Government of National Capital Territory of Delhi
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Bawana Road, Delhi-110042

EXPRESSION OF INTEREST DTU//CC/2018-19/53

Delhi Technological University (formerly Delhi College of Engineering) is a non-affiliating, teaching and research University at Delhi to facilitate and promote studies, research, technology incubation, product innovation and extension of work in Science, Technology and Management Education and also to achieve excellence in higher technical education. Currently, university is offering B. Tech. Courses, M.Tech courses, Ph.D courses and scholarships and Teaching-cum-Research Fellowships. In addition, a School of Management has also been established within the university campus to cater for MBA program.

DTU invites "Expression of Interest (EOI) for Network Security Solution" in the university.

Procedure for submission of EOI: Vendors proposing to submit EOI, kindly visit university website at www.dtu.ac.in for downloading full document of EOI including details of Scope of Work and the desired prerequisites. Any amendment/ update to the EOI or its Terms & Conditions will be uploaded on official websites of the University. The EOI be submitted in the prescribed format along with all supporting documents in compliance with the requirements of EOI. The companies will be short listed after detailed presentations by them before the designated Committee. The dates for presentations shall be informed/ notified individually and on University website.

Technical & financial bid will be invited through tender process only from those who meet the desired requirements and short-listed.

EOI may be sent in triplicate in a sealed envelope duly super scribed 'Expression of Interest for "**Network Security Solution of DTU**" either by registered post or personally, addressed to Assistant Registrar (S&P), Room No. 104, Admn. Block, Delhi Technological University, Shahbad Daulatpur, Bawana Road, Delhi – 110042. The university reserves the right to accept or reject any or all the EOIs at any stage of the process or any of the terms without assigning any reason. No correspondence in this regard shall be entertained. The closing date for receiving EOI is 17.06.2019 till 1500 hrs. and same shall be opened at 1530 hrs. on 17.06.2019.

Assistant Registrar (S&P)

DELHI TECHNOLOGICAL UNIVERSITY

Notice inviting Expression of Interest for Network Security Solution
at

DTU

Dated:17.05.2019

Delhi Technological University,
Formerly Delhi College of Engineering,
Shahbad Daulatpur,
Main Bawana Road,
Delhi – 110042

Document Name	Notice Inviting Expression of Interest for Network Security Solution of DTU.
Document Reference Number	DTU/CC/EOI/2018-19/53
Date of issue of EOI notice	17.05.2019
Opening of EOI notice	17.06.2019 (03:30 P.M)
Last date for receiving queries and date of responder(s) conference. Potential responders should make sure that they qualify all criteria as per EOI as only representatives of eligible companies will be allowed to attend the conference	17.06.2019 (03:00 P.M)
Last date for submission of EOI response	17.06.2019 (03:00 PM)
Cost of EOI	Downloadable from DTU website : Free

Note: The bidder must submit the response both in hard copy and two soft copies on CD either in person or in sealed envelope sent through registered post or speed post or in person addressed to Assistant Registrar (S&P) Delhi Technological University, Formerly Delhi College of Engineering, Room No. 104, Admn. Block, Shahbad Daulatpur, Bawana Road, Delhi – 110042 before the mentioned date and time of submission.

The envelope containing the EOI Response to be super scribed with the title "Expression of Interest for Network Security Solution of DTU".

Venue for Conference: Senate Hall, 2nd Floor, Admn. Block, DTU.

EOI for Network Security Solution of DTU.

1. SCOPE OF WORK

Objective: The objective of present work is EOI for Network Security Solution of DTU.

DTU has its present infrastructure of Network security and wants to update as per currently available solution to handle all types of threats, intrusion, etc.

