Pollution Control Board, Assam
Bamunimaidam, Guwahati-21

www.pcbassam.org
Email: membersecretary@pcbassam.org

NOTICE INVITING TENDER

NIT No. WB/COM-20/13-14/06 Dated Guwahati, the 06th March, 2020

Sealed quotations are invited from the reputed Authorized Dealers for supply and installation of **"Unified Threat Management (UTM)"** with buyback value at the Head Office of Pollution Control Board, Assam, Bamunimaidam, Guwahati-21. Quotations will be received upto **2:00 PM on 20th March, 2020** and will be opened on the same day **at 3:00PM** in presence of Quotationer or their authorized representatives. General Terms & Conditions, Letter of Acceptance, duly completed Check list, Financial Bid Document, Details of the Firm and Specifications are as per Annexure –I, II, III, IV & V respectively.

Name of works	:	**Supply and Installation of UTM Firewall (9 Nos.)**
Earnest Money	:	**Rs. 10,000/-** (Rupees Ten Thousand) only must be deposited by bidders in the form of Bank Draft in favour of **"Member Secretary, Pollution Control Board, Assam"** payable at **Guwahati** and should be submitted along with their bids.
Last Date of issue of paper for quotation.	:	**16.03.2020**
Last Date & Time of submission.	:	**20.03.2020 at 2.30PM**
Date & Time for opening	:	**20.03.2020 at 3.00PM**
Cost of Quotation Paper	:	**Rs. 500/-** (Rupees Five Hundred) - Non Refundable

Member Secretary
Pollution Control Board, Assam
Bamunimaidam, Guwahati-21

Memo No. WB/COM-20/13-14/06-A Dated Guwahati, the 06th March, 2020

3594

Copy to:

1. P.A. to the Chairman, PCBA for kind appraisal of the Hon'ble Chairman.
2. Website(www.pcbassam.org) / Notice Board of the Board's Head Office, PCBA.

Member Secretary

POLLUTION CONTROL BOARD : ASSAM
BAMUNIMAIDAM, GUWAHATI-781 021
Items Details

SL No.	Item Name	Quantity	Buyback Device
1.	UTM for Head Office, PCBA	1 No.	Fortinet 80C (1 No.)
2.	UTM for Regional Office, PCBA	8 No.	Fortinet 40C (8 No.)

General Terms & Conditions

1. This document contains the following
   A. Copy of Quotation Notice.
   B. General Terms and Conditions of Bid.
   C. Acceptance Letter (Annexure-I).
   D. Check List (Annexure-II).
   E. Financial Bid Document (Annexure-III).
   F. Details of the Firm / Company / Dealer (Annexure-IV).
   G. Detailed specification of the products (Annexure-V).

2. The Quotation is Single Bid Quotation.
3. The PCBA is having its headquarters at Guwahati, Assam. Presently, PCBA is having 30 Mbps OFC Line network from BSNL at Head Office. 4 Mbps OFC Line Network from BSNL at each Regional Offices at Guwahati, Nagaon, Bongaigaon, Tezpur, Golaghat, Sivasagar, Dibrugarh and Silchar.
4. Presenting PCBA is having 80C Fortinet Firewall (1 No.) at Head Office and 40C Fortinet Firewall (8 Nos.) at each Regional Offices.
5. All the equipment shall be supplied installed, tested, demonstrated and commissioned at PCBA, Head Office and at each Regional Offices within **15 days** from the placement of purchase order.
6. The vendor should submit the equipment wise documents (manuals in the form of hard copy or soft copy DVD/CD) which should include the system descriptions, installation and commissioning procedure, operating procedure, step by step fault diagnosis and fault rectification, circuit or block diagram etc.
7. The Quotation Document is not transferable by the purchaser. Each sheet including that provided by the Board with this document must be signed by the bidder.
8. The Board takes no responsibility for delay or non-receipt of Quotation Document sent by post either way and also reserves the right to accept; or reject any or all the quotations in part or full without assigning any reason thereof.
9. This Quotation notice is also available on PCBA's website www.pcbassam.org. Bidders have to collect the detail quotation paper (Specification & Terms) from Board's office at Bamunimaidam, Guwahati - 781021 or can be downloaded from the website on payment of Rs. 500/- (Rupees Five Hundred) only (Non-refundable) in the form of Bank Draft to be drawn in favour of "Member-Secretary, Pollution Control Board, Assam".
10. **Bidder should not have been blacklisted or debarred from business by any Government institutions/undertakings/recognized educational intuitions,**

