

INDIAN INSTITUTE OF TECHNOLOGY GOA

भारतीय प्रौद्योगिकी संस्थान गोवा

Farmagudi, Ponda 403401, Goa, India

Phone no: 0832-2490875, email: purchase@iitgoa.ac.in



GSTIN: 30AABAI1653D1ZF

PAN: AABAI1653D

TAN: BLRI08261B

Date: 07-11-2019

Notice Inviting Tender

Tender No: IITGOA/2019-20/035

Due Date: 28/11/2019

Dear Sir/ Madam,

On behalf of the **Indian Institute of Technology Goa**, sealed quotations are invited in two bid system for the supply of Firewall UTM Bundle. The items are to be door delivered at IIT Goa, GEC Campus, Farmagudi, Ponda- Goa – 403401.

Items Required at IIT Goa

Sl.No	Description of Item (configuration is given below)	Qty
1	Supply & commissioning of Firewall / UTM with installation, configuration, Subscription & Support	01

TECHNICAL SPECIFICATIONS FOR FIREWALL/UTM	
Sr No.	Description
1	The firewall should be appliance based Next Generation Firewall.
2	The proposed firewall OEM must be in Leader's quadrant of Gartner Enterprise Firewall report of 2017 and 2018 (Attach documentary evidence)
3	The proposed firewall OEM must have 'Recommended' rating in NSS Labs NGFW report of 2016, 2017 and 2018. Bidder/OEM should also mention if product got 'Recommended' rating in first attempt or in retest for all 3 years. (Attach signed note/declaration)
4	The Firewall should be hardware based, reliable, purpose-built security appliance with hardened operating system supporting statefull policy inspection technology.
5	Firewall appliance should have at least 2x 10GE SFP+ Slots, 8x 1GE SFP Slots and 8x 1GE RJ45 interfaces from day one. All these interfaces should be available simultaneously.
6	Firewall appliance should have 2 dedicated 1GE RJ45 management ports in addition to interfaces mentioned in point 5.
7	2x SFP (SX 1GE) transceivers should be provided from day one.
8	Application control throughput should be at least 13 Gbps.
9	Firewall should have minimum SSL Inspection Throughput of at least 5.5 Gbps. Vendor's claim must be supported by publicly available document to be submitted while bidding.
10	Threat Prevention (including FW, IPS, Application Control & Antivirus) throughput must be at least 4.5 Gbps with real-world / enterprise mix traffic. Vendor's claim must be supported by publicly available document to be submitted while bidding.
11	NGFW (including FW, IPS, Application Control) throughput must be at least 5 Gbps with real-world / enterprise mix traffic. Vendor's claim must be supported by publicly available document to be submitted while bidding.
12	Firewall should support more than 290,000 new sessions per second.

13	Firewall should support at least 8 million concurrent sessions.
14	The Firewall solution should support NAT46, DNS46 & DHCPv6.
15	The proposed system should be able to operate in Transparent mode and NAT/Route mode simultaneously without creating virtual context or virtual firewall.
16	The physical interface should be capable of link aggregation as per IEEE 802.3ad standard, allowing the grouping of interfaces into a larger bandwidth 'trunk'. It should also allow for High Availability (HA) by automatically redirecting traffic from a failed link in a trunk to the remaining links in that trunk.
17	The proposed system should have integrated Traffic Shaping functionality.
18	The proposed system should support advanced routing features like PBR (Policy Based Routing) without affecting security functionalities like IPv6, SSL Inspection, Anti-Spam, Sandboxing etc.
19	The Firewall module should have ICSA or other equivalent Certification.
20	The Firewall should have integrated solution for VPN and there should be no user based licensing for SSL VPN & IPSec VPN (both Site-to-Site and Client-to-Site) as well.
	Intrusion Prevention System
21	The IPS capability of proposed OEM should have received NSS Labs' "Recommendation" rating of NGIPS 2017 and NGIPS 2018 test report by delivering minimum 99% exploit block rate for both years.
22	IPS throughput should be at least 5 Gbps or better for real-world / enterprise mix traffic. Vendor's claim must be supported by publicly available document to be submitted while bidding.
23	The IPS detection methodologies should consist of: a) Signature based detection using real time updated database. b) Anomaly based detection that is based on thresholds.
24	The IPS should be able to inspect SSL sessions by decrypting the traffic.
25	The IPS system should have at least 11,000 signatures.
26	IPS Signatures should be updated in different ways: manually, via pull or push technology. Administrator should be able to schedule checking of new updates. If the device has a public IP address, updates can be pushed to the device each time an update is available.
27	In the event of IPS ceasing to function, it should fail open by default and be configurable so that crucial network traffic should not be blocked and firewall should continue to operate while the IPS problem is being resolved.
28	IPS solution should have capability to protect against Denial of Service (DoS) attacks. Should have flexibility to configure threshold values for each of the anomaly. DoS protection should be applied and attacks stopped before firewall policy look-ups.
29	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 an alert and logging the incident.
30	Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low).
	Web Filtering Features:
31	The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should have at least 2 billion WebPages and 75+ categories without external solution, devices or hardware modules.
32	The proposed system shall provide ability to allow, block attachments or downloads according to file extensions or file types.
33	Solution should have the ability to assign Quota per Web Category or Website. Example: 100 Mb quota for Streaming Media / YouTube. If individual user exceeds 100 Mb limit for YouTube, Streaming Media / YouTube should be Blocked but rest of the allowed categories should remain accessible.
	Application Control Features:
35	The appliance should have at least 4000+ application signatures database.
36	Should have the intelligence to identify & control popular IM & P2P applications like KaZaa, Bit Torrent, Skype, You Tube, Facebook, LinkedIn etc.
37	Firewall must have capability to do cloud application based routing not by means of manually adding IPs and or FQDNs i.e. firewall should have database of O365 and other

