Request for Proposal

National URL Filtering and Blocking System

Introduction

The National ICT R&D Fund invites proposals from academia/research institutions, companies, organizations for the development, deployment and operation of a national level URL Filtering and Blocking System. Institutions/organizations/companies desirous of developing, deploying and managing the proposed system are requested to submit their proposals to the ICT R&D Fund Islamabad by 1500 hrs on 2nd March, 2012 as per the prescribed format.

GENERAL INSTRUCTIONS

Proposal Submission

a. All proposals must be accompanied by a bid security (refundable) of PKR 50,000 in the form of a Pay Order/Demand Draft in favor of "National ICT R&D Fund" (cheques will not be accepted).
b. Proposals will be accepted and evaluated using a two stage process. In the first stage only technical proposals are being solicited to be evaluated against the evaluation criteria given below.
   Please note that Financial Proposals are not required at this stage of the process.
c. Financial proposals will be solicited from shortlisted institutions/organizations in the second stage. Final award will be on the basis of combined technical and financial score in the following manner:

Proposal	**Weight**
Technical	70%
Financial	30%
Total	**100%**

d. Proposals shall be submitted in English language.
e. The proposals shall be clear and elaborative. Different sections of the proposals shall be numbered and separated using color separators, flags or tags. The proposals shall be prepared without any interlineations or overwriting.
f. Bidders/Applicants may request in writing, for clarification of any of the provisions of this RFP up till 15 (fifteen) days before the submission date. All queries may be sent to sed@ictrdf.org.pk. Responses to queries will be emailed and also placed on the Fund's website.
g. The Fund reserves the right to accept or reject any or all of the proposals submitted without assigning any reason thereof.
h. The costs of preparing the proposal and of negotiating any subsequent funding, including visits for discussion with the Fund are not reimbursable.

Technical Proposals

Technical Proposals shall be in compliance with the requirements laid down in the RFP and the proposed Program model. The technical proposal shall include the following:

a. A covering letter from the applicant.
b. Table of Contents with page numbers
c. Profile of the applicant
d. Details of Core technical team for proposed assignment clearly identifying the team lead. Resumes of the core technical team are to be provided.
e. Experience in the subject area with details of prior commercial/research work undertaken in this field. Please provide details of relevant deployments, publications, etc. during the past five years.
f. Details of existing/proposed national and international collaborations/affiliations in the proposed program area with industry, academia and government (Pl provide supporting documents).
g. Proposed solution, methodology and work plan
h. Contact List

Proposal Submission

a. Each Proposal shall be submitted as one printed copy and one soft copy on a CD or DVD (MS Word compatible file format).
b. Proposals must be sealed and clearly marked.
c. Technical proposals must be delivered at the address given below before 1500 hrs (PST), on 2nd March, 2012.

    Solicitation and Evaluation Department
    National ICT R&D Fund
    6th Floor, HBL Tower, Jinnah Avenue
    Blue Area, Islamabad, Pakistan
    Tel: 051-9215360-64
    Email: sed@ictrdf.org.pk

d. Upon submission, Technical Proposals shall be opened at 1530 hrs, on 2nd March, 2012 in presence of all applicants who choose to be present.
e. The technical proposals will be evaluated on the basis of Evaluation Criteria given below. Bidders shortlisted on the basis of their technical submissions will be asked to submit a Financial Proposal.

Evaluation Criteria

The evaluation committee appointed by Fund will evaluate the technical proposals on the basis of their compliance with the RFP and by applying the evaluation criteria and the point system as specified

below. A technical proposal shall be rejected at this stage if it fails to achieve the minimum score indicated in table below:

Table 1: Technical Evaluation Criteria and Marks

No.	Requirements	Marks
a.	Clarity of proposal, compliance to RFP and proposed project concept	5%
b.	Core technical team for proposed project clearly identifying the team lead. Resumes of the core technical team to be provided.	20%
c.	Experience in the subject area with details of prior commercial/research work undertaken in this field. Please provide details of relevant deployments, publications, etc. during the past five years.	25%
d.	Details of existing/proposed national and international collaborations/affiliations in the subject area with industry, academia and government (Pl provide supporting documents).	10%
e.	Proposed Solution, Methodology and Work Plan	40%
Minimum qualification score		**65%**

Financial Proposals

Institutions shortlisted on the basis of their technical submissions will be asked to submit a Financial Proposal including three year O&M costs.

TERMS OF REFERENCE

Internet access in Pakistan is mostly unrestricted and unfiltered. The Internet traffic is coming from two IP backbone providers, i.e., PTCL and TWA. The Internet Service Providers (ISPs) and backbone providers have currently deployed manual URL filtering and blocking mechanism in order to block the specific URLs containing undesirable content as notified by PTA from time to time.