Banks/financial institutions / public Sector companies in the last 10 years. The bidder has to give a declaration that the firm / supplier and the firm has not need blacklisted of debarred in the past by any Govt. or Private Organization. In case any false declaration is submitted, the bidder shall be permanently blacklisted from this organization and legal proceedings may be initiated against such parties.

11. The Board at its discretion may extend the last date of submission of Quotation and opening of Quotation. **The final authority for acceptance of a quotation will rest with the Member-Secretary, Pollution Control Board, Assam who does not bind himself to accept the lowest quotation and is vested with the authority to reject any or all of the quotations received without assigning any reason.**
12. The warranty period is between twelve months to thirty-six months depending on the item quoted and starting from the date of successful commissioning of the instrument.
13. The bid shall contain no interlineations, erasures or overwriting words except as necessary to correct errors made by the bidder, in that case, such correction shall be initialed by the person or persons signing the bid.
14. It is advised that the outside suppliers should send the Quotation through Registered Post/ Speed Post. However, the local supplier may drop their quotations in Quotation Box kept in the Board's office for the purpose. In no case Quotation should be handed over to any employee of the Board.
15. Canvassing in any form will disqualify the Bid.
16. The Quotation Notice No. WB/COM-20/13-14/06 dated 06th March, 2020 should be invariably be quoted in the bid and for further correspondence in this regard.
17. All rights reserve Chairman, Pollution Control Board, Assam.
18. The office of the undersigned reserved the right to modify the term and conditions partially or wholly or cancel the tender without assigning any reason thereof.
19. The courts at Guwahati shall have exclusive jurisdiction to entertain and try all matters arising out of this contract.
20. Party should have Registration Certificate, PAN card, Trade license, GSTN registration.
21. All the Quotation should be addressed to:

    THE MEMBER SECRETARY,
    POLLUTION CONTROL BOARD, ASSAM
    BAMUNIMAIDAM, GUWAHATI-781021

22. The EARNEST MONEY (Fixed Amount) shall be in the form of Demand Draft only in favour of "MEMBER SECRETARY, POLLUTJON CONTROL BOARD, ASSAM" payable at GUWAHATI. Quotation shall not be entertained where a quotation has not furnished adequate Earnest Money as specified in the NIT. The Earnest Money will be refunded after successful installation and commissioning of the Rack Server. In case of non-supply within stipulated time or the item supplied is found defective and not attended by the supplier, the Earnest Money deposited by the supplier will be forfeited.
23. The installation and commissioning of the equipments is the entire responsibility of the supplier. It must be done within one week of the receipt of the equipments by the Board.
24. The validity of Quotation would be for a minimum period of 90 days from the date of opening of quotations. A Bid valid for a shorter period may be rejected by the Board as non-responsive.
25. The rates should be quoted both in words and figures. If there is discrepancy between words and figures, the amount mentioned in words will prevail.
26. The Bidder must sign the every page of the quotation.

27. To assist in the examination, evaluation and comparison of bids the buyer may, at its discretion, ask the Bidder for a clarification of its bid. However, no change in the price or substance of the bid shall be sought, offered, re-permitted
28. Full payment will be released on delivery, installation and successful commissioning of the instruments/equipment (to be certified by concerned Officer/In-charge of the Division), and on submission of bills in triplicate. No advance payment will be made in any case and no proposal for documents through Bank will be considered.
29. **Agency should have authorized service center in Assam (attach Address Proof).**
30. **The bidder should be authorized dealer of the OEM (OEM Authorization is mandatory).**
31. **The Agency should have adequate manpower / support staff to install and maintain all UTM in all Regional Offices.**
32. Agency should provide proof of sales and service of device in any organization worth minimum of 50 lakhs in any of the last three financial year.

