السورية للاتصالات
SYRIAN TELECOM

STE Building
Fayaz Mansour Street
Almazzah
Damascus, Syria
Tel: +963 11 2240300
Fax: +963 11 2242000

FAX

Our Ref : 768 /20/1/1
Date : 2/10/2007

To : AGT
Fax no : 0097143904757
Sub : Technical Tender Book to Central monitoring system for public data network (PDN) and the Internet in the Syrian Arab Republic.

Dear Sirs,

You are kindly requested to submit a trial project of the above mentioned tender according to the technical requirements specified in the enclosed book of conditions.

Please be noted that STE will send the legal and financial book of conditions and the final technical vision of the future network. And later you can submit a financial and technical bid with the legal proving documents per the provision **of law no. 51 of 2004** under condition that the complete bid is to be submitted two weeks after putting the trial project under testing.

Please be noted that all costs resulted from submitting and testing of the trail project will be at your expense.

Waiting for your trial project within /3/ weeks from the date of this correspondence.

Best regards

STE Director General

Syrian Arab Republic

Syrian Telecommunication Establishment

Department of Technical Affairs

Technical Tender Book to central monitoring system For public data Network services (PDN) and the Internet In Syrian Arab Republic

1- introduction:

Syria is considered one of the most growing countries in the Middle East Region concerning the use of Internet. The Public Data Network (PDN) constitutes a complete and integrated infrastructure which was built for this purpose. This network is built over the port wholesale concept.

This increasing growth has imposed many challenges in the face of achieving monitoring requirements which are needed by LEA: Law Enforcement Agencies. It has clearly become necessary to move towards a monitoring system that has the ability to cope with the fast increase in the number of Internet users, in addition to the great diversity of applications.

The aim of this tender is to build a centralized monitoring system which should be independent of the Network, high-performance, highly scalable, and has the ability to meet the monitoring requirements mentioned here in this tender.

The current network contains about 18600 dialup ports, and 3500 broadband ports (DSL) in service. In addition to this, 12500 broadband ports are being installed and should enter service before the end of 2007. The network is expected to scale up to 300 thousand broadband ports and 30 thousand dialup ports by the end of 2008.

Concerning internet services providers, there are seven providers currently connected with the PDN. There are also two providers that own their own independent access networks and international links (which will be later

connected to the PDN). It is expected that three new Internet service providers (ISP) will enter into service bye the end of 2007. The network is being expanded with the goal that it accepts 30 ISPs by the end of 2008.

Please check annex No 1 which describes the current and the proposed design of the PDN.

2- General requirements:

Bidders are requested to provide a complete offer include the following tasks:

1- Supply of hardware and software needed to meet the requirements mentioned in this tender.

2- Supply, install, and put into operation a complete live testing system over the current network. The testing system will be put under continuous evaluation for a period of 2 months at least, in order to verify its performance and reliability. It should be capable of monitoring a network with about 15.000 broadband ports, and meet all qualitative requirements of the monitoring system. The result of technical evaluation will rely heavily on the output of this live testing.

3- The testing system should be equipped will a requirements for connection with the PDN, and with the ISPs (if it is needed). Two monitoring terminals should be supplied (item 3-7).

4- Provide two levels of training:

   i- Training the users to use and operating the system (30 users).

   ii- Training a number of technicians and engineers on the operation and management of the system which includes complete and partial installation (20 technicians).

5- Provide the necessary upgrades to meet expansion requirements as they are explained in the annex. These upgrades should be provided within a period of 4 months after the notification to the bidder.

6- Repair or replace failed equipment within a period of 48 hours maximum.

7- Perform periodic full tests to the system each 3 months to verify the security of the system, its overall performance, and its immunity against attacks. In addition to this, systematic auditing of the sensitive parts of the system should be carried on a monthly basis at least. The bidder is asked to provide a clear and detailed description of testing steps and procedures, along with a sample of the resulting report.

8- The bidder must commit to provide spare parts for the system equipment for a period of 10 years at least. In case the provider cannot commit to this, the system should be able to work over alternative standard equipment (e.g. Inter-based servers) and without a performance drop exceeding 10%. The bidder should prove this through direct testing.

9- The bidder should provide as a mandatory part of his answer, a list of compliance statements including detailed response to each of the technical points in this tender book. The bidder may use only one of two possible answers : compliant, or Not compliant (partial compliance is considered as not compliant). All the conditions are considered mandatory (except conditions where it is stated clearly that "it is preferable"), and non-compliance of one of them may lead to disqualification of the offer.

10- The bidder has to offer a detailed technical design explaining the different stages of capturing, collecting, analyzing and storing the data. He has also to mention clearly the eventual bottlenecks and the means of expansion, along with a detailed description of the protocols used in the system and their compliance with international standards. Priority is given to the standards of ITU, the standards of IETF and then the standards of ETSI.

11- The system will be put into service in two phases: the first phases covers the current network and it should be done as soon as possible. The second phase aims at covering the system that will have been installed bye the end of 2008.

