Indian Institute of Technology, Kharagpur
Kharagpur 721 302, WB, India

Sub: Procurement of Security Devices (02 nos.)

Ref: Tender Notice No. IIT/CIC/IT/SECURITY/2017-18/38 Dated 24.11.2017

Indian Institute of Technology Kharagpur, an Institute of National Importance, invites sealed bids from reputed **Original Equipment Manufacturers (OEMs)** OR **their Authorized System Integrators** who have adequate credential for supplying, installing and maintaining similar product in IITs or similar Autonomous Institutions /Universities, Government /Public Sector Undertakings, etc., for procurement of two numbers UTM (Unified Threat Management) or NGFW (Next Generation Firewalls) devices with **five years** comprehensive onsite warranty.

Interested vendors are requested to send their sealed bids under a **two cover system** as per requirement mentioned in tender document, along with the Technical Specifications & Compliance Certificate (as mentioned in **Specification Annexure I)** and the required quantities as specified in tender document.

Details are also mentioned in the Institute website **www.iitkgp.ac.in** [link: tenders].

There will be a **pre bid meeting which will be held on 01.12.2017 at 3:30PM** in the Office of the Head, Computer and Informatics Centre, IIT Kharagpur. The final quotation for consideration is to be sent after the pre bid in a sealed packet, containing two separate sealed envelopes (**Technical Bid** and **Price Bid**) duly superscripted with Reference Number (Tender Notice No. **IIT/CIC/IT/SECURITY/2017-18/38 Dated 24.11.2017),** to the Office of the **Head, Computer & Informatics Centre, Indian Institute of Technology, Kharagpur, P.O. Kharagpur Technology, PIN : 721 302 on or before 19 December 2017 by 3:00PM.**

The **technical bids (should also contain detailed un-priced bill of material) which will be opened on 19 December 2017 by 3:30PM** in the presence of the vendors and their authorized representatives and price bids will be opened (to be notified separately), only of those firms, who will be found technically qualified/shortlisted, after evaluation of their technical bids.

Head
Computer & Informatics Centre

Copy to:
1. Newspaper
2. Institute website
3. CPPP
4. Notice Board

PROCUREMENT OF TWO SECURITY DEVICES TO REPLACE TWO EXISTING CISCO ASA-5580 FIREWALLS

Introduction

A part of the internet traffic originating from the Institute campus network is flowing through two Cisco ASA-5580 firewalls working in active-standby mode to the internet gateway of National Knowledge Network (NKN). Institute is in the process of replacing the existing Cisco ASA-5580 firewalls by hardware appliances for perimeter security solution with the following minimum services.

a) Firewall protection in High Availability mode with 2 Gbps application throughput and 1 Gbps threat prevention throughput with comprehensive standard functionality such as Application wise classification, Implementation of policies for different IP Subnets, users and group of users, site to site and site to end user VPN, Logging, Reporting, etc.

b) Authentication for particular IP subnets or group of users (user id based) from which traffic to be channeled through it. This will enable the option to channel the traffic from the specific user/ specific subnets to the Internet directly.

c) 5 years Threat prevention subscription for full featured IPS, anti-malware and command-and-control protection, including protection from zero-day threats.

d) 5 years URL filtering to enforce web browsing policies.

e) Access logging.

1. Scope of work:

I. The scope of the work includes supply, successful installation/integration/migration and commissioning of the two Security devices by replacing the existing Cisco ASA-5580 firewalls and maintenance of the entire solution for a **period of five years** in terms of onsite comprehensive warranty and necessary subscription charges.

II. The participating bidders are requested to visit the site during pre-bid for a clear understanding of the existing setup as selected bidder must be able to migrate the path from existing ASA 5580 firewalls to the new security devices within 6 hours on an Institute holiday.

