Rajiv Gandhi Institute of Technology, Kottayam

No. D3/2380/17/RIT

Dated: 24.11.2017

TENDER SCHEDULE

Superscription	: Tender No.D3/2380/17/RIT, Upgrading the firewall by purchasing a new one with three year licence and support under buy back scheme.
Last date and time receipt of tender	: 30/12/2017 1 p.m
Date and time of opening of tender	: 30/12/2017 2 p.m
Last date and time of sale of tender form	: 29/12/2017 1 P.M
Date upto which the rates are to be firm	: 30/06/2018
Cost of tender form	: **Original Rs.1008/- including GST** **Duplicate Rs.560/- -do-** **By Post Rs.1043/-including GST & postal charges**
Address of the Officer from whom Tender Forms are to be obtained to whom tenders are to be send	: THE PRINCIPAL, RJIV GANDHI INSTITUTE OF TECHNOLOGY, KOTTAYAM, VELLOOR P.O, PAMPADY, KOTTAYAM, KERALA, PIN - 686 501

List of Items Required

Details of items	Quantity
1 List attached	

RAJIV GANDHI INSTITUTE OF TECHNOLOGY

PRINCIPAL

PRINCIPAL
RAJIV GANDHI INSTITUTE OF TECHNOLOGY
KOTTAYAM- 686 501

List of items required

SPECIFICATIONS FOR UNIFIED THREAT MANAGEMENT SYSTEM (Firewall)

The firewall must be appliance based, rack mountable and it should support internal or external redundant Power Supply, Licensing: should be per device licence for unlimited users for Firewall / VPN (IPSec & SSL) and other features. There should not be any user/IP/host based licenses - The device should be having security functions like Firewall. VPN (IPSec &SSL), Applicatiojn firewall, Gateway level antivirus, Antispam, Category based web filtering, Intrusion prevention system, Traffic shaping etc. Device should support for Virtualization (ie Virtual Systems / virtual Domains) with minimum 5 virtual System support. The platform must be capable of supporting a aminimum of 15 interfaces with auto sensing 10/100/1000 capability and 4 Gigabit SFP slots. The Firewall must support at least 1,800,000 concurrent connections and 130,000 new sessions per second, Firewall throughput for 512 & 1500 Bytes packet should be more than 15 Gbps and minimum 8 Gbps throughput for 64 byte packets. Should support 8 Gbps IPSec VPN throughput and 1500 Tunnels. The firewall sh0ould support a minimum of at least 2 Gbps IPS throughput & Minimum 1.5 Gbps NGFW throughput, Should support up to a minimum three ISP link with automatic ISP link failover as well as ISP link load sharing for outbond traffic. The firewall should support minimum 1 Gbps SSL Inspection Throughput, The firewall should support minimum 1 Gbps threat protection throughput, Should Support IPv6 functions such as management over IPv6, IPv6 routing protocols, Ipv6 tunneling, firewall and full UTM protection for IPv6 traffic, NAT46, NAT64, IPv6 IPSEC VPN, Should support IPv4 and IPv6 Rate based DOS protection with threshold settings against TCP Syn flood, TCP/UDP/ port scan, ICMP sweep, TCP/UDP/ SCTP/ICMP session flooding. Threshold settings must be customizable for different sources, destinations & services, Device should support Static routing, RIP,OSPF, BGP, IS-IS, RIPng, OSPFv3 and BGP4+, Support for authentication for Users and Firewall Administrators (Local and Remote -RADIUS, LDAP & TACACS+), Support for Native windows Active directory, The device should have IPS protection for 6000+ signatures, Should identity and control over 2500+ apllications, Gateway AV should be supported for real-time detection of viruses and malicious code for HTTP, HTTPS, FTP, SMTP, SMTPS, POP3, POP3S, IMAP, IMAPS, IM and SMB, The solution should be having facility to block communication to Botnet server using IP reputation database, Antivirus module should support Advanced Threat Protection (ATP). It should be having an option to submit suspicious file to External cloud-based file analysis (OS sandbox) for threat detection, Should support Gateway Data Loss prevention (DLP) feature for popular protocols like HTTP, HTTPS, FTP, POP3 IMAQP, SMTP, POP3S, IMAPS, SMTPS with Document Fingerprinting, The security appliance should be having configurable option to quarantine source address if that address tries to download infected file, The security appliance should be having configurable option to quarantine attack generating source address.

OEM should be having the following certifications/Ratings

SSL-TLS

network Intrusion Prevention System (NIPS) and should be ICSA Labs certified

Warranty: service support and License agreement

The equipment should have three year onsite/ online OEM warranty (including license agreement).

Rate for extended two year warranty and license may be quoted.

Purchase of the equipment is on *buy back of Fortigate 200B

Quantity -1 no

(*Present state of the equipment can be examined during working hours from Monday to Friday)

RAJIV GANDHI INSTITUTE OF TECHNOLOGY
KOTTAYAM- 686 501