Corrigendum -IV

Sub: Request for proposals for "**Supply, Installation, Integration, Customization, Testing, Training & Commissioning of AAA and B/OSS Infrastructure for Wi-Fi and Broadband Services for RailTel**"

Ref: i) This office Tender No. RAILTEL/TENDER/OT/CO/DNM/2017-18/AAA and BSS&OSS/389 Dated: 19.05.2017

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

1.   **Clause no. 18.2 of Pre-Qualification Criteria (PQC) may be read as:**

   i. SI's experience in implementation of AAA and B/OSS Infrastructure System with Indian/Global Telecom Service Provider or Government Organization: references required. Confirmation from Telecom Operator/System Integrator who has deployed.

2.   **Clause no. 18.3 of Pre-Qualification Criteria (PQC) may be read as:**

   i. OSSP/OEM's reference for AAA and B/OSS Infrastructure System with Indian/Global Telecom Service Providers or Tier-1 or Tier-2 Telecom Service providers or Government Organization.: references required. Confirmation from Telecom Operator/System Integrator who has deployed the Solution.

3.   **Clause 2.1.1 Techno-Commercial Capability- Product supplier's Credibility, Chapter-4B may be read as:**

   a. For point **Product supplier's Credibility** No. of References in Telco environment with scale of 1 Lakhs Concurrent Users / 5 Lakhs Subscriber users is required from a single operator. Confirmation from the Telecom Operator/System Integrator who has deployed the solution of this Scale.
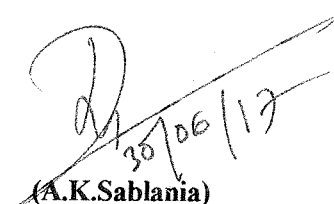
4.   **Clause VIII Point 4 Chapter 2 ,Schedule of Requirement may be read as:**

    4. Installed Hardware and Software should support 100% of the capacities requirements for AAA and IP   Logger above from Day 1. Hardware make should be present in the Gartner report under leaders Quadrant for Servers. Third party Licenses/Operating Systems should be enterprise version and must have professional Support Services from OEM

5.   **Clarification against Point no. 13, Clause 1.3 Technical Capabilities, chapter-4B:**

    NAT and protocol based log monitoring scope is defined in Annexure-I of corrigendum-IV and should quote commercials accordingly.

6.   All other terms and conditions will remain same.

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

NAT and protocol based log monitoring System

1. The system must be able to accept Netflow data from Cisco routers, Cflowd from Juniper and Alcatel routers and Sflow data from Foundry or other Sflow based routers. The system must support Netflow versions 1, 3, 5, 7 or 9, Cflow versions 5, 9 and Sflow version 2, 4, 5 and IPFIX.

2. The solution must be able to collect and process up to 100k concurrent users flows (100 Nos average flows per minute assumptions may taken for one user) .The solution should be scalable to support 500k concurrent user flows .

3. The system must be able to replicate ("tee") received Netflow data and export it to other Netflow receivers in the network.

