The Institution of Engineers (India)

AN ISO 9001: 2015 CERTIFIED ORGANISATION
(ESTABLISHED 1920, INCORPORATED BY ROYAL CHARTER 1935)
8 GOKHALE ROAD, KOLKATA - 700 020

A Century of Service to the Nation

No. T- 1665 13.12.2019

NOTICE INVITING TENDER

Sealed Tenders in Single Stage two Envelope Bid system are invited for **Supply & Installation of Unified Threat Management Devices.**

The tender document to be downloaded from the website of The Institution of Engineers (India) (www.ieindia.org).

The sealed tenders are to be submitted in prescribed format duly stamped and signed and dated on each page of **Part 'A' & 'B'** as their unconditional acceptance to the terms prescribed by the Institution. Details/supporting documents wherever applicable, if attached with the tender should be duly authenticated by the vendor/s. No over-writings shall be accepted unless authenticated with full signature of the vendor/s.

The tender shall be in two parts viz. **Technical Bid - (Envelope - 'A')** and **Financial Bid (Envelope -'B')** (Envelope 'A' and 'B' with the content shall be clearly marked on the top of the envelopes separately).

Technical Bid - (Envelope - 'A') shall comprise of compliance documents against Qualification Requirement, Earnest Money Deposit of Rs. 5,000/- and other documents in support of technical capability. The Technical bid should not contain any financial indication, violation of which will invite disqualification. **Financial Bid** shall comprise of quoted price only in the format provided with the tender document in **Envelope - 'B'**. Both **Envelope - A & B** shall be put in a **third envelope**, sealed and submitted within the prescribed date & time and with signature of the tenderer over it.

The sealed tender duly superscribed, **"Supply & Installation of Unified Threat Management Devices."** with Tender No. should be addressed to Director (Administration), sent at the Institution's address either by registered post/speed post/or by hand. Postal / couriered tender must reach to this office within time and date **i.e. up to 16-00 hrs on 30.12.2019.**

Tenders received after the stipulated date and time shall not be entertained. The Institution shall not be liable for any postal delays what so ever and tender received after the stipulated time/date are liable to be rejected summarily without giving any reason and any correspondence.

(Shukla Das)
Director (Administration)

NAME OF JOB: SUPPLY & INSTALATION OF UNIFIED THREAT MANAGEMENT DEVICES

T-1665

Signature of tenderer with date

TECHNICAL PART (ENVELOPE - A)

Qualification Criteria for Installation of Unified Threat Management Device:

The Eligible bidder should satisfy the below mentioned criteria and should submit valid documentary evidence for the below mentioned points:

1. The bidder should be a company registered under the Companies Act, 1956 and submit the following:

    a. Copy of Certificate of Incorporation
    b. Copy of Memorandum & Articles of Association

2. The bidder should submit the following:

    a. Self certified copies of the audited balance sheet and profit & loss statement for the last 3 completed financial years
    b. Copy of PAN Card
    c. Copy of GST registration certificate

3. The bidder should have executed (during last 5 years) at least 5 such projects for implementation of UTM devise.
4. Bidder should have experience of implementing group wise bandwidth management for the users of an Active Directory though the UTM.
5. Bidder has to submit their clientele.
6. Bidder should be authorized partner / service provider of the UTM manufactures
7. The bidder must have single fully functional contact support centre with 24 X 7 support.
8. Bidder must ensure Single point of contact for troubleshooting or a helpdesk team will function as a single point of contact for all sorts of problem for this system.
9. Bidder have to assist Institution with proper support, if required, in case there is change in Internet connectivity.

Guidelines on Bid submission:

1. The language of the documentation & details in the Bids must be in English.

2. All bids to be submitted in single stage two envelopes in separate covers.
    i) Technical Bid :- Envelope A should be superscribed Tender No and Name of Job and word "**TECHNICAL BID**" along with earnest money in envelope A
    ii) Financial Bid :- Envelope should be superscribed Tender No and Name of Job and word "**FINANCIAL BID**" containing rate coated by the party duly signed by authorized representative.

