INDIAN INSTITUTE OF MANAGEMENT BODH GAYA
Directorate of Distance Education Building
Magadh University Campus, Bodh Gaya
Bihar- 824234

NOTICE INVITING TENDER

Tender No: NIT/IIM Bodh Gaya/Firewall/05/2017-18 Dated 24.08.2017

Sealed quotations are invited from the bonafied vendors having experience and exposure in similar nature of work as per prescribed format mentioned below.

Sl	Description of Work	Qty	Unit price	Applicable Taxes (GST)	Total Price
1.	NGFW UTM with all related accessories & support pack as per Annexure-A	2 Nos.			
2.	NGFW UTM Licenses for 3 years	2 Nos.			
3.	Installation of above equipment				
	Total				

Note:

- All rates should be in INR.
- The selected vendor has to rectify all damages occur during the execution of the work at his own cost.

Eligibility Criteria of the Bidder:

- Bidders (OEM /Authorized distributors/SI) in India are allowed to bid for the items as mentioned in the tender document. Manufacturer's authorization letter (MAL) from OEM(s) clearly indicating that the bidder is competent to sell & provide services for the items.
- Bidder should be experience in these field and at least 3 years in IT field on software/hardware/ networking.
- Last 3 years turnover should not be less than 50 Lakhs in each year.
- Bidder should submit the relevant experience documents of similar field in education sector in every items/ technology. They need to submit a single order of above 10 Lakhs on similar field within 2 Years.
- Bidder should submit the relevant documents of the "post sales service team" details along with experience & certificate with Bio-Data, which should be minimum 2 persons.
- Bidder should have submitted all OEM certificate (MAF letter) along with the technical bid.
- Team leader of the entire project should be knowledgeable on similar field on technical ground & value added service & need to present the entire system after "receiving the eligible letter of technical evaluations".
- Bidder should be ISO Certified.
- Bidder must submit copy of the trade license, PAN, GST registration along with the bid.
- Bidder should mention the problem escalation matrix.
- Bidder should submit the logical diagram in paper of the above two-appliance.

Terms & Conditions:

Time: Time allowed for the execution of the work is to be maintained strictly. Unless there is a compelling situation, extension of time will not be considered. Time is the essence of the contract.

Price: Price must be quoted in rupees and is inclusive of all taxes/duties/charges.

Delivery & Installation: Delivery of materials and installation at IIM Bodh Gaya must be done within 6 weeks from the date of issuance of purchase order. The rates should be inclusive of delivery charges at IIM Bodh Gaya.

Equipment Warranty: Three years from the date of installation.

Service Warranty: Three years from the date of installation.

Payment: Payment will be made after successful completion of the work & satisfactory certificate from IIM Bodh Gaya. The scope of work mentioned in the BOQ is indicative in nature and payment will be made based on actual quantities of work done at site.

Security Deposit: 10% of the billed value will be retained as Security Deposit for a period of 1 year (defect liability period) from the date of completion of the work.

Earnest Money Deposit (EMD): At the rate equal to 2% of the offered value as per tender, by Demand Draft in favor of "Indian Institute Management Bodh Gaya" and payable at Kolkata. Earnest Money Deposits are to be submitted in the form of Demand Draft on any scheduled bank in separate envelope, which will be opened first. Without proper EMD, no offers will be considered and opened. Under no circumstances, any other documents excepting Demand Draft will be considered as valid EMD.

Quality: Quality of the project is of utmost importance. This shall be adhered to in accordance with the provisions of relevant specifications and guidelines given in the relevant paragraphs of tender document and/or as per the standard practice.

Validity: The rate must be valid for three months from the date of opening of tender.

Risk Purchase: In case of supplier's failure to deliver the ordered item(s) as per stipulated time schedule, IIM Bodh Gaya reserves the right to cancel the order by serving notice instantly and in such case, EMD deposited by the selected vendor will be forfeited in the credit of IIM Bodh Gaya.

Jurisdiction: All questions, disputes and/or differences arising under and out of, or in connection with the contact, if not concluded, shall be referred to the High Court at Calcutta or any other court in the district of 24 Parganas (South).