III. Complete delivery of the material has to be accomplished within **Six Weeks** of receipt of the purchase order.

IV. Prior to delivery bidder has to arrange hands-on training (at any metro city of India) for two Institute nominated Network/System Engineers for a period of 5 days at free of cost. Boarding, lodging and transport for the Institute nominated Network/System Engineers will be arranged by Institute. Selected Vendor can also arrange demo boxes at IIT Kharagpur and conduct the onsite training to the Institute nominated five Network/System Engineers for five days (exclusive of time taken to setup the Proof of Concept).

V. Prior to the delivery a pre installation document has to be prepared by the selected bidder in coordination with the trained Institute nominated Network/System Engineers such that entire project can be completed within **two weeks** of the delivery.

VI. Time taken from the date of purchase order to the date of commissioning and smooth migration from existing setup to new setup is the essence of the project. Entire project has to be completed **within eight weeks** without disturbing the regular operation of Institute network.

VII. The warranty period will start after the acceptance of the installation and certification by Head, CIC, IIT Kharagpur (i.e. from the date of commissioning).

VIII. The acceptance of the installation and certification by Head, CIC, IIT Kharagpur are subject to meeting all functionalities specified in Annexure-I.

IX. Replacement of defective equipment and shipment of the same should be the responsibility of the selected vendor without any financial commitment from IIT Kharagpur. The same has to be completed within five working days**.**

X. In case of any future expansion / up-gradation necessary changes in the configuration has to be done by the selected vendor for smooth integration / migration.

XI. All necessary documentation related to time-to-time configuration has to done by the selected vendor.

XII. The vendor will be liable for any hardware and software up-gradation for maintenance without any extra cost during warranty period.

XIII. The vendor should supply all required hardware and software to meet the requirement of this project. Part bid will not be entertained.

XIV. The vendor has to resolve any hardware/software problem during installation and integration of the security device with the existing Campus Network.

2. Bidder Pre-Qualification Criteria:

Criteria	Documents Required	Remarks
The bidder should have minimum 3 years of working experience in the domain of network security and should have at least 3 orders of more than 50 Lakhs in total from any government/PSU/ PSU Banks or reputed private organization in last 3 years.	Purchase Order Copies	Only orders issued directly to the bidding entity will be considered
The bidder should have a minimum turnover of Rs. 20 Crores per annum during last three financial years.	Audited Balance sheet	
The bidder should be a profit making entity for the last 3 years	Audited P&L report	
The bidder should not have been blacklisted by any Government departments/PSU/PSE on the date of submission of this RFP.	A declaration from the Company Secy.	
The bidder should have valid ISO Certification	Valid Certificates	
The security device must be of enterprise class which should be	Declaration from OEM should be submitted	

declared by the OEM and the quoted products should not be under end of sales or end of support in next five years from the date of submission.		

3. OEM Pre-Qualification Criteria:

Criteria	Documents Required	Remarks
OEM TAC and RMA Depot should be in India	Documentary proof from OEM	
OEM should have Industry presence for more than 5 years	Documentary proof from OEM	
OEM should be NASDAQ listed company	Documentary proof from OEM	
Emergency response team should be available on 24 x 7 basis from OEM directly in case of malfunctioning of the device and changes in its functionalities	Documentary proof from OEM	

4. General Terms & Conditions:

I. **Last Date of Submission of Sealed Bids: 19.12.2017 by 3:00 pm (**In the Office of the Head, Computer & Informatics Centre, Indian Institute of Technology Kharagpur).

II. **Date of opening of the Technical Bids: 19.12.2017 at 3:30 pm (**In the Office of the Head, Computer & Informatics Centre, Indian Institute of Technology Kharagpur).

III. The technical bid should contain the technical solution as per the requirement of the tender document and Annexure-I**.** Unpriced Bill of Materials should be attached mentioning the model number and relevant part numbers for each component.

IV. Technical bid should contain the tender document signed by authorized signatory of the bidder as a token of acceptance of specifications, requirements and terms and conditions.