4. Deleted

5. The collector shall be supplied as software installable version on Linux x86-64 based servers.

6. The collector should be able to function as a store and forward node. This is required when flows need to be aggregated per Internet Gateway and processed at a central location at DC and DR . This is also needed to ensure no logs are lost of the central log collection facilities become unreachable due to interconnect issues. Collector should be able to store the data for one days. Recommended topology is given below :-
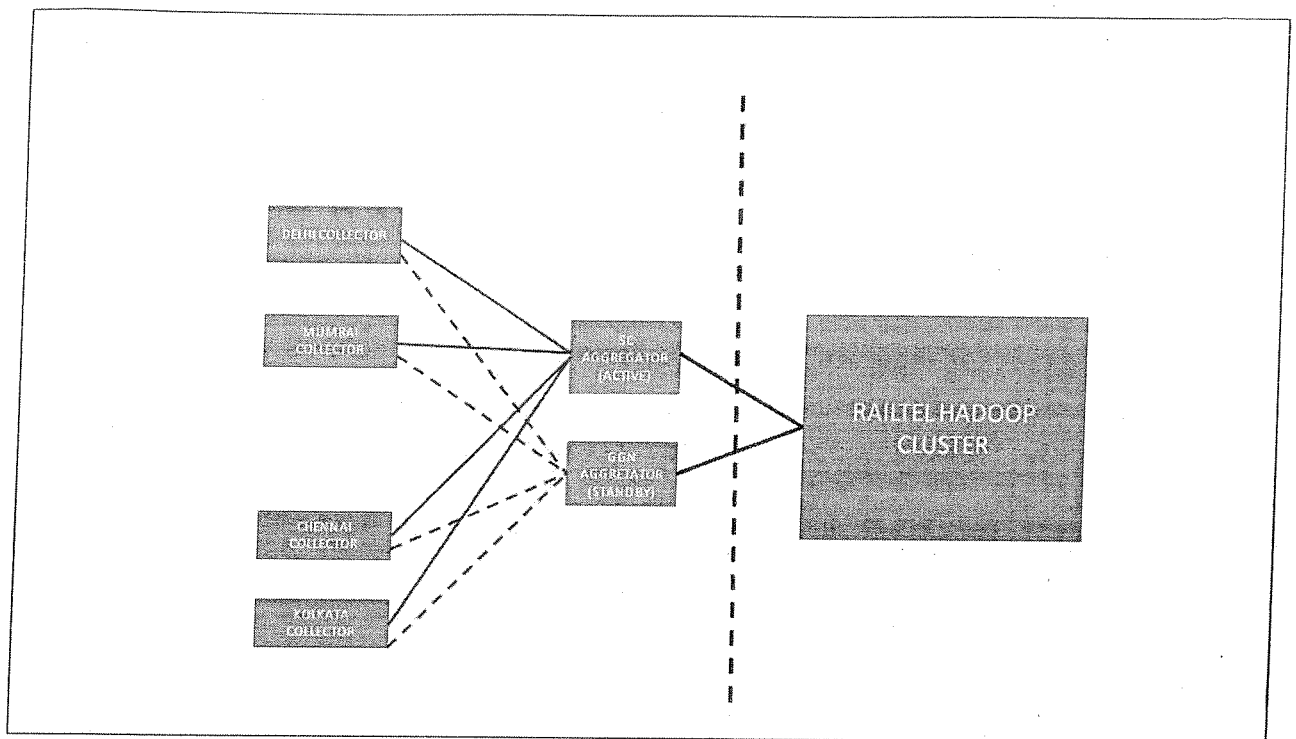
7. Each collector node should be able to injest IPFix/Netflow data from at least 100 network nodes .

8. The following RFCs should be supported the IPFix/Netflow nodes

   a. RFC 7011 - Specification of the IP Flow Information Export (IPFIX/NETFLOW) Protocol for the Exchange of Flow Information

   b. RFC 6313 - Export of Structured Data in IP Flow Information Export (IPFIX/NETFLOW).

9. Collector Protocols. The collector shall be able to collect IPFix/Netflow data over the following protocols:

   a. UDP
   b. TCP
   c. TCP with TLS 1.1 or better
   d. SCTP

10. Multiple Collectors should be able to work as a cluster to share load from different exporters.

11. It should be possible to configure ACL (Access Control Lists) for collectors from the management UI.

12. Health statistics of each collector in the cluster should be available, and should measure at least the following:
    a. Number of exporters concurrent (for UDP, a configurable timeout after which the exporter should not be counted as active)
    b. Number of IPFix/Netflow records exported in that session
    c. Number of IPFix/Netflow records not processed due to unknown template
    d. Number of IPFix/Netflow records processed.
    e. The system must be able to generate an alert due to a system error/over-load condition, e.g. process error, not getting flows and etc

13. Installation of the collector may be via CLI, however all management and operators of the collector shall be through WEB-GUI only.
14. Management Application

    a. Application should be driven via a roles and rights managed system
    b. Authentication of users shall be configurable and should support external LDAP/Active Directory .
    c. Management application should be able to manage stored data, it's archival, restore from archives and general information about it.