Many countries have deployed web filtering and blocking systems at the Internet backbones within their countries. However, Pakistani ISPs and backbone providers have expressed their inability to block millions of undesirable web sites using current manual blocking systems. A national URL filtering and blocking system is therefore required to be deployed at national IP backbone of the country.

ICT R&D Fund has decided to fund the indigenous development, deployment, operations and maintenance of such a system by companies, vendors, academia and/or research organizations with proven track record.

This system would be indigenously developed within Pakistan and deployed at IP backbones in major cities, i.e., Karachi, Lahore and Islamabad. Any other city/POP could be added in future. The system is proposed to be centrally managed by a small and efficient team stationed at POPs of backbone providers.

The system would have a central database of undesirable URLs that would be loaded on the distributed hardware boxes at each POP and updated on daily basis. The database would be regularly updated through subscription to an international reputed company maintaining and updating such databases.

System requirements would be as follows:

1. Should be capable of URL filtering and blocking, from domain level to sub folder, file levels and file types.
2. Should be able to block a single IP address or a range of IP address.
3. Hardware should be stand-alone that can be integrated into any Ethernet/IP network.
4. Hardware should be carrier grade, 1+1 redundant configuration, 100% uptime, redundant power supplies (-48 V DC) with minimum power consumption and other carrier grade specifications.
5. The system should be capable of network monitoring via SNMP. The system should also report critical system statistics, like CPU/Memory utilization, network throughput, etc.
6. The solution should support offline configuration with zero packet delay to the original traffic.
7. The system should operate on OSI layer 2 or 3.
8. The bandwidth handling capacity should be scalable. The current bandwidth of Pakistan is about 85Gbps in total as of December 2011, growing at 40-50% per year. The solution should be scalable and modular to cater for bandwidth expansion of future. Bandwidth expansion should be handled by adding/stacking hardware boxes in modular form. The solution should be deployed in distributed model with filtering boxes placed at the distribution points of backbone providers in major cities. Each hardware box should be capable of handling 10Gbps (or more) of traffic at line rate.

   The installation at PTCL IP Gateways at Karachi (Pak Capital and Marston Road Exchange requires to TAP 20 (twenty) 10G interfaces. The system should be able to handle 100Gbps traffic at each node.

   PTCL has decided to install 100Gbps interfaces at above location in near future, therefore the system should be able to support 100Gbps interfaces. Minimum change should be required to migrate from 10Gbps interfaces to 100Gbps interfaces.

   Similar design approach should be adopted after reviewing the core network of TWA.

9. The system should be modular and scalable to any number of interfaces at the backbone router/switches.
10. The system should have the ability to intercept the flow in both directions (in-bound or out-bound traffic).
11. The system should be rapidly programmable to support new protocols and applications.
12. The system should be preferably plug and play and require minimum configuration for setup.
13. The total delay introduced by each hardware box should not be more than 1 milliseconds at line rate of 10Gbps. In case of offline configuration there should be Fail Safe operation.

14. Each box should be able to handle a block list of up to 50 million URLs (concurrent unidirectional filtering capacity) with processing delay of not more than 1 milliseconds.
15. The system should support multiple languages to capture URL in any language.
16. The system must support IWF or any other equivalent 3rd party external URL Database.
17. Master Database update time should be user configurable.
18. The Master Database should be locally installed with support to update the Database from network.
19. The system should allow Proprietary DB definition or integration.
20. The Database should be flexible and could be locally modified to meet customer needs.
21. The Database should be flexible to add/remove filters or categories.
22. The backend control of the system to view access to block list URL database should be only with the solution holder (backbone operator). The solution supplier should not have access to view the categories defined by the customer.
23. The solution supplier should be able to provide remote and onsite support on 24 x7 basis in major cities of Pakistan.
24. The solution supplier should propose and quote for providing operations and maintenance (O&M) support of the system with service level agreement (SLA) for five years after system installation and commissioning.
25. System supplier should quote cost of yearly maintenance and up-gradation of the system.
26. No one should be able to view or access the customer defined categories in Database.
27. Separate hardware fast-path for delay-sensitive traffic, ensuring very low latency (~10micS) should be provided. The system should have load balancing and failover capabilities. In case of failure or degraded performance of the system, it should be capable of automatic bypass through a fail-safe port.
28. Updating of URL Database should be done through CLI commands. Support for bulk load through file/network should also be provided.
29. The solution should also support Web based administration via HTTP or HTTPS.
30. The solution should provide easy to use, user friendly web based application to easily block/unblock URL categories.
31. The solution should provide a hierarchical authentication system with configurable hierarchal access to the system management.
32. Blacklist database must be protected with some encryption technology method/key to protect tampering.
33. The system should allow to view statistics related to packet TX and RX.
34. The system should allow reset to factory default mode. User should be prompted if Database is to be reset too.
35. The system should allow to enable/disable all the features listed under filtering/blocking.

END OF RFP