INDIAN INSTITUTE OF MANAGEMENT KASHIPUR

Bazpur Road,
Kashipur Udham
Singh Nagar
Uttarakhand-244713

TENDER DOCUMENT

Supply, Installation and Maintenance of Firewall/Authenticator and Internet/Intranet Security Solution to IIM Kashipur.

NIT No:- IIM Kashipur/QTO/2017-18/06 **Dated : 22.05.2017**

Tender Processing Charges: Rs.3000/-

Last Date of Submission of filled bid to IIM Kashipur – 14.06.2017 up to 03:00 p.m.

Ref. IIM Kashipur/QTO/2017-18/05 **Dated: 22.05.2017**

INVITATION OF BIDS FOR SUPPLY, INSTALLATION AND MAINTENANCE OF FIREWALL AND INTERNET/INTRANET SECURITY SOLUTION. TO IIM KASHIPUR, QTY REQUIRED ONE.

IIM Kashipur is interested to purchase items as per the specifications mentioned in Annexure 'A' 'B' and 'C' and terms and conditions mentioned in Annexure 'D'. Please send your bids in sealed covers so as to reach IIM Kashipur on or before 14.06.2017, 3:00 pm.

TERMS AND CONDITIONS

1. This is a two-part bid. Vendor should submit their quotations in two SEALED envelopes. One indicating technical specifications (Technical Bid) and other containing commercial terms & prices (Financial Bid).
2. Prescribed format for Technical bid "Annexure A, B &C" and for the Financial Bid "Annexure D "are only to be used.
3. The payment will be made after successful on-site installation of ordered items.
4. The price quoted will be applicable to the specifications mentioned in this quotation notice.
5. The selected vendors will be required to supply the items within 4 weeks from the date of issue of purchase order.
6. Specify the minimum period for delivery if you are not able to supply within 4 weeks. Early delivery will be a crucial factor in deciding the successful bidder.
7. A penalty of 0.5% of the total order value will be imposed per week for late delivery.
8. A three year on-site warranty on the item will be required. Beyond these 3 years, specify the post warranty comprehensive annual maintenance charges for up to 3 years.
9. The Technical bid should be accompanied by an Earnest Money Deposit (EMD) of Rs. 100000/- value of bid to be attached as DD in favor of IIM Kashipur payable at Kashipur.
10. EMD of unsuccessful bidder will be returned subsequently.
11. The work order will be issued to L-I offer submission of security deposit of 2.5% of tendered amount. Bidder have submitted the SD within three days after receiving of LOA/LOI. SD will be released at the end of the defect liability period. For this work the defect liability period shall be of twelve months, effective from the completion of the work.
12. The successful bidder has to deposit Performance guarantee equal to 5% of total cost of the supplies in the form of Bank/FDR/TDR etc, during the warranty period. EMD amount will be returned subsequently.
13. No advance payment will be made; any offer linked with advance payment is likely to be ignored.
14. After winning the order, if you fail to supply, your EMD will be forfeited and you will be blacklisted from participating in any future bid/quotations.
15. Specify the partner of OEM please attached authorization letter from the OEM
16. Tender processing charges in the form of DD of Rs.3000/- in favor of IIM Kashipur shall be attached with the Technical Bid.

17. The bidder should possess minimum 3 year experience in direct supply Installation and Maintenance of Internet Security Solution of Firewall & Security Solutions product to Govt. /Public Sector/Reputed Institutions. Proof of direct dealership details (Manufacturer's authorization letter/ dealership certificate for supply of equipment) along with contact details of minimum 5 Prime Customers to whom the equipment has been supplied by the vendor are required to be attached with quotation.
18. Bidder should submit the certificates of sales Tax and VAT returns for last three years.
19. Bidder should not be blacklisted from any Govt. /Public Sector/Reputed organization. For this the bidder should furnish affidavit that the firm is not blacklisted.