Technical specification of firewall requirements are as mentioned below:

1. Firewall appliance should have at least 6 x 1GE interfaces and 4 x 10G SFP + SR interfaces + 1 out of band management interface. The Solution must have dedicated Data Plane and Management Plane.
2. Firewall should support minimum 5,000 concurrent users.
3. The solution should support minimum 8 Gbps of Threat Prevention (FW + IPS + AVC + AV+ Antimalware +Antispyware + Sandboxing + logging) throughput for Enterprise Mix and Production Mix with all enabled up-to-date security signatures
4. Firewall should integrate with LDAP for user authentication. Log should have user login details in report for web/application access.
5. Firewall should have provision to manually block any LDAP user.
6. The Firewall should have hot swappable fan tray.
7. The proposed system shall be able to operate on Tap mode to only report, Transparent (bridge) mode to minimize interruption to existing network infrastructure and NAT/Route mode. All modes should also be available concurrently without using Virtual Contexts.
8. Solution should be able to decrypt SSH and SSL inbound and outbound traffic to detect and block any unauthorized or malicious traffic over encrypted session. SSH and SSL inspection should not have dependencies on (atleast) port 22 and 443 respectively to work. Solution should be able to decrypt SSL on any port.
9. The proposed solution should support Virtualization. Minimum 10 Virtual Firewall license should be provided on day 1
10. The application signatures shall be automatically updated. Administrator should be able to configure schedule for download and install
11. System should have the capability to dynamically handle block source based on malware reputation.
12. To prevent evasive users and applications from bypassing security functions, all product functions for IPS, Threat Prevention, and Anti-Virus, shall not require specific software port and protocol combinations for detection, mitigation, or enforcement.
13. The Antivirus engine of the solution must be provided by the OEM itself and must not depend on a third party OEM for signatures. Any third party AV engine if used by the solution must be mentioned.
14. Solution shall prevent attack using identification of phishing URL and provide multifactor authentication for critical resources. Credential theft function should allow admin to define detection policies based on URL categories.
15. Solution should support consumption of malicious IP, bad Domain and malicious URL by integrating with third party using external block list with capability to auto update and use latest data in security policies. Firewall should be able to integrate with minimum 10 such lists by HTTPS method.
16. Solution should include capability to integrate with third party threat feed vendors to automatically consume, process and provide output of malicious IP, URL, Domain so

that can be integrated with firewall dynamic list. Should have default integration with minimum 10 threat feed vendors.

17. Proposed solution must include capability to send unknown files to sandbox server from day 1. Once malware is identified the firewall must receive automated signature update from sandbox server. OEM must furnish public link and public document to prove the claim.
18. The proposed solution shall support sandbox behavior based inspection and protection of unknown viruses and zero-day malware for HTTP, HTTPS, SMTP, FTP, IMAP, POP3 protocols.
19. Solution should support Session/Packet based load sharing over multiple ISP links of different bandwidth. It should work with both static and dynamic routing. Solution must support minimum 2 ISP links.
20. Firewall should have minimum 1TB RAID storage in Firewall and to have additional capability of minimum 1Tb storage for logging, analysis, and reporting into a dedicated system for delivering increased knowledge of security events throughout the network for centralized security event analysis and reporting. Reporting device can be dedicated appliance or inbuilt in firewall.
21. Solution support configuration and security updates as per OEM best practice recommendation.
22. The proposed solution must allow policy rule creation for application control, user based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS.
23. The proposed solution must be in the Leader's quadrant in Gartner Magic Quadrant of Enterprise Firewalls for at-least 2 years.
24. The confirmation to all above mentioned feature and specification must be listed in documents available on Public domain such as datasheet published on website. Confirmation on letterhead would not be acceptable.

Vendor will provide onsite technical experts for training of DTU personnel and rectification of problems during the complete period as mentioned in work order.

EOI for Network Security Solution of DTU.

3. Guiding Principles

DTU being an institution which has created and adopted best practices across its organizational operations, it expects all its partners also to follow the same. In view of this, DTU has framed the following guiding principles to be adhered by interested participants. The best practices may be more than what are specified below:

- The proposed solution should be an integrated, Scalable, Modular and Highly Available.
- The proposed solution must implement a multi-level security across various tiers and software layers of the IT platform.
- Best practices from the industry must be implemented across the tiers and layers of the proposed solution.

3.1 Software Support and Maintenance Practices

Software support and maintenance for a period of five years post implementation of security solution is mandatory and part of the scope of work of the proposed solution. The selected bidder must ensure that the technology / platform of the proposed solution (application and system included) be of the latest version as published by the OEM (where applicable) and made available at no extra cost to the institute.

