JUDICIAL ACADEMY, ASSAM

Hajo Road, National Law University Campus, Amingaon, Guwahati-781031
Fax :-(0361) 2458247# 2548649, 2458247**E-mail** :- ja@assam.gov.in

SHORT TENDER NOTICE

Sealed quotations affixing Court fee stamp of **Rs.8.25** (non refundable) are invited from GEM/GST registered/approved dealers/suppliers at Guwahati for supply, installation and maintenance of a Unified Threat Management (UTM) device with the following specifications:

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 v8.0 testing with a minimum exploit blocking rate of 99%
3	Proposed vendor must be in Leader quadrant of Gartner Magic Quadrant for Enterprise Firewall as per the latest two reports i.e. of 2017 & 2018
4	Appliance shall be ICSA certified for Firewall, IPS, Gateway AntiVirus, IPSec VPN, SSL VPN functionalities
Hardware & Interface requirements	
1	Minimum 12 x 1GE RJ45 inbuilt interfaces, dedicated 2 x 1GE RJ45 WAN slots from day one
2	The Appliance should have 1x USB, 1x dedicated Console Port
Performance and Availability	
1	The Firewall should be on multiprocessor based architecture with minimum 7 Gbps of Firewall throughput for 1518 byte packet size, 2,000,000 concurrent sessions, and 30,000 new sessions per second support from day one and Firewall Latency should not be more than 3 µs
2	Minimum IPS throughput of 500 Mbps for real world traffic or enterprise mix traffic
3	Minimum Threat Prevention Throughput (measured with Firewall, Application Control, IPS & Malware Protection enabled) of 200 Mbps for real world or enterprise mix traffic
4	IPSec VPN throughput: minimum 3500 Mbps
5	Simultaneous IPSec VPN tunnels: 500
6	Should have 200 SSL VPN peer support 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 like RIP, OSPF, BGP, ISIS

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 2048
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	Should support LDAP, RADIUS, Windows AD, PKI based Authentication & should have integrated 2-Factor Authentication server support & this two factor authentication can be used for VPN users for accessing internal network from outside and for Local users accessing internet from inside the network and for administrative access to the appliance or all of them
16	The solution should have basic server load balancing functionality as an inbuilt feature
17	Licensing should be a per device and not user or IP based (should support unlimited users)
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

Anti Virus& Anti Bot	
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	Solution should be able to block traffic between infected host and remote operator and not to legitimate destination
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
7	The AV should scan files that are passing on CIFS protocol
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 webpages in 72+ categories and 68+ languages without external solution, devices or hardware modules.
3	Should support detection over 3,000+ 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 product must supports Layer-7 based UTM/Firewall virtualization, and all UTM features should be supported in each virtual firewall like Threat Prevention, IPS, Web filter, Application Control, content filtering etc.
5	The solution should have the flexibility to write security policies based on IP Address & User Name & Endpoint Operating System
6	QoS features like traffic prioritization, differentiated services,. Should support for QoS features for defining the QoS policies.
7	It should support the VOIP traffic filtering
8	Appliance should have identity awareness capabilities
9	The firewall must support Active-Active as well as Active-Passive redundancy.
10	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	Solution must allow administrator to choose to login in read only or read-write mode
Warranty and vendor support	
1	Five years on-site warranty
2	The successful bidder have to install and integrate the UTM with the NKN connectivity available in the Academy with the assistance of NIC NOC, Dispur.

Quotations in sealed covers, complete in all respect along with processing fee of **Rs.1000/-** only (non-refundable) by way of Bank Draft in favour of "**Director, Judicial Academy, Assam**" should reach the undersigned on or before **05.05.2019** during office hours.

Bidders should submit the Manufacturer Authorization Form (MAF) of the quoted item duly signed by the authorized signatory. Documentary evidence for tie-ups/ techno-commercial collaboration with subsystems/ peripheral manufacturers to be submitted. A letter from each such subsystems/ peripheral manufacturer needs to be furnished ensuring the support for 5 years.

Bidders should provide escalation matrix for their sales & support function. The bidder must have a strong (24X 7) telephone/web based customer care cell and complaint registration mechanism.

The successful bidder have to deposit Security Deposit of **Rs.10,000/-** only (refundable) in favour of "**Director, Judicial Academy, Assam**"

The successful bidder has to submit a Performance Bank Guarantee @ 5% of the total bill amount for a period of five years in favour of "**Director, Judicial Academy, Assam**", at the time of bill submission.

By order
22/02/19.
(N.G. Das)
Administrative Officer
Judicial Academy, Assam

Memo No.JAA.22/2018/3032-33 **Dated Guwahati, the 22nd February, 2019**
Copy to:-

(1) The Systems Analyst / Programmer,Gauhati High Court. He is requested to up-load the Notification in the Website of Judicial Academy, Assam.
(2) Notice Board of Judicial Academy, Assam.

22/02/19'
Administrative Officer
Judicial Academy, Assam