	cloud services readily available to select as destination address in firewall policy and destination address in static route configuration to give particular ISP path.
38	Firewall vendor must keep updating application's backend FQDNs and IP addresses database on regular basis .
	Anti-Virus, Anti-Bot & Advanced Persistent Threat Features:
39	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
40	Firewall should offer both anti-virus scanning options - proxy mode and flow (streaming) mode.
41	Should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.
42	Firewall must include anti-bot capability using IP reputation DB, should be able to terminate botnet communication to C&C servers. Vendor needs to add any additional licenses if it is required.
43	Firewall should have 30000+ botnet definitions in its database and should be updated on regular basis to protect from new definitions.
44	Anti-Virus module should be ICSA certified.
45	The proposed solution should include licenses for Cloud Sandboxing from day one. It should automatically detect and confirm multi-stage zero-day malware and targeted attacks without prior knowledge of the malware by sending the file to Cloud Sandbox for analysis.
46	The proposed solution's Cloud Sandboxing technology should have threat extraction capabilities for files such as PDF, Word etc. Malicious content should be removed and file should be reconstructed with remaining clean content.
47	User Authentication
48	The proposed solution shall be able to support various form of user Authentication methods simultaneously, including: a) Local database entries b) LDAP server entries c) RADIUS server entries d) TACACS+ server entries e) Native Windows AD (Single sign-on capability) f) Citrix agent support for single sign-on
49	The solution should be capable of providing Windows AD single sign-on by means of collector agents which broker between users when they log on to the AD domain and the device.
50	System should also have capability to identify devices (ex. Android, iPhone, Windows etc.) & should be able to write policies on basis of device identity.
	Data Leakage Prevention
51	Firewall should have in-built DLP functionality without requiring any additional hardware or software license.
52	System should allow administrator to prevent sensitive data from leaving the network. Administrator should be able to define sensitive data patterns, and data matching these patterns that should be blocked and/or logged when passing through the unit.
53	Proxy solution must detect, protect and log sensitive data travelling through HTTP and HTTPS channels.
54	DLP feature must offer watermarking functionality which allows organizers to apply document marking for DLP.
55	DLP actions should be : Log only, Block, Quarantine User/IP/Interface.
56	It should have DLP fingerprinting feature which generates a checksum fingerprint from intercepted files and compares it to those in the fingerprint database.
	Logging and Reporting
57	Solution must integrate with an external hardware appliance from same OEM (and not third party integrations) to store logs and reports. In-built reporting will not be considered as it impacts firewall performance and there is a risk of loss of data in case of hardware / disk failures.