3. These two bids to be placed in separately large envelope superscribed with Tender No and Name of Job

4. **Earnest Money Deposit: Rs 5000**/- (Rs Ten thousand) only by way of demand draft in favour of The Institution of Engineers (India) payable at Kolkata, to submitted along with Technical Bid in envelope A. Envelope A not containing earnest money shall be rejected and Financial Bid shall not be considered further.

5. **Security Deposit:** 10% of the total product value (adjusting from the Earnest Money Deposit) shall be retained as security deposit during performance warranty period which is one year. However, same shall be released after expiry of warranty period if no outstanding complain is on record on performance of the system. Penalty against non-performance shall be realized from the security deposit.

Signature of tenderer with date

Technical Compliance for UTM (Unified Threat Management):

S.No	Specification & General Requirements
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.
2	The proposed vendor must have successfully completed NSS Labs' NGFW Methodology v9.0 testing with a minimum exploit blocking rate of 98%
3	Proposed vendor must be in Leader quadrant of Gartner Magic Quadrant for Enterprise Firewall as per the latest report
4	Firewall should be ICSA labs certified
Hardware & Interface requirements	
1	The platform must be supplied with minimum 14 x 1GE RJ45 inbuilt interfaces & 4 x 1GE SFP interface slots from day one
2	The Appliance should have USB & Console Ports
Performance and Availability	
1	Minimum 15 Gbps Firewall throughput, 1,500,000 concurrent sessions, and 130,000 new sessions per second support from day one
2	Minimum IPS throughput of 2000 Mbps for real world traffic or enterprise mix traffic
3	Minimum Threat Prevention Throughput (measured with Firewall, Application Control, IPS & Malware Protection enabled) of 1200 Mbps for real world or enterprise mix traffic
4	IPSec VPN throughput: minimum 3000 Mbps
5	Simultaneous IPSec VPN tunnels: 500
6	Proposed solution must support minimum 200 SSL VPN users from day one
7	Proposed solution must support minimum 10 virtual firewall from day one
Routing Protocols	
1	Static Routing
2	Policy Based Routing
3	The Firewall should support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, RIPng
Firewall Features	
1	Firewall should provide application inspection for LDAP, SIP, H.323, SNMP, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, IMAP, NFS etc
2	IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP
3	Allows secure deployment of next-generation IPv6 networks, as well as hybrid environments that require simultaneous, dual stack support of IPv4 and IPv6
4	The firewall should support transparent (Layer 2) firewall or routed (Layer 3) firewall Operation
5	The Firewall should support ISP link load balancing.
6	Firewall should support link aggregation functionality to group multiple ports as single port.
7	Firewall should support minimum VLANS 1024

Signature of tenderer with date

8	Firewall should support static NAT, policy based NAT and PAT
9	Firewall should support IPSec data encryption
10	It should support the IPSec VPN for both site-site and remote access VPN
11	Firewall should support IPSec NAT traversal.
12	control SNMP access through the use of SNMP and MD5 authentication.
13	Firewall system should support virtual tunnel interfaces to provision route-based IPSec VPN
14	The Firewall should have integrated solution for SSL VPN
15	It should support the authentication protocols RADIUS, LDAP, TACACS, and PKI methods
Integrated IPS Features Set	
1	IPS should have DDoS and DoS anomaly detection and protection mechanism with threshold configuration.
2	Support SYN detection and protection for both targets and IPS devices.
3	The device shall allow administrators to create Custom IPS signatures
4	Should have a built-in Signature and Anomaly based IPS engine on the same unit
5	Signature based detection using real time updated database & should have minimum 10000+ IPS signature database from day one
6	Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)
7	Signature updates do not require reboot of the unit.
8	Configurable IPS filters to selectively implement signatures based on severity, target (client/server) and operating systems
9	IPS Actions: Default, monitor, block, reset, or quarantine
10	Should support packet capture option
11	IP(s) exemption from specified IPS signatures
12	Should support IDS sniffer mode
AntiVirus & AntiBot	
1	Firewall should support antimalware capabilities , including antivirus, botnet traffic filter and antispyware
2	Solution should be able to detect and prevent unique communication patterns used by BOTs i.e. information about botnet family
3	The solution should support cloud based sandboxing for prevention from zero day threats
4	Should have antivirus protection for protocols like HTTP, HTTPS, IMAPS, POP3S, SMTPS protocols etc.
5	Solution should have an option of packet capture for further analysis of the incident
6	Solution should uncover threats hidden in SSL links and communications with a minimum SSL Inspection Throughput of 600 Mbps
7	The AV should scan files that are passing on CIFS protocol