V. The capabilities, operating characteristics and other technical details of the hardware and software offered should be furnished together with product brochures, literature, etc. in the technical bid. The bidder should confirm in writing that the software versions being quoted if any are latest.

VI. Technical bid should contain all relevant technical details; printed technical leaflet of models quoted and other details, which may be necessary to ensure that offer is complete in all, respect e.g. technical specification, delivery period, guarantee period, validity, etc.

VII. Technical bid should also contain a **signed "compliance certificate" (Specification Annexure – I)** duly signed by the bidder.

VIII. The authorization letter issued by the OEM (specifically against this tender) should be enclosed in original.

IX. If necessary, the vendor may be required to give presentation/demonstration on the systems offered as well as arrange site visit, where vendor has installed and integrated similar solution.

X. Complete delivery of the material has to be accomplished within **Six Weeks** of receipt of the purchase order, failing which Liquidation Damage (LD) @ 1% per month of the total order value will be imposed as per Institute purchase rules. Total liquidated damage will be capped at 5% of the PO value.

XI. The installation would be deemed as complete, when all the components (hardware, software and accessories etc.) are supplied, installed and implemented as per the technical specifications and integrated with the existing campus network and all the features as mentioned in the technical specifications in the tender are demonstrated and/or implemented to the satisfaction of IIT, Kharagpur.

XII. **Warranty & Maintenance:** The vendor should give warranty for **five years** from the final installation date of the security device. During the warranty period, the vendor will undertake the comprehensive maintenance of the security device (hardware, software and accessories supplied by them).

XIII. **Payment Terms:** 90% payment will be made after the successful installation and commissioning of the security device. Balance 10% of the payment will be made on submission of Bank Guarantee of 10% of the total purchase value valid for a period of five years and three months.

XIV. **Price:** Price should be quoted only in Indian Rupees on free delivery at site inclusive of all taxes and incidental charges. Tax component must be shown separately.

XV. Custom Duty Exemption Certificate/Excise Duty Exemption Certificate/Way Bill will be issued to the Selected Bidders as applicable in Institute rules.

XVI. **Tender Fee:** An amount of **Rs. 10,000.00** (Rupees ten thousand only) as tender fee (non refundable) has to be paid. The payment shall be made by Demand Draft from any Bank in favour of “Indian Institute of Technology Kharagpur”, payable at “Kharagpur”. Quotation will not be accepted without the Tender Fee. Tender fee should be enclosed separately in an envelope and stapled with the Technical Bid.

XVII. **Earnest Money Deposit (EMD)**: An amount of **Rs. 1,50,000.00** (Rupees One Lakh and fifty thousand only) in the form of Demand Draft/Bank Guarantee (as per format in Annexure – II) to be enclosed along with the technical bid. The E.M.D. will be drawn in favour of “Indian Institute of Technology Kharagpur”, payable at “Kharagpur”. The validity of the EMD should be 6 (six) months from the date of issue. Any bid without EMD will not be considered. This will be refunded to the unsuccessful vendors within 15 working days after completion of the purchase procedures. The EMD will be refunded to the selected vendor after successful execution of the Purchase Order. The Institute reserves the right to withhold or confiscate the EMD in the event of failure to supply the items in part or full, once the Purchase Order is accepted. E.M.D. should be enclosed with the Technical Bid documents. No interest is payable on refund of EMD.

XVIII. Conditional Offer or part bid will not be accepted.

XIX. **Period of Validity:** Bids shall remain valid for acceptance for a period of 120 days from the date of opening of the price bid but any benefit for downward revision of prices should be extended to the IIT Authority.

