GHULAM ISHAQ KHAN INSTITUTE
OF ENGINEERING SCIENCES AND TECHNOLOGY

Tender documents

For

SUPPLY, INSTALLTION AND COMMSIONING OF

"NEXT GENERATION FIREWALL"

No. GIKI/PO/C/IT-613/15
19 January 2016

The Ghulam Ishaq Khan Institute (GIK) of Engineering Sciences and Technology, located at Topi, District Swabi is a seat of excellence in higher engineering education and research. Sealed bids are invited from reputed firms/suppliers for supply, installation, commission of Next Generation Firewall:

1. **Specification of items:**
   Detail specification of the item, for which rate is required are given at Annexure-A

2. **Date for submission of the quotation:**
   Bids in sealed envelopes, on prescribed tender documents should reach to the Procurement Department, GIK Institute Topi before 3:00 pm on 3 February 2016. Write our inquiry No. GIKI/PO/C/IT-613/15 on the top of the envelope. Open bids will not be accepted.

3. **Tender opening date and venue:**
   Tenders will be opened by the Procurement Committee in the presence of bidders at 3:30 pm on the same date (3 February 2016) in the Conference Room of H. U. Beg Administration Block, GIK Institute, Topi-23640, District Swabi, Khyber Pakhtunkhwa.

4. **Price / rate:**
   Please quote unit price for each item on **FOR Islamabad** basis, inclusive of all taxes, transportation, installation, commissioning and training etc.

5. **Validity of the price:**
   Bids should remain valid for two months from the submission date of bids.

6. **Bid Security:**
   You are required to enclose the call deposit of Rs.50,000 (refundable) through demand draft/pay order payable on account of GIK Institute, Topi with your bids document.

7. **Mode of Payment:**
   Payment will be made through cross cheque subject to deduction of taxes, as per law, within 15 days after acceptance of materials / equipment.

8. **Delivery period:**
   Please mention the delivery time after placing the Purchase Order for each item.

9. **Penalty clause:**
   If you fail to supply the material in the above specified period, GIK Institute reserves the right to blacklist you for future business or forfeit the security money of 0.32% per day of the contract value or may impose any other financial penalty as deemed fit.

10. **Installation / Commission of the equipment:**
Equipment will be installed / commissioned by the trained engineer (s) of supplier / contractor at GIK Institute Topi, free of charge / are including in the cost.

Training:
Free of cost tanning will be provide on side and two engineers at your official lab.

11. **Warranty:**
Please indicate the warrantee period and terms & conditions of the warranty. Minimum three years warranty is required.

12 Please sign and stamp each page of the tender/bid document; otherwise, it will not be considered / accepted.

13. Bidders having minimum 3 years' experience of said work to the reputable organization/ institute/company etc are must.

14. Incomplete forms will not be acceptable and will not be considered in any case, and will be rejected.

15. Bids, will be accepted only, for the specifications given in the Tender (Annexure-A).

16. In case of any dispute the decision of the GIK Institute will be final and binding on you.

For further information:
Director (Procurement) GIK Institute, Topi,
District Swabi. Ph: 0938 281026 (Ext:2500/2213), Email: latif@giki.edu.pk

To be filled by the bidders

1. **Name of bidders:** ----------
2. **Address:** ----------
   ----
3. **Phone:** ---------- **Mobile** ----------
4. **Fax No.** ---------- **E-mail:** ----------
5. **NIC Tax No. -**---------- **Sales Tax No.:** ----------
6. **Branches (if any):** i. ----------
   ii. ----------
   iii. ----------

7. **Type of Business:** i. ----------
   ii. ----------
   iii. ----------

8. **Facilities**: i. List of technical staff with qualification and experience
   ii. Authorization of distribution / dealership ----------
   iii. Any other: ----------

9. **Monthly Turn Over:** ----------

10. **Previous Experience (**name of organization where said or like equipment supplied/installed/ commissioned):

    i. ---------- ii. ----------
    iii.---------- iv.----------
    v. ---------- vi. ----------
    vii. ---------- viii. ----------

Please enclose any supporting document

Name and signature: - ---------- **Date:** ----------

Seal:

Annexure-A

S.#	Name of Items	Qty. Required
	Next Generation Firewall	
4	***High end Next generation Firewall having back log analysis of 3 months minimum.*** **Next Generation Firewall Core Features Required:** 1. Avoiding the vulnerability exploitation for Web, Proxy, email, database and storage servers. 2. Web URL Filtering for http and https traffic including SSL inspection. 3. Controlling Inside and outside traffic of Data-center for viruses, intrusion and DOS – DDOS. 4. Avoiding the use of Open proxies inside Campus. 5. Usage of authorized proxy transparently inside campus. 6. Provide detail reports of the internet usage per IP and user base. 7. Provision of sending Alert email with details of the end user on violation of predefined set of policy. Like usage of the prohibited Links and prohibited wall of the social sites like Facebook, twitter etc. 8. Provision of sending email Alert on hacking attempts. 9. Provide forensic support for indecent internet usage report by Deep Packet Inspection (DPI). 10. Back log analysis data must be retained for minimum of 3 months. 11. Support bandwidth 150 mbps to 250 mbps [for 5 years future need] 12. No. of total users 3000 – 8000 [for 5 years] 13. No of total IP address 6000 – 16000 [For 5 years] **Detailed Firewall Specs** **Technical Specifications:** **Hardware** • 10-GbE SFP+ Interfaces - Min 3 • 10/100/1000 Interfaces (RJ-45) - Min 8 • GbE SFP or 10/100/1000 Interfaces – Min 8 • Management Interface – Min 2 • Internal Storage – Min 200GB • USB Ports – Min 1 **System Performance** • Firewall Throughput - At Least 72 Gbps	***1***

	• Firewall Latency - At Max 3µs • Firewall Throughput (PPS) - 78 Mpps or more • Concurrent Sessions (TCP) - 11 Million or more • New Sessions/Sec (TCP) - At Least 290,000/sec • Firewall Policies - 100,000 or more • IPS Throughput - 11 Gbps • Virtual Firewalls - 10 or more • Unlimited User Licenses - Yes **VPN Features required:** • IPSec VPN Throughput - 48 Gbps or more • Gateway-to-Gateway IPSec VPN Tunnels - 20,000 or more • Client-to-Gateway IPSec VPN Tunnels - 50,000 or more • SSL-VPN Throughput - 3.6 Gbps or more • Concurrent SSL-VPN Users - 10,000 or more • DES (56-bit), 3DES (168-bit), AES encryption - Required • MD5 and SHA-1 authentication - Required • Perfect Forward Secrecy - Group 1, 2, 5 • Prevent replay attack - Required • Remote access VPN - Required • Redundant VPN gateways - Required **Routing** • Static Routing - Required • OSPF: Instances per Device – 50 or more • OSPF: Routes - Required • Filter-based Forwarding - Required • Equal-cost multipath - Required • Reverse Path forwarding - Required **Virtualization** • Maximum number of Security Zones - 100 or more **Firewall Features** • Detect Network Attacks • DoS and DDoS Protection • TCP Reassembly for Fragmented Packet Protection • Brute-force attack mitigation • SYN Cookie • Zone-based IP Spoofing • Malformed Packet Protection	

	• WAN Optimization • Server Load Balancing **High Availability** • Active/Passive, Active/Active • Low Impact Chassis cluster upgrade • Configuration Synchronization • Session Synchronization for Firewall and IPSec VPN • Session failover for routing change . Link & upstream failure detection **Users & Device Identity Control.** • Local User database • LDAP, RADIUS & TACACS+ • Single Sign On: Windows, Novel, Citrix, Terminal Server agent • 2 factor authentication support • User & Device based policies **Administration** • Root admin, admin, and read-only user levels • software upgrades **UTM Features** • ATP (Advance Threat Prevention) • Antivirus • Web Filter (HTTP/HTTPS) • Application Control • Data Leak Prevention **IPS** • State full protocol signatures • Attack detection mechanisms: State full signatures, protocol anomaly detection (zero-day coverage), application identification • Attack response mechanisms: Drop connection, close connection session packet log, session summary, email, custom session • Attack notification mechanisms: Structured syslog , email alerts, SNMP trap • Worm protection • SSL encrypted traffic inspection	

	• Simplified installation through recommended policies • Trojan protection • Spyware/adware/key logger protection • Other malware protection • Protection against attack proliferation from infected systems • Reconnaissance protection • Request and response side attack protection • Compound attacks - combines state full signatures and protocol anomalies • Create custom attack signature **Management** • Local Management Web-based, Secure Shell Access, SSH • Product Certifications • ICSA Lab, NSS Labs, EAL 2+, EAL 4+, FIPS 140-2 **Power Supply** **1 + 1** **Reporting** • Retention minimum 3 months • Graphical Summary Reports • Network Event Correlation • UTM & Traffic Summary Reports • Built-in Report Templates • Import/Export Templates • Comprehensive alert builder • View logs in real-time or historical • Granular inspection with the log details pane ***Please note above are minimum requirements***	
Please note above are minimum requirements		