RailTel Corporation of India Ltd

(A Government of India Enterprise)

Plot No 143, Sector 44,
Institutional Area,
Opposite to Gold Souk,
Gurgaon,Haryana 122003
Work: 01244236083
Fax: 01244236084,

Website: **www.railtelindia.com**

Ref: RailTel/Tender/OT/CO/DNM/2015-16/URL-FILTERING/299
Dt. 29.09.2015

Corrigendum-I

Subject: - Tender for **"Supply and Installation of URL-filtering Appliance".**

Ref: i) This office E tender No: RailTel/Tender/OT/CO/DNM/2015-16/URL-FILTERING/299 Dt. 28.08.2015.

In reference to the above referred, the following amendments are issued in the Tender document. The bids may be submitted in consideration of these amendments.

1. **Chapter 3 , Clause 5.1.1 may be read as**

   Device should be deployed in High Availability mode (1+1)

2. **Chapter 3 , Clause 3.4 Network Architecture and Requirement may be read as**

   Device should be deployed in offline mode [TAP Mode] and should be able to block URL in offline mode [TAP Mode] by sending TCP-RESET to Source and destination IP.

3. **Chapter 3 , Clause 4.1 may be read as**

   The system shall comply with the provision of Cyber laws w.r.t. content/web filtering.
   The system shall also comply with the provisions of the Information Technology (IT) Act 2000, as amended from time to time. Latest IT ACT to be followed and same can be referred/download from DoT and DeitY site.

4. **Chapter 3 , Clause 5.1.6 is added**

   URL filtering device should maintain access and denied logs for at least 60 days based on URL and should be able to export to external Syslog Server.

5. **Chapter 3 , Clause 5.1.7 is added**

   URL filtering device should have functionality to integrate with any NMS software for device utilization monitoring.

6. **Chapter 3 , Clause 5.1.8 is added**

   Ability to block HTTPS traffic in sniff mode.

7. **Chapter 3 , Clause 5.1.9 is added**

   Ability to produce a block page for both SSL and HTTP traffic in sniff mode.

A.K.Sablania
(Group General Manager/DNM)

Consolidated Quires for URL Filtering Tender No 299

Tender No. RailTel/Tender/OT/CO/DNM/2015-16/URL-FILTERING/299
Tender Name Rate Contract for supply , installation and commissioning of URL-fitering System