58	It should show real-time traffic details.
59	Logs should also show per user statistics which must include sent/receive bytes, number of sessions, threat score, bandwidth usage, sent/receive packets & source IP or user, destination country detail.
60	It should show real-time session details like Source IP etc. for both LAN -> WAN as well as WAN -> LAN traffic (in case of port forwarding).
61	Logging and reporting appliance should have capacity of accepting and storing minimum 90 GB/day logs.
62	Logging and reporting appliance must have at least 4TB storage capacity to store historical logs and reports
Support and RMA	
63	Proposed solution should include any / all additional hardware / software / licenses / modules required to support above mentioned features and functionalities along with 24x7 remote support directly from OEM along with Next Business Day RMA replacement (5 years support) for Enterprise Firewall and 24x7 remote support directly from OEM for Logging and Reporting appliance (5 years support).
Log Analyser	
Features	
64	Graphical summary reports
65	Network event correlation
66	Scalable performance and capacity
67	Centralized logging of multiple record types
Log Viewer	
68	View logs in real-time or historical
69	Log filtering and search capabilities
70	Granular inspection with the log details pane
DLP Archiving	
71	Investigate DLP content archives
72	Should support archive types like email, HTTP, FTP, IM etc
Alerting	
73	Comprehensive alert builder
74	Should Trigger off of severity levels, specific events, actions and destinations
75	Should set varying thresholds by number of events within a certain timeframe
76	View or search through historical alerts
77	Should Notify via email/SNMP or raise a syslog event
Hardware Specifications (If required externally)	
78	Form Factor : 1 RU Rack mount
79	Total Interfaces : 4x GbE
80	Storage Capacity : Minimum 1 TB
Capacity and performance	
81	Days of Logs : 8 GB maximum

82	Sessions/Day : 18 M
83	Average Retention at 8 GB Logs/Day : 3Months
	High Availability
84	System should have built-in High Availability (HA) features.
85	Solution must be proposed to operate in Active-Active HA from day one. Bidder must quote any additional hardware / licenses required for Active-Active HA.
86	Should support stateful session maintenance in the event of a fail-over to a standby unit.
87	Firewall in HA should support seamless upgradation activity for all major and minor versions.
88	High Availability feature must be supported for either NAT/Route or Transparent mode.
89	Should support multiple heartbeat links.
90	High Availability Configurations should support Active/Active, Active/ Passive & Clustering (More than 2 appliances in HA).

Special instructions to the bidder:

- (1) The bidder should provide all the required features Licenses & subscriptions available from day one of implementation.
- (2) The bidder should strictly comply with the remark filled / provided with the Compliance matrix during the submission of bid as against the enquiry.
- (3) The bidder has to study the existing setup and list the requirement of additional features to take care of the existing setup and features requirements.
- (4) The bidder has to support either in-person or through remote, based on the situation for five years.
- (5) In addition, the bidder has to make provision for the support directly through remote from OEM when IIT Goa log the case through their portal. The case id has to be generated once the case has been logged.
- (6) A training for handling the appliance, daily monitoring, fine tuning and reporting should be provided to the IT personnel during installation / configurations.
- (7) The keys, passwords, subscription details should be handed over to personnel at the CITS section.
- (8) The bidder should register the name of IIT Goa with the OEM and IIT Goa should receive the mails for their support, news alert, technology updates etc.
- (9) The bidder has to maintain secrecy of the data, settings, mappings of Ips, configurations on UTM and the server detail entries entered during configurations and should not be disclosed to any third party.

The eligibility criteria for participation in bid are mentioned below:

- 1) The Bidder should have ISO 9001: 2015 certification. (Documentary evidence required)
- 2) The Bidder should have OEM certified partnership if the bidder is a partner. (Documentary evidence required)
- 3) Manufacturer Authorisation Certificate to participate in this tender with tender number.
- 4) Bidder should have in the business of providing firewall appliance since last 3 years (Attach company registration certificate and copies of previous orders)
- 5) Bidder should have valid GST Registration. (Documentary evidence required)
- 6) Bidder should submit last 3 years Income Tax Returns. (FY 16-17, 17-18,18-19)
- 7) Bidder is required to provide 5 years of technical support on all the items. (Provide contact number, service engineer details with escalation matrix)

- 8) The suppliers shall provide the banking details along with their quote on their letterhead duly signed and stamped.

The above-mentioned basic eligibility conditions are broad guidelines and the Director, IIT Goa hereby reserves the right to relax / alter / modify / add any or all the conditions as well as accept or reject any or all bids without assigning any reason.