15. Deleted .
16. Security – TLS mode
    a. It should be possible to create a CA and issue certificates.
    b. It should be possible to install public certificate of a CA to ensure only devices with certificates from trusted sources are accepted
17. Reports – Following analytics must be available
    a. AS number source and destination matrix based on packets and bytes (volume of traffic)
    b. Top sources (IPv4 & IPv6) and top destinations (IPv4 & IPv6)
    c. URLs, FQDNs from URLs
    d. Top utilization by username
    e. NAT Utilization Report
    f. Ability to schedule report and FTP/Emailed
    g. Trends and reports for volume of data stored, archived and available
18. High Availability
    a. Data should be stored internally in format that is resilient to failure of storage nodes. An example of this is storing data in backend with concepts of shards and replica sets.
19. Data Search
    a. Data should be searchable on all attributes present in the flows as sent by network devices .
    b. Data should be searchable on all meta attributes of the flows such as AS numbers, zone the network device is installed in.
    c. Since the quantum of data can get quite large, it should be possible to set searchable indexes per device, per day/hour
    d. These search indexes should automatically be archived to reduce storage overhead and search scope.
    e. It should be possible to move the archival data to Hadoop's HDFS . It should be possible to integrated with RailTel Hadoop's HDFS.
    f. It should be possible to use large file systems to move indexes to for off-search-index storage. It should be possible to move such indexes back to searchable scope via admin GUI.
    g. It should be possible to move the archival data in JSON ,binary ,text and csv format for external HDFS/storage for archival. Data may be stored in binary format while it is being transmitted from store-and-forward node to main cluster.
    h. It should be possible to move the Netflow data automatically to external storage based on user Source IP Range .
    i. it should be possible to enrich the flow data by storing username based on source IP address.
    j. Data should be searchable for NAT logs present in the flows as sent by network devices . The following fields MUST be searchable
        a) Source IP with Username (In case of Broadband User . Radius Accounting Logs should be integrated with searchable engine) .
        b) Source Port
        c) Destination IP
        d) Destination Port
        e) NATed IP
        f) NATed Port

k. Search shall be type specific.
    i. IPv4/IPv6 address attributes, it should be possible to search by single IP or subnet
    ii. Text attributes: exact, substring, case sensitive and case non-sensitive

20. Product installation
    a. It should be possible to install the product on dedicated servers.
    b. Product should be provided as docker images or virtual machines.

21. Deleted

22. APIs
    a) All management functions should be usable via external API clients.
    b) RESTful API should be provided.

23. Capacity Required

    a) The Netflow/IPFIX collector should be provide at Delhi , Mumbai ,Chennai and Kolkata . The Netflow/IPFIX collector should support following minimum configuration.

1	Minimum Flow receive rate Per Collector/receiver at Delhi, Mumbai ,Chennai and Kolkata .	Min 100k Flows/Second
2	Searchable Flows within the platform	1 TB with RAID and 500 GB SSD cache .
3	Network Interfaces – Flow Collector/receiver	Min 2x10G ports
4	Network Interfaces – Management	1G or 10G Multiple Ports.
5	Redundant Power Supply	AC
6	Management Interface	Yes

    a) Centralized Systems at DC and DR for Aggregator/Management application should be provided at Gurgaon and Secundrabad with following minimum configuration.

1	Storage Capacity	50 TB with RAID for searchable data .
2	Management Interface	Yes
3	Network Interfaces	Min 2x10G ports
4	Network Interfaces – Management	1G or 10G Multiple Ports.
5	Redundant Power Supply	AC