WHILE SUBMITTING BIDS PLEASE NOTE THE FOLLOWING

a. In case of any queries on technical specifications, please refer the specifications mentioned in "Annexure 'A', 'B' and 'C'" only.
b. Delivery will be made at :

Indian Institute of Management Kashipur
Bazpur Road, Kashipur
Udham Singh Nagar
Uttarakhand-244713

c. VAT will be at concessional rates as applicable to non-profit, own-use institutions.
d. Quotation (Technical Bid & Financial Bid) should be **sealed in** separate envelopes and then to be sealed in one separate envelope clearly superscripting on the envelope, "**QUOTATION FOR SUPPLY, INSTALLATION AND MAINTENANCE OF FIREWALL AND INTERNET/INTRANET SECURITY SOLUTION TO IIM Kashipur"**.

Bids may be personally dropped into the Tender box kept at IIM Kashipur or may be sent through Speed Post/Registered Post or Courier addressed to:

Chief Administrative Officer,
Indian Institute of Management Kashipur
Bazpur Road, Kashipur
Udham Singh
Nagar Uttarakhand-
244713

e. The Decision of acceptance of the quotation will lie with the competent authority of IIM Kashipur, who does not bind himself to accept the lowest quotation and who reserves the right to himself to reject or accept any or all quotations received, without assigning any reason.
f. The quotations are liable to be rejected if any of the above conditions are not fulfilled or if the bid is not accompanied with the EMD and Tender processing charges.
g. Number of items may vary as required.
h. Technical and Financial bid will be opened on 014/06/2017.
i. Date of opening of financial bid will be subsequently informed separately to the qualified bidders.

IMPORTANT INFORMATION

S. No	Last date of Submission of filled bid to IIM Kashipur	Opening of Technical Bid	Opening of Financial Bid
01	14.06.2017 upto 03:00 pm	14.06.2017 04:00 pm	Will be informed.

Annexure A

"A" Technical Bid

Technical Specifications Firewall and Internet/Intranet Security Solution to IIM Kashipur

Please mention your compliance to the following Technical Specifications if comply Mention – 'Yes' and 'No' if don't comply.	**Make/Model**
Feature	**Yes/No**
The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operating system that eliminates the security risks associated with general-purpose operating systems	
Firewall appliance should have at least 2 x 10Gig interfaces, 16 GE SFP interfaces and 16 x 10/100/1000 GE interfaces from day 1	
Firewall Throughput should be 52 Gbps from day 1	
Firewall should have 3DES IPSec throughput of more than 25 Gbps	
Firewall Should have 5 Gbps NGFW Throughput	
Firewall should support 20000 Gateway-to-Gateway IPsec VPN Tunnels	
Firewall should support 280,000 new sessions per second	
Firewall should support 11 Million concurrent sessions	
The Firewall should have integrated redundant power supply.	
The Firewall solution should support NAT64, DNS64 & DHCPv6	
The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts.	
The physical interface shall be capable of link aggregation, otherwise known as the IEEE 802.3ad standard, allows the grouping of interfaces into a larger bandwidth 'trunk'. It also allows for high availability (HA) by automatically redirecting traffic from a failed link in a trunk to the remaining links in that trunk	
The proposed system should have integrated Traffic Shaping functionality	
The Firewall should have integrated SSL VPN solution to cater to 10000 SSL VPN concurrent users.	
The Firewall & IPSEC VPN module shall belong to product family which minimally attain Internet Computer Security Association (ICSA) Certification	
The proposed system should support	
a) IPSEC VPN	
b) PPTP VPN	
c) L2TP VPN	
d) SSL VPN	
The device shall utilize inbuilt hardware VPN acceleration:	
a) IPSEC (DES, 3DES, AES) encryption/decryption	
b) SSL encryption/decryption	
The system shall support the following IPSEC VPN capabilities:	
a) Multi-zone VPN supports.	
b) IPSec, ESP security.	
c) Supports NAT traversal	
d) Supports Hub and Spoke architecture	
e) Supports Redundant gateway architecture	
The system shall support 2 forms of site-to-site VPN configurations:	
a) Route based IPSec tunnel	
b) Policy based IPSec tunnel	
The system shall support IPSEC site-to-site VPN and remote user VPN in transparent mode.	
The system shall provide IPv6 IPSec feature to support for secure IPv6 traffic in an IPSec VPN.	
Virtualization	

