INDIAN INSTITUTE OF TECHNOLOGY GOA
At Goa Engineering College Campus
Farmagudi, Ponda, Goa 403401
E-mail: purchase@iitgoa.ac.in

CORRIGENDUM-III

Enquiry No: IITGOA/2019-20/035 **Date: 09/12/2019**

Corrigendum to the Tender for Supply & commissioning of Firewall / UTM with installation, configuration, Subscription & Support vide Enquiry No. IITGOA/2019-20/035 dtd. 07/11/2019.

For the tender for Supply & commissioning of Firewall / UTM with installation, configuration, Subscription & Support at IIT Goa, the following clauses / paragraphs have been modified:

Points numbered 84 to 90 will be considered according to the institute's requirement. The same should be quoted separately on a separate sheet in the financial bid and in the technical bid. This may or may not be considered depending on the institute's evolving requirements at the final stage of tender processing.

The Compliance matrix as per the specified format in **Annexure A** should be included in the tender. Deviations, if any should be reported against each specification. IIT Goa reserves the right to accept or reject deviations as it may deem fit.

Extended bid submission date: Dec. 18, 2019 till 05:30 PM.
Technical bid opening date: Dec. 19, 2019 at 03.00 PM

****All other items, terms and conditions remains unchanged.*

Annexure A

Sr No.	Description	Comply (Yes/No)	Deviation (if any)
1	The firewall should be appliance based Next Generation Firewall.		
2	The proposed firewall vendor must be in Leader's quadrant of Gartner Enterprise Firewall report of 2017 and 2018.		
3	The proposed firewall vendor must have 'Recommended' rating in NSS Labs NGFW report of 2016, 2017 and 2018. Bidder should also mention if product got 'Recommended' rating in first attempt or in retest for all 3 years.		
4	The Firewall should be hardware based, reliable, purpose-built security appliance with hardened operating system supporting stateful 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 10,000 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 the 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 500 million 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 the 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 a 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 user/group connections and access 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 each user/group connections and access.		
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 a 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 forms 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 the capability to identify devices (ex. Android, iPhone, Windows etc.) & should be able to write policies on the 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 the 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		
78	Form Factor : 1 RU Rack mount		
79	Total Interfaces : 4x GbE		
80	Storage Capacity : Minimum 4 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		

The Following Part will be considered according to the Institutes requirement. The same should be quoted separately on a separate sheet in the financial bid and in the technical bid. This may or may not be considered depending on the institute's evolving requirements at the final stage of tender processing.

	High Availability
84	System should have built-in High Availability (HA) features.
85	Solution must be proposed to operate in Active-Passive HA from day one. Bidder must quote separately as a line item any additional hardware / licenses required for Active-Passive 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).