Member-Secretary, i/c

(IN FIRM'S LETTER HEAD)

LETTER OF ACCEPTANCE TO BE SUBMITTED IN THE BID.

To

The Member Secretary
Pollution Control Board, Assam
Bamunimaidam, Guwahati – 781021

Sub: Acceptance of Terms and conditions of tender.
Ref: Tender No.

Sir,

Having examined in details of the above tender documents relating to the works and having acquired all the requisite information affecting the tender invited by you, I/We.....hereby agree to all terms and condition of the contract [as laid down in the tender document(s)]. I/We also agree that the printed term(s) and condition(s) if any at the back of our quotation form and I or any other paper enclosed are not applicable.

I/We undertake to complete the whole works within the period specified in the tender. In this connection we are providing with the following information.

1. **Firm Registration** certificate.
2. **Proof of address** of the firm.
3. In case bidder is an Authorized Dealer/ Distributor,
   a. Authorization certificate from parent company.
4. Fees.
   a. Details of EMD paid
      Amount..... Draft No.....Bank.....
   b. Cost of Tender Paper
      Amount..... Draft No.....Bank.....
5. GSTN Registration No.....PAN No..... (Copies Enclosed)
6. Declaration that the firm has not been banned or de-listed by any Govt. or quasi Govt. Agency or Public Sector Undertaking enclosed.
7. Previous Supply Order with other department, if any.
8. Any other relevant document.

(Signature with Seal)
(Name & Designation in block letters)

Annexure-II

Documents Check List

SL No.	Requirement	Bidder Compliance
1.	EMD & Tender Fee	
2.	OEM Authorization.	
3.	Product Literature / Information Brochure	
4.	Letter of Acceptance (Annexure-I)	
5.	Firm Registration Certificate	
6.	Proof of Address of the Firm	
7.	GSTN Registration Certificate	
8.	Pan Card Details	
9.	Validity of quoted rate agreed as per NIQ	
10.	Payment term agreed as per NIQ	
11.	Delivery terms agreed as per NIQ	
12.	Warranty period agreed as per NIQ	
13.	Declaration that the firm has not been banned or de-listed by any Govt. or quasi Govt. Agency or Public Sector Undertaking.	
14.	Previous supply order with other organization, if any	
15.	Any other relevant documents.	

Annexure-III

Commercial Bid for UTM Firewall

SL. No.	Description of the item	Qty.	Unit rate with Buyback value in Rs.	Total Amount in Rs.
	Supply, installation and programming of 9 nos. of UTM with 3 years			
1.	UTM for Head Office	1 No.		
2.	UTM for Regional Offices	8 Nos.		
3.	Installation, commissioning and programming charges.	Lot		
	Total cost including taxes			

Signature of Bidder

*****

Annexure – IV

DETAILS OF SERVICE PROVIDER AGENCY

1. Name of the Service Provider Agency :
2. Name of Owner/Director :
3. Complete Address :
4. Contact Telephone No :
5. Fax No :
6. E-mail :
7. PAN/TAN No :
8. GST Registration No :
9. Name – telephone & Mobile No of the dealing / authorized representative:
10. Any other Information :