The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN). Minimum 10 Virtual Firewall license should be provided.	
Intrusion Prevention System	
The IPS capability shall minimally attain NSS Certification	
IPS throughput should be more than 8 Gbps	
The IPS detection methodologies shall consist of:	
a) Signature based detection using real time updated database	
b) Anomaly based detection that is based on thresholds	
The IPS should be able to inspect SSL sessions by decrypting the traffic.	
IPS Signatures can be updated in three different ways: manually, via pull technology or push technology. Administrator can schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available	
In event if IPS should cease to function, it will fail open by default and is configurable. This means that crucial network traffic will not be blocked and the Firewall will continue to operate while the problem is resolved	
IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied and attacks stopped before firewall policy look-ups.	
IPS signatures should have a configurable actions like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending a alert and logging the incident	
Signatures should a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)	
Antivirus	
Firewall should have Inbuilt Gateway level Antivirus.	
The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services:	
a) HTTP, HTTPS	
b) SMTP, SMTPS	
c) POP3, POP3S	
d) IMAP, IMAPS	
e) FTP, FTPS	
The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.	
Web Content Filtering	
The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules.	
The proposed solution should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.	
The proposed system shall provide web content filtering features:	
a) which blocks web plug-ins such as ActiveX, Java Applet, and Cookies.	
b) Shall include Web URL block	
c) Shall include score based web keyword block	
d) Shall include Web Exempt List	
The proposed system shall be able to queries a real time database of over 110 million + rated websites categorized into 78+ unique content categories.	
Application Control	
The proposed system shall have the ability to detect, log and take action against network traffic based on over 2700 application signatures	
The application signatures shall be manual or automatically updated	
The administrator shall be able to define application control list based on selectable application group and/or list and its corresponding actions	
Data Leakage Prevention	

The proposed system shall allow administrator to prevent sensitive data from leaving the network. Administrator shall be able to define sensitive data patterns, and data matching these patterns that will be blocked and/or logged when passing through the unit.	
High Availability	
The device shall support stateful session maintenance in the event of a fail-over to a standby unit.	
High Availability feature must be supported for either NAT/Route or Transparent mode	
The proposed system shall support multiple heartbeat links	
High Availability Configurations should support Active/Active, Active/ Passive & Clustering	

Annexure B

"B" Technical Bid
Technical Specifications of Authenticator System/Server to IIM Kashipur

Please mention your compliance to the following Technical Specifications if comply Mention – 'Yes' and 'No' if don't comply.	**Make/Model**
Feature	**Yes / No**
Standards-based secure authentication which works in conjunction with soft/hard tokens to deliver secure two-factor authentication to any third-party device capable of authentication via RADIUS or LDAP	
The System should support minimum 2,000 Local + Remote Users or more.	
Should support minimum 6,000 soft/hard tokens or more	
Should support atleast 200 User Groups or more	
Number of supported CA Certificates should be 10 or more	
Should support atleast 10,000 User Certificate Bindings	
Should support minimum 15 numbers of Remote LDAP Servers and Domain Controllers	
The appliance should have atleast 4 x 10/100/1000 (copper, RJ-45) interfaces	
The appliance should have minimum 2TB of local-storage	
The appliance should have a manageability over CLI and Console and HTTPS.	
The system should support SNMP v1 / v2c / v3.	
The system should support atleast 45 numbers of Static-Routes	
Integrates with existing solutions such as LDAP or AD servers to lower the cost and complexity of adding strong authentication to your network	
Support for E-mail and SMS tokens enables rapid deployment of two-factor authentication without the need for additional dedicated hardware	
Should support User self-servicing and password management to allow users to manage their own registrations and passwords without administrator intervention	
Support for Certificate Authority functionality to simplify the CA management and to deliver user certificate signing, VPN, or server x.509 certificates for use in certificate-based two-factor authentication	
Single Sign-On (SSO) Transparent User Identification with zero impact for enterprise users	
SSO Portal based authentication with tracking widgets to reduce the need for repeated authentications	
Monitoring of Carrier RADIUS Accounting Start records	
User self-service certificate enrollment supported for specific devices using the following protocols and methodologies	
iPhone/iPad to Automated SCEP	
Android to Manual PKCS#12	
Windows to PKCS#10 CSR	
Other to SCEP, PKCS#10 CSR, Manual PKCS#12	
The appliance should support EAP-MD5, EAP-TTLS, EAP TLS, EAP-GTC and PEAP protocols for authentication via 802.1X for Port Based Network Access Control	
The Soft/Hard token should generate a 6 character key	
Time-based One-time Password Algorithm (TOTP) hardware tokens RFC6238 compliant	
RADIUS Challenge Request, Post username/password authentication Token prompt	
Token Drift Support	
160-bit seed should be used for all OTP tokens	
Seed should be generated using RNG method	
Seed should be encrypted with 2048-bit RSA and stored in secured database	
Should support one token one seed procedure, ensures seed is non-duplicable	

Seed should be injected into hardware token by automatic processing system, seed never exposed to operators	
Should support Multi-level security access control to manufacturing system and database with Smartcard access control protection	
"Seed destroy" service should be available upon confirmation by client	
Configurable Time Step should between 30 and 60 seconds	
Supported Algorithm, TOTP or HMAC-based One Time Password (HOTP)	

Annexure C

"C" Technical Bid
Technical Specifications of Logging and Reporting System/Server to IIM Kashipur

Please mention your compliance to the following Technical Specifications if comply Mention – 'Yes' and 'No' if don't comply.	**Make/Model**
Feature	**Yes/No**
The offered logging and reporting solution shall provide Logging through	
a. Comprehensive event logging	
b. Historical Reporting	
c. Report generation	
d. Real Time Monitor	
e. E-mail Notification	
f. GUI based interface	
The offered logging and management solution shall be manageable through:	
a. Web User Interface HTTPS / client software for GUI access	
b. Command Line Interface (console)	
c. Command Line Interface (SSH)	
The bidder shall provide a appliance based Reporting Server with the specifications as per the recommendations of the OEM.	
The logging and Reporting Server shall be able to handle 10GB logs / day. The Central logging and Reporting Server shall have storage configured in RAID 0/1/5/10	
The communication between all the components of Firewall System shall be authenticated and encrypted with one or more of standard authentication and encryption mechanisms like SSH, MD5, SHA, DES, 3DES & IPSec.	
The logging and reporting Server shall generate comprehensive GUI based Reports (both Real-time as well as Historical) which could be customized as per requirement. It shall provide comprehensive reports on attacks, source & destination of attacks, vulnerabilities exploited etc.	
The Historical Reports shall be provided for multiple timeframe i.e. hourly, daily, weekly, monthly and customized period.	
The logging and reporting Server shall support filtering of Reports based on various factors such as Source / Destination IP Address, TCP/UDP Port Number, Protocol, Signature ID, Application, Device ID, Traffic flow between the Zones, Timestamp, Human readable description of event and action taken (Block / log / email) etc.	
The logging and reporting Server shall provide forensic / investigative features wherein, in case of some attack, it would indicate type of attack, source destination of attack and other relevant information.	

Note:
A, B &C of technical bids may be in the same appliance or separate appliance

1	Minimum 3 year onsite warranty required	Agree	
		Cannot Provide	
2	Delivery period	Minimum	
		Maximum	**4 Weeks**
3	Installation is to be done free of cost.	Agree	
		Cannot Provide	
4	Validity of Rates are for 90 Days	Agree	
		Do not agree	

Signature :
Vendor Name :
Office Address :
with seal

Date_____

"Annexure D"

Financial Bid

Supply, Installation and Maintenance of Firewall/Authenticator/Logging & Reporting System and Internet/Intranet Security Solution to IIM Kashipur

S No.	Item Descriptions		Unit Price (Rs.)
1	Please specify-Make & Model Number along with necessary details, if required.		**Make** **Model:**
2	Price of one Firewall and Internet/Intranet Security Solution. (Including all Components of Annexure "A") (Rs.)		
3	Price of Authenticator System/Server (Including all Components of Annexure "B") (Rs.)		
4	Price of Logging and reporting System/Server (Including all Components of Annexure "C") (Rs.)		
5	Installation to be done by the supplier free of cost.	**Agree**	
		Do not Agree	
6	Onsite 3-year, warranty		
7	**Total Amount (Inclusive of all Taxes)**		

Signature of bidder

Date ……..

Full Address_____

-Sd-
P.K. Srivastava
Engineer In- Charge