Signature of tenderer with date

8	The proposed system shall provide ability to allow, block attachments or downloads according to file extensions and/or file types
9	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	
1	Should support features like Web-Filtering, Application-Control & Gateway level DLP from day one
2	The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should support over 250 million web pages in 70+ categories without external solution, devices or hardware modules.
3	Should support detection over 4,000+ 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)
4	The solution should have the flexibility to write security policies based on IP Address, User Name & endpoint operating system
5	QoS features like traffic prioritization, differentiated services,. Should support for QoS features for defining the QoS policies.
6	It should support the VOIP traffic filtering
7	Appliance siould have identity awareness capabilities
8	The firewall must support Active-Active as well as Active-Passive redundancy.
9	Solution must support VRRP clustering protocol.
Management & Reporting functionality	
1	Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI.
2	Support accessible through variety of methods, including console port, Telnet, and SSHv2
3	Support for both SNMPv2 and SNMPv2c, providing in-depth visibility into the status of appliances.
4	Should have capability to import configuration and software files for rapid provisioning and deployment using Trivial File Transfer Protocol (TFTP), HTTP, HTTPS
5	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
6	The solution should provide log storing facility on the cloud with minimum one year log retention capability for generating reports from day one
7	Solution must allow administrator to choose to login in read only or read-write mode
8	All users logs with URL details shall be available for reporting as per the following criteria - a) Category wise b) User wise c) IP wise d) Bandwidth wise e) Device wise

Signature of tenderer with date

Scope of Work for UTM (Unified Threat Management):

1. The vendor has to install the UTM in the premises of the Institution of Engineers (India), HQ
2. The vendor has to configure the firewall and other security features of UTM.
3. The vendor has to implement the group wise bandwidth management for the users of an Active Directory though the UTM
4. The vendor has to configure the UTM for generating the reports.
5. The vendor has to ensure the updation of UTM in respect of all software related patches/ updates.
4. The vendor must provide single fully functional contact support centre with 24 X 7 support.
5. The vendor must ensure Single point of contact for troubleshooting or a helpdesk team will function as a single point of contact for all sorts of problem for this system.
6. The vendor have to assist Institution with proper support, if required, in case there is change in Internet connectivity.
7. Vendor has to mention the Escalation procedure and matrix for customer complaints
8. Any fault in the UTM will need to be resolved by the vendor within 4 hours of fault booking.
9. Incase of hardware failure the vendor has to provide a standby UTM device within 72 hours of diagnosis of problem as hardware fault.
10. If the problem not resolved within the 4 hours then penalty will be charged @ Rs 2000/- per day to the Vendor. The same penalty will be applicable if a stand by UTM device is not provided in case of hardware failure.
11. Training to be provided by the vendors to the IEI personnel for performing day to day operation of the device.
12. The vendor has to provide onsite support, when required.
13. The vendor has to ensure one year full support and warranty.

Commercial Terms and Conditions:

- Payment within one month from the date of satisfactory completion of job.
- Standard LD clause for delay in supply/completion of job 2% per week subject to max 10%
- Receipt of material is subject to inspection.

Signature of tenderer with date

FINANCIAL PART (ENVELOPE - B)

SUPPLY & INSTALATION OF UNIFIED THREAT MANAGEMENT DEVICES

Sl No	Description of Item /Work	Basic Rate (Rs)	GST (Rs)
1	Unified Threat Management (as per technical details and specification quoted in Envelope A)		
2			
3			
4			
5			
6			
7			
	Total		

(Rupees in words..)

Date:

Signature of the Tenderer with date and seal

Name of the Company:

Address with PIN Code:

Phone number & e-mail id: