

**This document contains responses to questions that were communicated to IISc by email, with reference to the “Tender notification for the procurement of Unified Threat Management (UTM) Appliance for Indian Institute of Science
Last date : Feb. 16, 2016, 11.00 am”**

1. You have mentioned about Gartner magic quadrant. There is a category called Enterprise Network Firewall and UTM. Which category you are referring to?
(A) We are referring to the UTM category.
2. Are you looking at a scalable open architecture in this solution in both hardware and software?
(A) The RFP asks for an appliance-based solution. However, if required, we should be able to deploy more than one such appliance. In that case, the appliances should be able to work together, for example, in a fault-tolerant mode.
3. Is the throughput mentioned in the document is based on the internet bandwidth available which is 1.2Gbps?
(A) No. We expect the solution to work even after reasonable-sized bandwidth upgrades happen in the near future.
4. Do u want a solution that will not make the IPS fail open by default?
(A) Suppose the IPS module has failed or is disabled. Then the default action should be that traffic should pass through the UTM box in both directions. This is what we understand by “fail open.”
5. Is the throughput mentioned here is based on real world traffic/IMIX traffic or LAB performance?
(A) The throughput mentioned is based on projected requirements, given the current traffic demand that we observe.
6. Firewall Inspection Mode required is Proxy Mode or Packet Filtering?
(A) We require both modes.
7. You have mentioned fully protected throughput. Does this mean the throughput measurement is calculated with the appliance scanning all bytes within the session of AV, IPS?
(A) Yes, all bytes need to be inspected.
8. Is the throughput mentioned here is calculated with all Security features (IPS, AV, ABOT, URLF, Anti-SPAM) enabled?
(A) Yes, the throughput mentioned in the fully protected mode assumes that all functionalities are enabled (please see pg 14, 3(h) of the RFP).
9. Is the throughput mentioned here is calculated based scanning of all parts of the session (scan all bits and bytes in a packet)?
(A) Please see the response to Q7.
10. Do you need network forensics as a part of this solution which can identify first infected machine and the complete chronology of infection?
(A) The RFP does not specify forensics as a requirement.

11. Do you want the Anti-bot solution which can detect Bot infected host inside your network?
(A) We consider BOT traffic as part of malware. We need the BOT detection capability assuming BOT traffic passes through the UTM appliance, without any “clients” installed on user machines.
12. Do you want the solution to prevent BOT attacks in both the directions i.e., from downloading BOTs/Malware and also block the BOT from communicating to external hackers (command & control servers)?
(A) Please see Pg 18, point 20 of the RFP. We need protection from BOT attacks in both directions.
13. You have mentioned about zero day attacks, do you want the solution do prevent zero day attacks or just detect them?
(A) Yes, we want the ability to *prevent* zero-day attacks.
14. Kindly let us know the total % usage of NKN network currently and also the anticipated growth of usage in the next 3 years.
(A) The specifications that we have provided on pages 13 and 14 of the RFP should be used for sizing of the proposed appliance. The percentages being asked for are not required.
15. Kindly let us know if any hosted servers are there in the network to be secured.
(A) Yes, we do have hosted servers to be secured.
16. How many 1G SFP+ connections will get connected now?
17. How many 10G SFP+ ports are required now?
18. How many copper GBE ports are required?
(A) to (16), (17), (18): The answers to all these questions are available on page 13 of the RFP.
19. Kindly let us know to the traffic profile/pattern being considered to arrive at the throughput. This will help us in sizing the right model/solution for your setup.
(A) The throughput mentioned is based on projected requirements, given the current traffic demand that we observe.
20. You have mentioned "The technology proposed by the bidder for this requirement should have been evaluated by Gartner in 2014-2015 and should appear either in the leader's or the challenger's". In order to look at a consistent and a good performing solution we recommend you look at it for 3 or more consecutive years.
(A) As explained in the pre-bid clarification meeting, two years would be enough for our requirement.