Instructions to the Bidder:

- 1) **Preparation of Bids:** bidders must ensure that bids are submitted in **two bid system (i.e.) Technical bid and Financial bid in separate envelopes.**
 - a) **Technical bid:** The technical bid should consist of all technical details/brochures along with commercial terms and conditions super-scribed as TECHNICAL BID with Tender No. and date and time of closing and the bidder's name and address. No prices should be included in the technical bid. Bidder should submit non-commercial bill of material along with Technical Bid. Include a document that lists the specification as mentioned in this tender and whether complied or deviated. In case of any deviation, the deviation should be clearly mentioned.
 - b) **Financial (Price) Bid** should indicate firm and fixed figures and words super-scribed with the Tender No. and date of closing of the Tender with name of supply/work and the bidder's Name and address. The price bid should not contain any conditional clauses. No price escalation for any reasons whatsoever is allowed.
 - c) The technical and financial bids duly signed by the bidders or their authorised signatories with name and seal should be put in separate cover and sealed. Both sealed covers should be put into a bigger cover duly super-scribed with PT No. and due date/time with name of supply /work. **Technical bids must either be spiral bound / stapled together. No loose sheets will be accepted. All pages must be numbered.**
- 2) **Submission of the tender:** The complete sealed bids in all respects shall be sent to the following address well in advance either by post or by courier or by hand so as to reach this office on or before the due date and time specified in the Schedule. The bids received after the closing date and time shall not be considered.

The Assistant Registrar (S&P),
Indian Institute of Technology Goa,
GEC Campus, Farmagudi,
Ponda, Goa - 403401.

While submitting the bids, the bidders must sign all the tender documents as a token of accepting of tender documents as well as terms and conditions stipulated therein. Tender documents without signature of bidders or their authorised signatories will be treated as invalid bids.

No conditional offer or terms and conditions will be entertained by the institute and such bids will be treated as invalid.

- 3) The tender documents can be downloaded from IIT Goa web site: <http://www.iitgoa.ac.in/announce.php?type=tenders> or from <https://eprocure.gov.in/cppp/>.
- 4) **Opening of the tender:** The Technical Bids will be opened by the tender committee duly constituted in the presence of bidders or their authorised representatives, if they desire on **29-11-2019 at 4.00 pm**. Then the bids will be evaluated by the Technical Evaluation Committee which will decide the suitability of the technical bids as per our requirement and terms and conditions. Once the technical evaluation is completed, the price Bids of only those bidders who are found technically acceptable will be opened in the presence of Authorized Representatives of such bidder(s), if any on a date and at a venue to be intimated by IIT Goa to the shortlisted bidders.
- 5) The bidder shall note that any unsolicited post-tender reduction by them would disqualify them from participating from the bidding and forfeit the security bid.
- 6) **Incomplete bids are liable for rejection.**
- 7) **Prices:**
- I) For Import Supplies:**
- It is mandatory to quote prices in CIF basis only to be door delivered in IIT Goa.
 - In case of multiple options of same product, bidders are requested to quote only one best option and not multiple options.
 - Payment terms: 90% payment by letter of credit and balance 10% will be paid by wire transfer after satisfactory installation and commissioning.
 - If quoted in US Dollars, the exchange rate to INR on the date of opening of financial bid will be used for price comparison.
- II) For Indigenous Supplies:**
- It is mandatory to quote prices in FOR basis only to be door delivered in IIT Goa.
 - In case of multiple options of same product, bidders are requested to quote only one best option and not multiple options.
 - Payment terms: Within 30 days after the delivery and installation of the item at IIT GOA.
- 8) **Offer validity:** The offer must be valid for 120 days from the closing date. If the validity of offers for acceptance is less than 120 days, the same will not be considered.

Important Terms and Conditions:

- The last date for the submission of the tender is **28-11-2019 at 5.30 pm**.
- Delivery and installation must be made within 4 weeks of getting a confirmed order.
- GST as applicable. IIT Goa will provide GST Concession Certificate, if required.

- 4) For any query you may contact us regarding purchase to 0832-2490875 / purchase@iitgoa.ac.in and for technical to 09158577660; amol@iitgoa.ac.in
- 5) Send the two sealed documents (Technical bid and Financial bid) in one envelope directly to **The Assistant Registrar (S&P), IIT GOA, GEC Campus, Farmagudi, Ponda, Goa – 403401.**
- 6) **Bid Security (EMD):** *EMD either in the form of Bank Demand draft of Rs.1,00,000.00 initially valid up-to 90 days drawn in favour of INDIAN INSTITUTE OF TECHNOLOGY GOA payable at GOA, must be sent along-with the Technical bid only.*

The technical bid without EMD would be considered as UNSOLICITED and will be REJECTED. Photo/FAX copies of the Demand Draft/Banker's pay orders will not be accepted. No interest will be paid for the EMD and the EMD (Bid Security) will be refunded to the successful bidder on receipt of Performance Security (Security Deposit) and in case of unsuccessful bidders, the EMD will be refunded on finalisation of tender.