The bidder is requested to provide a detailed schedule explaining in it the expected following tasks starting from the date of obtaining commencement order.

- The first phases: monitoring the current network, implementation should start immediately after obtaining commencement order.
    - i- Supplying of the equipment.
    - ii- Training of users (technical).
    - iii- Installation of monitoring system to the current network and put it into operation.
    - iv- Installation all centralized parts of the system needed for monitoring upon achieving the expected capacities at the end of 2008.
- The second phase: monitoring of the future network which will be executed after the kickoff of the expansion project. The final design for the network will be provided to the bidder in order to proceed with the implementation.

The bidder is asked to provided the detailed set of hardware, software, and various tasks which need to be carried on during each of these phases.

3- The technical requirements:

3-1- general requirements

1- The system must be centralized and has the ability to monitor all the networks which use data communication services inside the Syrian territories and with all its different forms as follows:

- Different entities linked to the PDN including service providers and other corporate networks.
- ISPs which are not connected to the PDN.
- The entities which have data networks not connected through the PDN (e.g. using leased lines to connect between branches)

- Providers of Internet via satellites (with terrestrial upload and satellite download).
- VSAT systems linked to the central node which will be installed in STE.
- Customers connected to the network regardless of their ways of connection (WIMAX – GPRS –DIALUP – DSL – LL – ISDN – and WIFI).

2- It is preferable that the system is independent of the service providers as much as possible. The amount of equipment to be installed at the ISP premises should be minimal if needed. This equipment should be immune against hacking, tampering or inspection of its content, and the ISP should not be able to know the data being gathered and collected.

3- There should not be any interference of the monitoring system with the network functions or the monitored network performance. Monitoring activities should be fully transparent for all parties so the user cannot feel he is being monitored.

4- All monitoring activities should be done undetected, neither by the monitored targets, nor by ISPs, and not even by the management of the PDN. Consequently all the communications between capturing points and the monitoring centre must be encrypted.

3-2- Designed requirements:

1- Modular design: the system design must be modular, with scalable and upgradeable software and hardware, so that it has the ability to monitor the future Internet service. The bidder has to provide a clear description of the upgrade means which shouldn't result in a considerable modification in the current services and not affect the overall performance of the system. The upgrades should be done without the need to stop the whole system or any of its sensitive functions, except in cases where a full reinstallation is needed.

2- Network equipment manufacturer independence: It is not permissible for the system to depend on the availability of nonstandard or vendor specific

- Providers of Internet via satellites (with terrestrial upload and satellite download).
- VSAT systems linked to the central node which will be installed in STE.
- Customers connected to the network regardless of their ways of connection (WIMAX – GPRS –DIALUP – DSL – LL – ISDN – and WIFI).

2- It is preferable that the system is independent of the service providers as much as possible. The amount of equipment to be installed at the ISP premises should be minimal if needed. This equipment should be immune against hacking, tampering or inspection of its content, and the ISP should not be able to know the data being gathered and collected.

3- There should not be any interference of the monitoring system with the network functions or the monitored network performance. Monitoring activities should be fully transparent for all parties so the user cannot feel he is being monitored.

4- All monitoring activities should be done undetected, neither by the monitored targets, nor by ISPs, and not even by the management of the PDN. Consequently all the communications between capturing points and the monitoring centre must be encrypted.

3-2- Designed requirements:

1- Modular design: the system design must be modular, with scalable and upgradeable software and hardware, so that it has the ability to monitor the future Internet service. The bidder has to provide a clear description of the upgrade means which shouldn't result in a considerable modification in the current services and not affect the overall performance of the system. The upgrades should be done without the need to stop the whole system or any of its sensitive functions, except in cases where a full reinstallation is needed.

2- Network equipment manufacturer independence: It is not permissible for the system to depend on the availability of nonstandard or vendor specific

3- Chatting rooms with its two types: through specialized web sites, or through special applications.
4- File transfer (FTP, TFTP).
5- Instant messaging services (like YAHOO MESSENGER, MSN, SKYPE) and all the annexed services, including:
    a. VOIP.
    b. Video.
    c. File transfer.
    d. Chatting.
6- SMS sent through the Internet.
7- Services of the internal Virtual Private Networks of the type MPLS VPN.
8- The ability to detect and distinguish encrypted communications like HTTPS, VPN, and SSL, etc… With the ability to decode its content in the case of knowing encryption keys are provided.
9- The system must be able to detect, distinguish and display the content of voice calls based on VOIP services which will be licensed to operate over the data network.
10- The bidder has to obligation to provide and install the upgrades which permit the monitoring of new services and the improvement the monitoring of current services which he will issue for five years at least.
11- STE may request during the lifetime of the system to develop software or make additional upgrading aiming at monitoring of specific services. The bidder has to be committed to that, except the case where this is not technical feasible, and in such cases the non-feasibility has to be demonstrated.

3-4- Requirements of capturing data

1- Capturing data must be done transparently and in a passive, non-intrusive way.
The parameters represented in this paragraph are the minimum requirements .
The bidder has to mention clearly the maximum limits of the system which will be installed, and expansion requirements and mechanisms.