Signature of authorized Signatory

Specification for UTM (1 No.) at Head Office

SL. No	Specification	Compliance (Y/N)
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 97%	
3	OEM should be in Leaders quadrant of Gartner's – in Network Firewall Magic Quadrant as per the latest report	
4	Appliance shall be ICSA certified for Firewall	
Hardware & Interface requirements		
1	The platform must be supplied with minimum 8x GE RJ45 inbuilt data interfaces from day one	
2	The Appliance should have 1x USB & 1x Console Ports	
Performance and Availability		
1	The Firewall with minimum 5 Gbps of Firewall throughput & support of 300,000 concurrent sessions, and 25,000 new sessions per second from day one.	
2	Minimum IPS throughput of 1000 Mbps for real world traffic or enterprise mix traffic	
3	Minimum SSL Inspection Throughput of 500 Mbps	
4	Minimum Threat Prevention Throughput (measured with Application Control and IPS and Anti-Malware enabled) of 500 Mbps for real world traffic or enterprise mix traffic	
5	IPSec VPN throughput: minimum 1 Gbps	
6	Simultaneous IPSec VPN tunnels: 100	
7	Proposed solution must support minimum 100 SSL VPN users from day one	
8	Proposed solution must support minimum 5 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 for outbound traffic & also should support SDWAN functionality for future scalability	
6	Firewall should support link aggregation functionality to group multiple ports as single port.	

7	Firewall should support minimum VLANS 200	
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 & both IPSec & SSL VPN functionality should be ICSA certified	
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	IPS should be ICSA Certified & should be recommended by NSS Labs	
AntiVirus & AntiBot		
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 provide cloud based sandboxing solution from day one to prevent from zero day threats	
10	The gateway Anti-Virus functionality should be ICSA certified	
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 200 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 solution should have the flexibility to write security policies based on IP Address & User Name & Endpoint Operating System	
5	The product must supports Layer-7 based Firewall virtualization, and all Firewall features should be supported in each virtual firewall like Threat Prevention, IPS, Web filter, Application Control, content filtering etc.	
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, SSHv2 and should support both SNMPv2 and SNMPv2c providing in-depth visibility into the status of appliances.	
3	The Firewall should have option for inbuilt functionality of automated configuration audit by simple license upgrade	
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	

- **Bidder should mention specification in details.**

Specification for UTM (8 Nos.) at Regional Offices

SL. No	Specification	Compliance (Y/N)
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 97%	
3	OEM should be in Leaders quadrant of Gartner's – in Network Firewall Magic Quadrant as per the latest report	
4	Appliance shall be ICSA certified for Firewall	
Hardware & Interface requirements		
1	The platform must be supplied with minimum 5x GE RJ45 inbuilt data interfaces from day one	
2	The Appliance should have 1x USB & 1x Console Ports	
Performance and Availability		
1	The Firewall with minimum 700 Mbps of Firewall throughput & support of 300,000 concurrent sessions, and 10,000 new sessions per second from day one.	
2	Minimum IPS throughput of 250 Mbps for real world traffic or enterprise mix traffic	
3	Minimum SSL Inspection Throughput of 100 Mbps	
4	Minimum Threat Prevention Throughput (measured with Application Control and IPS and Anti-Malware enabled) of 100 Mbps for real world traffic or enterprise mix traffic	
5	IPSec VPN throughput: minimum 50 Mbps	
6	Simultaneous IPSec VPN tunnels: 100	
7	Proposed solution must support minimum 100 SSL VPN users from day one	
8	Proposed solution must support minimum 2 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 for outbound traffic & also should support SDWAN functionality for future scalability	
6	Firewall should support link aggregation functionality to group multiple ports as single port.	
7	Firewall should support minimum VLANS 200	
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 & both IPSec & SSL VPN functionality should be ICSA certified	
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	IPS should be ICSA Certified & should be recommended by NSS Labs	
AntiVirus & AntiBot		
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 provide cloud based sandboxing solution from day one to prevent from zero day threats	
10	The gateway Anti-Virus functionality should be ICSA certified	
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 200 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 solution should have the flexibility to write security policies based on IP Address & User Name & Endpoint Operating System	
5	The product must supports Layer-7 based Firewall virtualization, and all Firewall features should be supported in each virtual firewall like Threat Prevention, IPS, Web filter, Application Control, content filtering etc.	
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, SSHv2 and should support both SNMPv2 and SNMPv2c providing in-depth visibility into the status of appliances.	
3	The Firewall should have option for inbuilt functionality of automated configuration audit by simple license upgrade	
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	

- **Bidder should mention specification in details.**

*****