- 7) **Bid security be forfeited** without any intimation in such cases as below: -
 - a) If a bidder withdraws its bid during the period of bid validity.
 - b) If a successful bidder fails to accept the awarded contract within 15 days of award of the contract.
- 8) **Performance Bank Guarantee:** Performance Bank guarantee for 5% of Purchase order value should be produced in the form of B.G from the nationalised /scheduled Bank valid till the completion of warranty / guarantee period plus sixty days as claim period. Wherever installation/commissioning is involved, the guarantee/warranty period shall be reckoned from the date of completion of installation/commission. Failure to render contracted service during the warranty/guarantee period by the contractor, the performance bank guarantee will be forfeited. No interest is payable on the performance Bank guarantee amount.
- 9) **Guarantee/Warranty:** The Contractor shall guarantee that the material supplied shall comply fully with the specifications laid down, for material, workmanship and performance after acceptance of the material **for a period of five years.** The tenderer should clearly mention in the bid the period of guarantee/warranty offered by him. If any defects are discovered therein or any defects therein found to have developed under proper use arising from faulty stores design or workmanship, the Contractor shall remedy / replace such defective items at his own cost.
- 10) **Installation& Commissioning:** The vendor should Install all the items satisfactorily at IIT Goa campus within 10 days of supplying the items. Installation report is mandatory for the payment process.
- 11) **Insurance:** IIT Goa being a Central autonomous body under Ministry of HRD, Government of India, we will not insure our goods. However, to safeguard the ordered material from probable transit damage while in transportation the contractor may insure the goods at his risk and cost.
- 12) **Delivery Schedule:** Please note that delivery is the essence of the contract. In case there is any deviation in the delivery schedule, liquidated damages clause will be levied for the delayed period of supply. Therefore, it should be ensured that all the ordered items should

be supplied within one month from the date of receipt of Purchase Order on door delivery basis at our Institute as per Purchase order terms with securely and sufficiently packed by following standard packing procedure to withstand transit damages. In case of import supply, the item should be delivered at the cost of supplier to our institution. The installation and commissioning should be completed as specified in our important terms and conditions.

- 13) **Extension of time:** If the completion of stores is delayed due to reasons of force majeure such as acts of God, acts of public enemy, acts of Government, fires, floods, epidemics, quarantine restrictions, strikes etc., the contractor shall give notice within 15 days to Institute in writing of his claim for an extension of time. The Institute on receipt of such notice after verification, if necessary, may agree to extend the Contract delivery date as may be reasonable but without prejudice to other terms and conditions of the contract.
- 14) **Micro and Small Enterprises (MSEs)** registered with National Small Industries Corporation are exempted from payment of Earnest Money Deposit. However, vendors covered under this category have to submit copy of registration certificate with present validity along with technical bid, failing which, the bid will be disqualified.
- 15) **Modifications of specification:** The supply to be made by the Supplier under this Purchase order can be modified or changed by the request from the IIT Goa provided that for such modifications or changes the parties shall first agree to possible addition or reduction in cost, the delivery date and such other terms and conditions occasioned by or resulting from such modification or change. Such agreement shall be effected either by way of exchange of letters duly signed by authorised representatives of the parties or by signed change order form or by minutes of meeting signed by authorised representatives of the parties, which shall constitute the necessary amendments to the contract. Possible increase or decrease in the contract price shall be calculated in accordance with unit prices. The cost of such additional jobs should be reasonably fixed with reference to the quoted price for such or similar items.
- 16) **IIT Goa reserves the full right** to accept / reject any tender or all tenderers at any stage without assigning any reason in public interest.
- 17) **IIT Goa** reserves the right to accept in full or part a bid depending on its requirements.

18) **Important Dates:**

Sr. No.	Description	Date	Time
1	Pre bid submission meeting- survey for installation. (Kindly send the confirmation mail to amol@iitgoa.ac.in)	15-11-2019	10:30 AM to 12:00 AM
2	Bid submission last date	28-11-2019	05.30 PM
3	Bid opening date	29-11-2019	04.00 PM