2- The monitoring system should be able to capture, analyze and archive the data from the monitored network according to the following definitions:

1- URL (200 addresses).

2- Free E-mail address, example: when adding @hotmail.com he can capture all the incoming and outgoing traffic to the Hotmail email and with the possibility of using wildcards (500 strings).

3- IP address (single and range), (200 IP).

4- Mac addresses (500 Mac addresses).

5- Port number (200 addresses).

6- IP address with port number (50 addresses) taking into consideration storage of captured data according to item 3, 4, 5 and 6 in files that have standard format (example: pcap).

7- User name (500 users).

8- Phone number (fixed phone or mobile) (500 numbers).

9- Name of application (example: MESSENGER, MSN, SKYPE, YAHOO MESSENGER, PALTALK, FTP, TFTP and VPN), (500 application). Applications should be identified by their traffic signature and not by port number.

10- A set of random key words (example: the word "terrorism" in the context of E-mail (electronic mail), (100 word simultaneously).

3-5- Special requirements

1- The delay separating the collection of data and displaying it should be in the order of a few minutes (except hot targets).

2- The system must allow the definition of a certain number of hot targets whose activities should be monitored in real time. The bidder should specify the number of hot targets, minimum requirement is 50.

3- The system must provide the possibility of identifying hot targets according to the following parameters:

a. Phone number

b. IP@

c. Subscriber account.

d. E-mail address.

4- The activities of hot targets will be displayed on special terminals with a sound alarm. It is preferable that sound alarms could be programmable.

3-6- requirements of storing data

The resulted data from monitoring the previous services is stored in a database, so that the data remains available in the database for a period not less than 12 months, after that it will be exported to a special archive system. The database must have high performance and a quick response time.

1- The database is required (with all its software and hardware) to have sufficient capacity to store the resulted traffic from the mentioned monitoring services in item (3-3) and according to the mentioned conditions in item (3-4) for 500000 (five hundred thousand) DSL users with an average of speed 512 Kbps and for 50000 (fifty thousand) dialup phone connections .

2- The data base contains the data in its complete form (example: an E-mail message with all attached information).

3- The data base must be expandable to upgrade and store the resulted data from 10000000 broad bands DSL at the same speed and also the previous services.

4- The archive system receive the data from data base to store it in a secondary storage unit, it also makes an issue of a special patch which clarifies starting and ending date of the archived data with a serial number.

5- The archived system is connected to a special terminal to search into the archive

6- the bidder has to supply the archive system with (jukebox) system

3-7 : description the monitoring interface

The system is required to support up to 20 monitoring terminals and has the ability to connect with 40 terminals. The GUI should be web-based and contain the following pages

1- Login page:

It is the regular login page, which include username and password.

2- The page of parameters for capturing data.

The user can login to this page through special username and password to communicate with the system in order to set data capturing parameters. It should also be possible to specify the timing of the start and stop of data capturing.

3- The page of configuring the monitored targets:

This page is specialized in configuring targets which required to monitor its activities include the different services.

Also the system should permit to follow up the subscriber from the following:

a- Phone number.

b- the account name

c- E-mail address.

d- IP address.

e- Set of keywords

The system will record the activities of this targets automatically, and it is possible to define the important required targets to be followed up within the real time.

4- Page for tracking targets .

This page displays the different activities of the followed up targets and classifies it according to the kind of every target in an independent way with user related information , it is possible to transport the result to the printer or to secondary storage (e.g. :CD) or send it to a specific file .

5- a page for free search :

This page allows to make search within the recorded data for all categories which are being monitored during a certain timeframe, this search includes the following:

A : the search according to a set of keywords. The user is free in making the search within the captured activities of the monitoring services. like searching within the added comments to web sites or within the instant massages and other recorded texts.

B: search according to E-mail addresses:

This allows user to select searching within the sender or the receiver fields or carbon copy or the massage text or all of them at the same time.

C: the search according to phone number or username:

for all the previously mentioned activities and that user should be able to select the activity to search within , like searching for all incoming and outgoing email massages related to the user of a phone number, idem for browsing , adding comments and the instant massages and the other required activities for monitoring .

D: searching according to IP or port number:

This page displays all the data related to the IP in a standard way for the known applications, especially monitored applications like (E-mail , browsing , comments and instant massages, etc).

As for the non-standard applications they data should be displayed in a standard analyzing format depending on the protocols (e.g.: display the fields of TCP/IP).

E: according to application name :

The user selects an application name and the system should display all users of this application and the content of their data, like using MSN MESSENGER, or selecting VPN to know people and IPs which are using this service.

6 - Access log file:

This page contains all access logging data for all the users of service providers including the records of the central RADIUS server of the PDN.

This aims to have the ability to know the user of a specific IP @ within certain timeframe. This page should provide all possible searching options.

د.إباء عويشق	م. علي علي	م.مازن محمد
26/07/2007		