SN	Chapter	Clause No	Description	Vendor/SI/OEM Name	Clarification	Justification by Firm	Railtel Response
1	Chapter-3	Clause 1.16	The web filtering solutions shall be deployed at all Internet Gateway locations covering the completer IP traffic of RAILTEL	M/s Sophos		Please suggest whether you are planning to deploy these solutions in standalone mode or in high availability at each location	maky kindly refer corrigendum -I
2	Chapter-3	Clause 4.16	The typical deployment of web filtering solution should be in offline mode at internet gateway locations.	M/s Sophos		Gateway solution would not work in offline mode hence request you to change it to Standalone/ Transperant/ Bridge mode	maky kindly refer corrigendum -I
3	Chapter-4	Clause 1.16	The system shall comply with the provision of Cyber laws w.r.t. content/web filtering. The system shall also comply with the provisions of the Information Technology (IT) Act 2000, as amended from time to time.	M/s Sophos		Please suggest how to coinsider the changes which are going to amended in future	maky kindly refer corrigendum -I
4	Chapter-4	Clause 11.17	While deploying the solution, existing Routing architecture of the RAILTEL need not be changed or revamped.	M/s Sophos		How the traffic would be routed to web appliance	Tender document is very lear
6	Chapter-5	Clause 1.1.5	Each Gateway should support concurrent 5000 IP/end points	M/s Sophos		Please confirm how many total user license is required.	Tender document is very lear
7	Page 18	Note	In case of bidder is proposing appliance based solution for URL filtering , In that case Appliance should have min 2 x 10G SFP+/XFP port , dual DC power supply (-48 V) Redundancy and CE/FCC certifications .	M/s Sophos		Please suggest if you are planning to connect Web appliance with SFP ports if not request you to please remove this requirement.	Tender document is very lear
8	Chapter-4	Clause 4.1	The system shall comply with the provision of Cyber laws w.r.t. content/web filtering. The system shall also comply with the provisions of the Information Technology (IT) Act 2000, as amended from time to time.	Fortinet	Please share the IT Act 2000 or high level specfic requirement wrt to URL filtering		maky kindly refer corrigendum -I
9	Chapter-4	Clause 4.9	Solution shall able to prevent objectionable, obscene, unauthorized or any other content, messages or communications infringing copyright, intellectual property etc., in any form, from being carried on RAILTEL IP network, consistent with the established laws of the country.	Fortinet		I believe the list of urls having these kind of objectionable, obscene, unauthorized contents will come from DOT. URL filtering appliance need to block the urls based on DOT guideline and list of URLs provided by DOT. Infringment, copyright, intellectual property etc. should not be a part of URL filtering solution. URL filtering solution should be block / allow the urls based on DOT URLs.	Tender document is very clear
10	Chapter-4	Clause 4.10.2	No limitation on the URl list	Fortinet	Everything has some limit. I would request to mention some realistic value.		Tender Condition is very Clear
12	Chapter-5	Clause 1.3	Flow based HTTP filtering throughput – minimum 2 Gbps and scalable up to 10 Gbps.	Fortinet		In case some vendor is proposing fixed chassis hardware appliance and it can't scale from 2Gbps to 10Gbps. Then will it be OK to cosider the box of 5Gbps throughput at initial and then latter we can deploy additional appliance of same model to achieve 10Gbps of throughput. This is to avoid sizing of 10Gbps appliance from day one.	Tender Condition is very Clear
13				Netsweeper	For sizing what is the total bandwidth to be considered per location? Also, what is the bandwidth per location redirected towards URL filtering solution?		Tender Condition is very Clear
14				Netsweeper	Can you please confirm what kind of TAPs you have deployed in the network and will you be forwarding only all outbound traffic or only outbound HTTP/HTTPS requests towards Netsweeper servers?		Tender Condition is very Clear
15				Netsweeper	Is there any segregation between Management and Data segments?		Tender Condition is very Clear
16				Netsweeper	Do you have any specific template or format to be used for technical solution proposal or we can use our own?		Use your own
17				Netsweeper	Do we need to provide the costing for only software licensing and AMC or include hardware costing as well?		Propose software/appliance bases solution
18	Chapter 3	Clause 3.4	The typical deployment of web filtering solution should be in offline mode at internet gateway locations.	Bluecoat	Railtel will be responsible for creating the TAP in network devices and confirm that all relevent traffic would be hitting the URL filtering servers. Kindly suggest.		Network TAP will be provided by RailTel
19	Chapter 3	Clause 4.1	The system shall comply with the provision of Cyber laws w.r.t. content/web filtering. The system shall also comply with the provisions of the Information Technology (IT) Act 2000, as amended from time to time.	Bluecoat	Please suggest how to consider the changes which are going to amended in future in IT act.		Tender Condition is very Clear
20	Chapter 3	Clause 10.15	The System support to block http and https based URLs	Bluecoat	from the clause we understand that offered solution is expected to intercept, decrypt https traffic for URL filtering purpose? If yes, we would need intermediate CA certificate, buyer is expected to provide the same. Secondly for HTTPS traffic symmetric routing is require to intercept SSL handshake and decrypt the traffic, do we have symmetric routing available or can be made available. Kindly suggest		Tender Condition is very Clear
21	Chapter 3	Clause 5.1.1.2	Outbound HTTP Throughput Capacity of more than 2 Gbps per server	Bluecoat	As per solution requirement, only http get requests going out of network would be required to examined. All outbound traffic is not required to be monitored. So we do not need 2Gbps outbound traffic handling capability. Kindly clarify.		Tender Condition is very Clear

22	Chapter 3	Clause 5.1.1.3	Flow based HTTP filtering throughput - minimum 2 Gbps and scalable up to 10 Gbps	Bluecoat	As per solution requirement, only http get requests going out of network would be required to examined. All outboud traffic is not required to be monitored. So we do not need 2Gbps outbound traffic handling capability. Kindly clarify.		Tender Condition is very Clear
23	Chapter 3	Clause 5.1.1.4	Http request per second - minimum 50k per sec	Bluecoat	Please suggest the scalability		Tender Condition is very Clear
24	Chapter 3	Clause 5.1.1.5	Each Gateway should support concurrent 5000 IP/end points	Bluecoat	Please confirm how many total user license is required.		Tender Condition is very Clear
			Addional Points	Bluecoat	Do we need Reporting and logging capabilities in offered solution like who tried to access what, when, IP and allowed or not? Kindly suggest.		maky kindly refer corrigendum -I
			Addional Points	Bluecoat	Is it required to be integrated to any SIEM or NMS or reporting tool? Kindly suggest.		maky kindly refer corrigendum -I
25				Netsoft		Ability to block HTTPS traffic in sniff mode	maky kindly refer corrigendum -I
26				Netsoft		Ability to produce a block page for both SSL and HTTP traffic in sniff mode	maky kindly refer corrigendum -I
27				Netsoft		Allow policies to be assigned according to VLAN tags in sniff mode	Tender Condition is very Clear
28				Netsoft		Allow for Username resolution by connecting Directory Service like Active Diretory in sniff mode	Tender Condition is very Clear
29				Netsoft		The Purposed solution should be a purpose built stand alone web filtering solution and should not be a UTM/Firewall based web filtering solution	Tender Condition is very Clear