Documents need to be submitted with Technical BID:

1. Signed copy of the original bid documents
2. Details of the company as per documents
3. Signed copy of the terms & conditions
4. All relevant documents/certificate against "Eligibility Criteria"
5. Technical Compliance Acceptance report
6. OEM authorisation letter
7. Make & Model of the appliance with DATA Sheet

Tender document sealed and signed in each page along with EMD must be submitted at the office of Senior Administrative Officer, IIM Calcutta latest by **14.9.2017 before 2.00 p.m**

Tender/ quotation must be address to:

Senior Administrative Officer (Purchase)
Indian Institute of Management Calcutta
P.O. Joka, Diamond Harbour Road,
Kolkata-700104

Quotation must be titled **"Procurement of Firewall for IIM Bodh Gaya."** on the top of the envelop. Quotations received incomplete and/or conditional are liable to summarily rejected without any further reference.

The Institute reserves the right to modify the requirements and reject any on all tenders wholly or partly without assigning any reason thereof.

Senior Administrative Officer (Purchase), IIM Calcutta &
Convener (Purchase Committee), IIM Bodh Gaya

INDIAN INSTITUTE OF MANAGEMENT BODH GAYA

Annexure - A

NGFW Router & VPN Functionalities with UTM Features (Security)			
Sl.No.	**Specification**	**Compliance(Y/N)**	**Remarks / Deviation**
A.	**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 ASIC Based Firewall should be ICSA Labs certified for ICSA 4.0 and EAL 4 certified or equivalent of EAL4		
3	All the UTM functionalities like antivirus, ips, ipsec & ssl vpn should be ICSA certified		
4	The platform should be based on real-time, secure embedded operating system		
5	Should provide a Http, Https, SSH, Telnet, SNMP based management console for managing and configuring various components of the appliance		
6	Should support minimum 10 virtual systems (The product must support layer 7-based UTM/Firewall virtualization, and all the UTM features should be supported in each virtual firewall like thread prevention, ips, web filter, application control, content filtering etc.)		
7	The device should belong to a family of products that attains IPv6 Ready Phase 2 & IPv6 Certification		
8	The Appliances/Solution should support basic server load balancing functionalities		
9	OEM should be in Leaders quadrant of Gartner's – in Enterprise Firewall Magic Quadrant, as per the latest report of 2017.		
10	Should support HA		
B.	**Networking & System Performance Requirements:**		
1	The Firewall should support a minimum of 8x 1GE RJ45 interfaces & 6x 1GE SFP Interface slots & 2x 10GE SFP+ Interface slots from day one		
2	The platform should support the standards based Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.		
3	The Firewall should support IEEE 802.1q VLAN Tagging with about 2048 VLANs supported (in NAT/Route mode)		
4	Should support automatic ISP failover as well as ISP load sharing for outbound traffic		

5	The Firewall should support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, RIPng		
6	The Firewall should support Static, Policy Based, and Multicast routing		
7	The Firewall should support throughputs of 20 Gbps or better		
8	The firewall should support VPN throughput of at least 5 Gbps		
9	The Firewall should support minimum 2Gbps of Threat Prevention throughput (measured with Firewall + IPS + App-Control + Malware-Protection enabled on real world traffic or enterprise mix traffic)		
10	should support concurrent session at least 5,000,000		
11	Should support new session per second at least 250,000		
12	The solution should have minimum 8GB of RAM from day one		
C.	**Operating System & Management Requirements:**		
1	Be proprietary to prevent inheriting common OS vulnerabilities		
2	Allow multiple OS firmware image for booting options		
3	Upgradeable via Web UI or TFTP		
4	Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI, SSH, Console Port etc.		
5	Should support SNMPv1, SNMPv2, SNMPv3		
6	The system shall support profile base login account administration, offering granular access control such as only to Policy Configuration & Log Data Access		
7	The proposed system shall be able to limit remote management access from certain trusted network or host with corresponding administrator account		
8	The administrator authentication shall be facilitated by local database, PKI & remote services such as Radius, LDAP and TACAS+		
9	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		
D.	**Firewall Requirements:**		
1	The Firewall should support deployment modes as; “Route Mode" or "Transparent Mode”		
2	The proposed system should have integrated Traffic Shaping / QoS functionality		