3.2 Software Licensing

The institute would require various software licenses (OEM or otherwise) to be made available for use enterprise wide and is not specific to any user level.

3.3 Setup and Commissioning

Installation, Setup and Commissioning of the system along with the portfolio applications will be part of the scope of work. Ensure that all non-functional requirements are catered to and will be part of the design and the proposed solution.

3.4 Documentation

Providing all design, documents, user and operational manual.

4. Eligibility Criteria/Prequalification

The bidder must possess the requisite experience, strength and capabilities for providing the services necessary to meet the requirements, as described in the EOI document. The bidder must also possess the technical know-how and the financial wherewithal that would be required to successfully provide the complete solution along with support services sought by DTU. The bids must be complete in all respect and should cover the entire scope of work as stipulated in the EOI document. The invitation to bid is open to all bidders who qualify the eligibility criteria as given below. Eligibility criteria are mandatory and any deviation in the same will attract bid disqualification.

S.No.	Criteria	Document to be provided
1.	The bidder should be a company registered under the Companies Act, 1956	Certificate of incorporation
2.	The bidder must have successfully implemented at least one similar examination system in University/Govt. institute of repute having at least 5000 student's registration.	Documentary proof from earlier institute/university where the project was completed. List of successfully completed projects indicating cost & customer name. The proof should be applicable to the responder only and not for its sister concern or subsidiary or parent company.
3.	Bidder must have ISO 9001:2000 and ISO 27001 or other such certification	Valid Copy of Certificate
4.	The bidder or each member in case of a consortium should have positive net worth and an annual turnover of more than INR 10 Crore or above for the last three Financial Years.	Practicing Chartered Accountant Certificate for Net worth and Copy of the audited balance sheet of the company for last 03 years.
5.	The Bidder should not be under a Declaration of Ineligibility or black listed with any of the Government/ Public sector unit Agencies	Self-Declaration from Authorized Signatory of the Bidder
6.	The responder shall be the single point of contact for DTU and shall be solely responsible for the all warranties, upgrades and guarantees etc. Offered by the OEM etc. An undertaking to this effect should	Self-certification
7.	Having minimum manpower strength of 50	List of employees

8.	Having at least 06 years' experience of handling big project of network security implementation solutions	
9.	Having Set-up/ Office in Delhi	
10.	Able to provide total integration & solution	Self-certification
11.	Agreeable to sign SLA documents	

EOI for Network Security Solution of DTU.

5. EOI Submission

The bidder must submit a Demand Draft (DD) for the value of INR 1500/-(Rupees One Thousand Five Hundred Only) along with the EOI Response. The DD should be in favor Ior "Registrar, Delhi Technological University" payable at Delhi / New Delhi. This is a non-refundable amount.

6. Bid Evaluation process

All responses including the proposed solution(s) received by DTU shall be evaluated by an evaluation committee duly constituted by DTU, on the basis of eligibility criteria mentioned in this document. The responders may be called to present the solution date, time and venue to be communicated to them at least seven days in advance. Only the eligible bidders will be informed of their selection. The RFP will be issued only to eligible bidders.

DTU shall be at liberty to reject any response received from any company or consortium for the Expression of interest in reply of notice inviting Expression of Interest dated 17/06/2019.

Annexure-A

7. Annexure

7.1. Annexure A- Checklist for response submission

The following check-list must be filled in and submitted with the response

Description	Response	If yes, mention page no.
Have you provided the EOI Response containing the details mentioned in the document?	Yes/No	
Have you provided the documentation proof of being a ISO 27001 certified organization?	Yes/No	
Have you submitted the undertaking pertaining to the single point of contact? (on firms letter head)	Yes/No	
Have you attached documents pertaining to similar work experience?	Yes/No	
Have you attached the documents pertaining to 6 years of company's incorporation?	Yes/No	
Have you attached audited balance sheets for last three years	Yes/No	
Have you submitted the DD for INR 1,500/- in favor of Registrar, DTU toward EOI submission?	Yes/No	
Have you submitted all documents as per **eligibility criteria/prequalification**	Yes/No	

7.2. EOI response form

To be submitted with EOI response

Note: Details filled in this form must be accompanied by sufficient documentary evidence, in order to verify the authenticity and correctness of the information.

S. No.	Description	Details (To be filled in by the responder to the EOI)
1.	Name of the Company	
2.	Official address	
3.	Phone No. and Fax No.	
4.	Corporate Headquarters Address	
5.	Phone No. and Fax No.	
6.	E-Mail address of contact person	
7.	Web Site Address	
8.	Details of Company's Registration (Please enclose attested copies)	
9.	Name of Registration Authority	
10.	Registration Number and Year of Registration	
11.	Product/ Service For which Registered with validity period	
12.	GST Registration No.	
13.	Permanent Account Number (PAN)	
14.	Whether the company complies with the Requirement under the Contract Labour (Regulation and Abolition) Act	
15.	Name of Bankers along with Branch (as appearing in MICR Cheque) & Account	
16.	Name of the Authorized Signatory, who is authorized to respond to the EOI	
17.	Others documents provided	

7.3 Annexure B

The following notes offer guidance to proposing responder in the form of a model outline for their response document. All the headings indicated below must be addressed in the sequence shown, providing as much relevant detail as possible. (Conformance to this outline will assist the subsequent evaluation and selection activities, and any variations should be documented).

Additional headings and information may be provided by the proposing responder where they are required to include additional details or explanations.

Description of the proposing responder:

I. Specifically include legal status, ownership, and the name of the person within the company who is responsible for this project.

II. The proposing responder's general understanding of the project requirements and the proposed total solution.

III. The main features of the proposed solution and any areas of financial, operational, development risks that are perceived.

IV. Upgrade and technology refresh strategy for the proposed solution.

V. Describe the strategy suggested for future upgrade of the supplied equipment and / or products and any impact this strategy may have on operation etc.

VI. Scope of work compliance as per the document.

7.4. Annexure C

UNDERTAKING
(To be submitted by the responder on the responder's letter head)

I/We hereby undertake that I/We have studied and understood the Expression of Interest document completely.

I/We hereby undertake that I/We understand that the Section Scope of Work and Requirement of this EOI is indicative only and not exhaustive in any manner and that the final scope of work and technical specification will be decided by DTU at their discretion.

I/We hereby undertake that I/We understand that the DTU reserves the right to finalize the scope of work and requirements at its discretion, which may be based on my/or proposed solution and/or any other responder's proposed solution and/or as decided by the DTU. I/We hereby declare that I/We shall not be having any claim and/or right for the said usage. I/We hereby undertake to provide the requisite OEM authorization as and when required and/or asked for by DTU, as per the solution and/or requirements, as decided by DTU at their discretion.

I/We hereby undertake that I/We hereby undertake that I/We understand that the DTU reserves the right to float a separate tender for the scope of work and requirements as mentioned above of this EOI irrespective of the outcome of this EOI. I/We understand that in such a case I/We shall bid separately for that tender and in no case our response to this EOI shall be deemed as a bid for the said tender.

I/We hereby undertake that the DTU reserves the right to short list responder(s) for further tendering of this EOI and in case of my/our response being rejected I/We shall have no claim of any short in the further tendering process. Further DTU shall be at liberty to allow any company to respond in the tender process at the stage for "Request for Proposal" irrespective of the fact that the company allowed has participated in the EOI or not and I/We shall have no claim of any sort on such process.

I/We hereby undertake that we shall comply with the scope of work and requirements and there are no deviations of any manner in this regard from my/our side.

I/We hereby undertake that in case my/our response to this EOI is short listed I/We agree to bid for the further tender as and when asked for by DTU based on the terms and conditions and technical specifications and scope of work as finalized and decided by the DTU at their discretion.

I/We undertake to be the single point of contact for DTU and shall be solely responsible for all warranties, upgrades, and guarantees etc. offered by the OEM, and system integration and facilities management and for the entire scope of work and requirements
as per the service levels defined in the subsequent tender document.

I/ We here by affirm that our response is valid for a period of 180 days from the date of EOI submission.

EOI for Network Security Solution of DTU.