update the signatures automatically without manual intervention.	
36	The new attack signatures and new major software releases should be avliable in OEM website for free download.	
37	Should be integrated solution with appliance based firewall on a single chasis.	
38	Should be an ASIC's based or quad core or higher processor based solution for faster processing.	
39	Should have minimum 1.0 Gbps or higher of Anti-Malware inspection throughput.	
	Firewall should be capeable to do inbound and outbound scanning for gateway antivirus and anti spyware.	
40	Antivirus should provide real-time detection of viruses and malicious code at the gateway for SMTP, POP3, HTTP, FTP etc internet traffic and should minimum have 50Million signatures on appliance or cloud based.	
41	The proposed solution should be licensed per unit as against per user.	
42	Should support full DPI throughput of 700 Mbps or higher including Gateway Antivirus	
43	OEM to declare IMIX internet mix for appliance and should not be less than 1.5 Gbps	
44	Antivirus gateway should have option to configure to respond to virus detection in several ways	
45	Automatic Frequent updates of virus pattern files should be available from the vendor without manual intervention	
46	Should have facility to block files based file extensions.	
47	Should be an unlimited user based appliance.	
48	Should have capacity to scan unlimited file size .	

49	The proposed solution should be scaleable and offer fault tolerance to safeguard against hardware failures. The failover should be capable of taking over the traffic without any manual intervention and session loss.	
50	The solution should support load balancing for UTM, for the traffic which needs to be scanned in case appliance fails.	
51	Should have reporting facility to generate reports on virus dedected over different protocols, top sources for viruses, destination for viruses, top viruses etc.	
52	Web content filtering solution should work independently or through an integrated proxy server.	
53	Should have facility to block the URL's based on categories.	
54	URL database should have at least 15 million sites and 50 + categories.	
55	URL database should be updates regularly by the OEM automatically with no reboot after update.	
56	Should be able to block or override using pass phrase with different categories / sites based on users/groups.	
57	Should have facility to configurable policy options to block web sites based on banned words.	
58	Appliance should be able to re rate website into custom URL category.	
59	The solution should support facility to generate reports on virus dedected over different protocols, top sources for viruses, destination for viruses, top viruses etc.	
60	Should have configurable policy options to define the URL exempt list.	
61	The solution shuold be able to block spywares/adwares etc.	
62	The solution should have options to block java applets, active X as well as cookies.	
63	The Solution should have RBL database of known spam sources to validate / check wheather the mail is a spam or not	
64	Solution should have the abilities to block the appliaction not based on port and protocols.	
65	Should support policy based on FQDN, Mac address, along with IP address.	
	should support FQDN based routing on route policy	
66	Logging and reporting solution should be supported.	
67	The solution should generate the reports for the firewall, gateway level AV, IPS web filtering requested.	
68	Should support deep packet SSL to decrypt HTTPS traffic for scanning(IPS,Gateway Antivirus,Content Filtering, Application control) transparently for future requirement and then re-encrypt to send to destination if no threat found.	
69	The solution shall have readymade templets to generate reports like complete reports or attack reports, bandwidth report etc.	
70	The solution should help to analyze/understand attacks over various protocols like HTTP , FTP , SMTP etc.	
71	The solution should help to analyze/understand the live application usage in the network.	

72	Should have options to generate reports in terms of which are the frequent attacks as well as top sources and destination for attacks.	
73	Should have options to generate reports in different formats	
74	The solution should have configurable options to send the reports as a mail to the designated email address	
75	Should have configurable parameters to send alert emails based on event type.	
76	Should have configuarble parameters to set aleart	
77	The solution should have configurable options to schedule the report generation.	
78	The solution should be running its own syslog server or integrated server to collect the logs. If separate server and/or appliance is required for the logging & reporting , the BOM & cost should be included in the proposed solution.	
79	All the UTM functionalities along with IPSEC & SSL VPN fuctionalities should be on single platform.	
80	All the UTM services should be quoted with 3 years support & services .	
81	The OEM should be in the leader/challengers quadrant of gartner latest & being recommended by NSS Labs for atleast 3 years	
82	The proposed solution should have a reporting tool from same OEM external or on device.	

Station : _____

Date : _____

Signature : _____

Name : _____

Designation: _____

& [Seal]

Annexure –II

TAMIL NADU OPEN UNIVERSITY

No. 577, Anna Salai, Saidapet, Chennai – 600 015.
Phone: (91-44) 2430 6645 / 6600 Fax: (91-44) 2430 6640
Email : registrar@tnou.ac.in ; website : www.tnou.ac.in

PARTICULARS REQUIRED IN THE STATEMENT TO BE FURNISHED BY THE TENDERER

Sl.	Details Required	Particulars to be furnished Correctly and legibly
1	Name of the Firm	
	Permanent Address	
		E-mail:
		Land line:
		Mobile:
		Fax:
2	Firm Registration Number & Registration Date *[Enclose copy of the Registration Certificate issued by the Government Department concerned]*	
3	State whether the Firm is a Proprietorship/ Partnership / Private Limited/ Public Limited Concern.	
4	Details of EMD	
5	Details of Cost of Bidding Document	
8	PAN / TAN Card Details *[Enclose copy of the Certificate]*	
9	GST / VAT Details *[Enclose copy of the Certificate]*	
10	Service Tax Registration Details *[Enclose copy of the Registration Certificate]*	
11	Income Tax Return Statement (Last 3 years) *[Enclose copy each of the remittance particulars with clearance the Statement]*	

12	Audited statement from Chartered Accountant (Last 2 years) *[Enclose copy of the Statement]*	
13	ISO 9001 - 2008 Certificate (Mention Date of Expiry of Certificate) *[Enclose copy of the Certificate]*	
14	Proof of Experience & List of Clients indicating quantum of work executed with them *[Enclose copy of the Certificate]*	
15	Any Experience in dealing with Govt. Departments *[Enclose copy of the Certificate]*	
16	Whether the firm is blacklisted by any Government Department of any criminal case is registered against the firm or its owner / partners anywhere in India	
17	Company Profile *[Enclose copy of the Profile]*	

DECLARATION

[i] I/We declare hereby that the particulars furnished in the above statement are true to the best of my/our knowledge.

[ii] The rate(s) quoted in the statement above is/are my/our competitive rate(s) for the Purchase and Installation of Firewall at TNOU concerned.

[iii] I/We have thoroughly studied the Terms and Conditions of the Tender and also abide by the University Rules.

[iv] I/We will abide to the procedures and formalities of the University in finalizing and selecting the limited suppliers/tenderers as per the discretion of the authorities.

[v] I/We agree that the University reserves the rights to accept or reject the limited tenders partly or fully without assigning any reasons as per the discretion of the authorities.

Station : _____

Date : _____

Signature : _____

Name : _____

Designation: _____

& [Seal]

Check List Enclosures: (Please write the page number in all documents)

Sl	Name of the Enclosure	Page No (From – To)