3	Should support Static Routes & Policy Based Routing		
4	Should support IPv6 ACL to implement security Policy for IPv6 traffic		
5	All protocols should be supported like TCP/IP, PPTP, RTP/ L2TP, IPSec / GRE, DES, 3DES, AES, PPPoE, FTP, HTTP, HTTPS, SNMP, SMTP, DHCP, DNS		
6	Allows secure deployment of next-generation IPv6 networks, as well as hybrid environments that require simultaneous, dual stack support of IPv4 and IPv6		
7	The proposed system should have integrated Enterprise-class static URL Filtering solution with minimum capacity of 50000 URL entries		
E.	**High Availability Requirements:**		
1	The firewall must support Active-Active as well as Active-Passive redundancy.		
2	The Firewall must support state-full clustering of multiple active firewalls, and the firewalls must load balance the traffic between them to share the load.		
3	The cluster should support simple and minimal downtime during upgrade		
F.	**VPN Requirements:**		
1	The proposed system shall comply/support industry standards, L2TP, PPTP, IPSEC, and SSL VPN without additional external solution, hardware or modules:		
2	The device shall support for IPSEC (DES, 3DES, AES) encryption/decryption & SSL encryption/decryption		
3	The system shall support the following IPSEC VPN capabilities:		
3.1	Supports NAT traversal		
3.2	Supports Extended Authentication		
3.3	Supports Hub and Spoke architecture		
3.4	Supports Redundant gateway architecture		
4	The solution should support 6,000 client-to-site IPSec VPN tunnels from day one		
5	The Firewall should be integrated solution for SSL VPN & should support minimum 3000 SSL VPN users from day one		
6	The proposed solution shall allow administrators to create multiple bookmarks to add to a group and make these bookmarks available for SSL-VPN users.		
G.	**Security (UTM & NGFW) Features**		
	1) IPS Policies :		
	IPS should have DDoS and DoS anomaly detection and protection mechanism with threshold		

	configuration.		
	Filter based selection: Category, Severity, Platform and Target (Client/Server)		
	User-based policy creation		
	Should have a built-in Signature and Anomaly based IPS engine on the same unit		
	Signature based detection using real time updated database & should have minimum 10000+ IPS signature database from day one & also shall allow administrators to create Custom IPS signatures		
	Security Policy based on end-point operating system		
	2) Application Filtering :		
	Solution should be able to detect and prevent unique communication patterns used by BOTs i.e. information about botnet family		
	Control over 3,000+ Applications classified in 18 Categories		
	Filter based selection: Category, Risk Level, Characteristics and Technology		
	Schedule-based access control		
	Visibility and Controls for HTTPS based Micro-Apps like Facebook chat, YouTube video upload		
	Custom application signature support		
	3) Web Filtering :		
	On-Cloud Web Categorization		
	Controls based on URL, Keyword and File type		
	Block Malware, Phishing, Pharming URLs		
	Block Java Applets, Cookies, Google Cache pages		
	Data leakage prevention & block HTTP and HTTPS upload from day one		
	Country Blocking		
	Solutions should support 2 billion web-page		
	Group Based Access		
	Schedule-based access control		
	Botnet server IP blocking with global IP reputation database		
	4) Gateway Anti-Virus & Anti-Spyware :		
	Virus, Worm, Trojan Detection and Removal		
	Spyware, Malware, Phishing protection		
	Scans HTTP/S, FTP, SMTP/S, POP3, IMAP, VPN Tunnels		
	Customize individual user scanning		
	Scan and deliver by file size		
	Block by file types		
	5) Gateway Anti-Spam :		
	Inbound and Outbound Scanning		
	The proposed system shall provide ability to allow or block attachments or downloads according to file extensions and/or file types		
	Filter based on message header, size, sender, recipient		

	Option to treat Windows executables in email attachments as viruses		
	IP Reputation based Spam filtering		
	6) Country-based Traffic Control		
	7) Access Scheduling		
	8) Policy based Routing, Source and Destination NAT		
	9) DoS and DDoS attack Prevention		
	10) Spoof Prevention		