XX. Past Performance of the Vendors will be judged at the time of Technical evaluation.

XXI. Bidders should enclose the following documents in the technical bid as proof of their credential:

- ❖ Certificate of Registration
- ❖ Current Income Tax, PAN Number, GST registration
- ❖ Banker's Solvency Certificate.
- ❖ Summary of Audited Statement of Accounts for the last three years.
- ❖ A write up on deployment planning, manpower support for this tender, service and maintenance capability, mitigation of risks or breakdown and replacement capability, with the escalation support matrix proposed for the Institute. Vendors must indicate their sales and support service center in India and their plan to address issues about services.
- ❖ Signed Tender document as a token of acceptance for the Terms & Conditions specified in various sections of the Tender Document

5. Acceptance of Tender

I. The Institute does not bind itself to offer any explanation to those bidders whose technical bids have not been found acceptable by the Evaluation.

II. The Institute does not bind itself to accept the lowest tender and reserves the right to reject any or the entire tender received without assigning any reason thereof.

III. The bids (technical and price bids) once submitted shall be the property of the Institute and shall not be returned to the vendor in future.

IV. A bid submitted with false information will not only be rejected but the vendor may also be debarred from participation in future tendering processes.

V. Canvassing in any form not only invites disqualification in this tender but also debar the vendor participation in the future tendering processes.

VI. The person/officer signing the tender/bid documents should be delegated with an appropriate Power of Attorney (essentially endorsed by a Notary Public) by the Chief Executive Office/MD of the Company, to sign such documents.

VII. **Opening of Price Bids:** The Price Bid(s) of only those vendor(s) who are found technically qualified will be opened. The date and time will be informed separately.

VIII. Authorized representative (with proper authorization letter to attend opening of technical bids and also for opening of price bids) may choose to be present at the time of opening of Technical Bids/Price Bids.

IX. Director may accept or reject any or all the bids in part or in full without assigning any reason and does not bind himself to accept the lowest bid. The Institute at its discretion may change the quantity/upgrade the criteria/drop any item or part thereof at any time before placing the Purchase Order. In case of any dispute, the decision of the Director of this Institute shall be final and binding on the bidders.

X. In case of any dispute or differences, breach and violation relating to the terms of this agreement, the said dispute or difference shall be referred to the sole arbitration of Director of IIT Kharagpur (IIT) or any other person appointed by him. The award of the arbitrator shall be final and binding on both the parties..

XI. This Tender Document and the Contract shall be governed by and interpreted in accordance with Laws in force in India. The Courts at Midnapur shall have exclusive jurisdiction in all matters arising under the contract.

For any query pertaining to this tender, correspondence may be addressed to:

The Head, Computer & Informatics Centre
Indian Institute of Technology, Kharagpur-721 302
Email: head@cc.iitkgp.ernet.in

In case the due date for submission and/or opening of the tender happens to be a holiday, the same will be accepted on the next working day. The timings will however remain unchanged. Please Note that the Institute remains closed during Saturdays & Sundays.

6. Price Bid Format

SL.NO	Item Description	Part No.	Quantity	Unit Price (INR)	Taxes in INR	Total Price (INR)
1						
:						
:						
Total Price of 2 nos. security devices with 5 years Comprehensive Onsite Warranty with all necessary subscription charges						

ANNEXURE- I

SPECIFICATION OF SECURITY APPLIANCE

Sl No.	Specification	Compliance (Yes/No)	Remarks (if any)
1	The proposed security device should be hardware appliance		
2	**Appliance throughput and interfaces**		
2.1	Firewall throughput of 2 Gbps or higher and Threat prevention throughput should be of 1 Gbps or higher		
2.2	IP-Sec-VPN Throughput 300 Mbps or higher		
2.3	New session per second 40,000 or higher		
2.4	Maximum Session 2,50,000 or higher		
2.5	Interface support from day 1 • Minimum 8 x 1G SFP Interfaces • Minimum 12 x 10/100/1000 copper Interfaces • Dedicated HA ports in addition to requested data ports		
3	**Power Supply** Single AC power supply		
4	**Disk drive** Capacity based on log retention support for one year (minimum 100 GB)		
5	**High Availability** Should support Active/Active and Active/Passive mode		
6	**Interface** The proposed firewall should support Dual Stack IPv4 / IPv6 application control and threat inspection support in a way to access data flowing across a computer network		
6.1	The deployment should allow passive monitoring of traffic flows across a network by way of a switch SPAN or mirror port in Transparent mode (IPS), Layer 3 and should be able to mix multiple modes		
General Requirement			
7	**Firewall Features**		
7.1	Should be Identity based firewall		
7.2	Must be able to support Network Address Translation (NAT) and Port Address Translation (PAT) for a pool of IP-address and for specific subnets		
7.3	Should support the following routing protocols: - Static		

	- RIP v2 - OSPFv2/v3 with graceful restart - BGP v4 with graceful restart - Policy-based forwarding - PIM-SM, PIM-SSM, IGMP v1, v2, and v3		
7.4	Needs to classify all applications, across all ports, all the time, regardless of port, encryption (SSL or SSH) or technique used to evade detection. Application classification is needed along with other Layer 7 controls, like User-ID		
7.5	Should allow to setup basic QoS, controlling traffic leaving the firewall according to the network or subnet, and extend the power of QoS to also classify and shape traffic according to application and user		
7.6	Should have User/IP/MAC binding functionality to map username & IP address & MAC address		
8.0	**IPS Features**		
8.1	Should have capabilities to Inspect and apply policy to encrypted traffic (SSL or SSH), both inbound and outbound		
8.2	Should have the capability to control the transfer of sensitive data patterns, including credit card and social security numbers in application content or attachments		
8.3	Should be able to detect & prevent bot infected machines		
8.4	Should be able to detect & prevent unique communication patterns used by bots i.e. Information about botnet family		
8.5	Should be able to detect & prevent attack types i.e., such as spam sending click fraud or self-distribution, that are associated with bots		
8.6	Should be able to block traffic between infected host and remote operator and not to legitimate destination		
8.7	Should block vulnerability exploits, buffer overflows and port scans. Additional capabilities, like blocking invalid or malformed packets, IP defragmentation, TCP reassembly, protect users from the evasion and obfuscation methods used by attackers.		
8.8	The appliance vulnerability based signatures needs to be updated weekly and should provide protection from a range of exploits in a short span of time		
8.9	The appliance threat signatures should be applied for applications with no dependence on port for inbound and outbound traffic. It should allow policy-based SSL decryption to ensure the IPS functionality over the encrypted traffic		
8.10	The appliance should detect known malware as well as unknown variations of known malware families and block in-line at very high speeds		
8.11	Should be able to stop malicious outbound		

	communications stemming from malware infections, passively analyzes DNS queries, and identifies the unique patterns of botnets		
8.12	The appliance should have sandboxing feature inbuilt		
8.13	Should support detection & prevention of cryptors & ransmoware viruses and variants (cryptlocker, cryptoWall etc.) through use of static and/or dynamic analysis		
9	**Gateway Antivirus, AntiSpyWare and Antispam Features**		
9.1	Should be able to detect and remove Virus, Worm and Trojan		
9.2	Should be able to protect from Phishing, Spyware and Malware		
8.3	The virus signature database update should be automatic		
9.4	The appliance Antispam feature should be able to block illegitimate mail traffic via Real-Time blacklist, via MIME header check		
9.5	Should be able to redirect spam mails to dedicated email address to detect false positivity. At the same time it should be able to generate customized spam notification to the users		
9.6	The appliance should be equipped with Zero hour Virus outbreak and Spam protection via Recurrent pattern Detection technology		
10	**Web Content & Application Filtering Features**		
10.1	The solution be able to filter and block URL, Keyword, File type, Java applets, Cookies, ActiveX, Malware, Phishing, Pharming URL, P2P application, Anonymous Proxies etc.		
10.2	It should have the customized blocking and white listing capability of URLs		
10.3	The URL filtering database should be updated with newly discovered malicious URLs every 60 minutes. The URL filtering database should have the total control over web-related activity		
10.4	The solution should be able to control granular access to sites that fall under dangerous categories and prevent downloads from these sites. It should be able to generate automated warning message for users, or restrict access altogether		
10.5	Should be able to detect and protect against SQL Injection, Cross Site Scripting (XSS), Session Hijacking, URL tampering, Cookie Poisoning of organization portals		
11	**Bandwidth Management Features**		
11.1	Should be able to maintain and control/restrict		

	bandwidth on a per application, per user and per user-group basis		
11.2	Should have application and user identity based bandwidth management capability		
11.3	Should support multiple VLAN bandwidth management		
11.4	Should guarantee burstable bandwidth policy		
12	**Appliance Reporting Features**		
12.1	The logs should show overall traffic in details per application wise, per user wise and per user group wise		
12.2	Should show in details about threat, suspicious activity, alerts, url and data filter, viruses and spams		
12.3	Should allow creating the custom reports, based on our needs		
12.4	The centralized management console and reporting should provide clear indications that highlight regulations with serious indications of potential breaches with respect to access policies, intrusion, malwares, bot, url, applications etc.		
13	**User Identification and Authentication Features**		
13.1	Should have capability to Integrate with a wide range of user identity repositories so that policies can follow users and groups regardless of their location. The User repositories should support external directory servers, SQL databases etc.		
13.2	Should support the following authentication protocols: • LDAP – Radius (vendor specific attributes) • Token-based solutions (i.e. Secure-ID),- Kerberos • NTLM		
13.3	Should support user authentication via Active Directory, RADIUS, LDAP, Captive Portals etc.		
13.4	Should support both per user basis and per subnet basis authentication control		
13.5	Should support logging of authentication requests with IP details		
14	**VPN Features**		
14.1	Should have the capabilities to setup site-to-site tunnels over Ipv4/Ipv6. Should allow remote users to setup a secure remote access or virtual private network (VPN) connectivity to Institute network.		
15	**APT Protection Features**		
15.1	The appliance should allow detailed behavioral		

	analysis to understand how newly discovered malware operates, and enable us to quickly identify infected users and investigate potential breaches with detailed analysis of and visibility into unknown threat events		
15.2	Once a new threat is uncovered, it should allow to generate automatic protections across the attack and then it should be delivered to our firewall with-in five minutes		
15.3	The APT subscription should be enabled to prevent attacks based on global threat intelligence without the headache of having to implement and manage separate devices for web and email at every ingress/egress point within institute network		
16	**Comprehensive subscription of security appliance for 5 years**		
16.1	Web/URL Filtering		
16.2	Gateway Antivirus, Spyware, Malware, Proxy Avoidance		
16.3	RBL		
16.4	Content and application filtering		
16.5	IPS		
16.6	APT		
16.7	Reporting and logging		
16.8	VPN users		
17	**Certification**		
17.1	EAL4 +		

ANNEXURE- II

MODEL BANK GUARANTEE FORMAT FOR FURNISHING EMD

Whereas……(thereinafter called the "tenderer") has submitted their offer dated ……for the supply of ……(hereinafter called the "tender") against the purchaser's tender Notice No. …… KNOW ALL MEN by these presents that WE ……..……of ……having our registered office at …….. are bound unto …….. (hereinafter called the "Purchaser") in the sum of ……for which payment will and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this ……Day of ……..… 20 ……

THE CONDITIONS OF THIS OBLIGATION ARE

(1) If the tenderer withdraws or amends, impairs or derogates from the tender in any respect within the period of validity of this tender.

(2) If the tenderer having been notified of the acceptance of his tender by the Purchaser during the period of its validity:

(a) If the tenderer fails to furnish the Performance Security for the due performance of the contract.

(b) Fails or refuses to accept/execute the contract.

WE undertake to pay the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of one or both the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including 45 days after the period of tender validity and any demand in respect thereof should reach the Bank not later than the above date.

(Signature of the authorized officer of the Bank)
Name and designation of the officer
Seal, name & address of the Bank and
Address of the Branch