PAKISTAN TELECOMMUNICATION COMPANY LTD.
HEADQUARTERS, G-8/4 , ISLAMABAD

RFI (REQUEST FOR INFORMATION) FOR AAA AND DNS SOLUTION SETUP

1. PTCL is seeking information from the original manufacturers/authorized distributors/suppliers etc. for a state of the art AAA and DNS solution for its enterprise and corporate requirements.
2. This Request for Information is an information gathering process in which PTCL seeks to collect information and opinions from the industry best brands of AAA and DNS solution. This request for information does not constitute a Request for Proposal (RFP) or a promise to issue an RFP in the future. This request for information does not commit the PTCL to contract for any supply or service whatsoever. PTCL will not pay for any information or administrative costs incurred in response to this RFI; all costs associated with responding to this RFI will be solely at the interested party's expense. However, this RFI and the responses provided may be used a precursor to a procurement process.
3. Interested party may obtain the detailed requirement documents for AAA & DNS upon a formal request to contact detail given in this RFI Notice. The proposals in response to this RFI (technical + high level costing comparison of intended solution), prepared in accordance with the instructions provided for AAA and DNS solution, must reach at PTCL HQ in the O/O GM Procurement (Business Support) on or before 12:00 Hours February 06, 2020. Those Vendors unable to submit the proposed solution in Hard Copy, may send scanned copy of the proposed solution along with the soft copy in Word Format.
4. The PTCL will treat all responses confidentially. Proprietary information, if any, should be minimized and must be clearly marked. PTCL Technical representatives may or may not choose to meet with potential offerors. Such discussions would only be intended to get further clarification of potential capability to meet the requirements.
5. The information provided in the RFI and attached documents is subject to change and is not binding on the PTCL. The PTCL has not made a commitment to procure any of the items discussed, and release of this RFI should not be construed as such a commitment or as authorization to incur cost for which reimbursement would be required or sought. All submissions become PTCL property and will not be returned.

SM Procurement (Business Support)
Room# 18, 4th Floor, Old Building
PTCL H/Qs, G-8/4, Islamabad
Email: tanvir.ahmad@ptcl.net.pk
Tel: +92-2283123

PAKISTAN TELECOMMUNICATION COMPANY LTD.
HEADQUARTERS, G-8/4 , ISLAMABAD

AAA RFI

1. Solution should support integration with Multi-vendor BRAS
2. Solution should support 3rd party systems integration.
3. Solution should support fixed, wireless, Wi-Fi and 3g offload technologies.
4. Solution should support OSS integration.
5. Solution should support COA features.
6. Solution shall support integration with external database.
7. Solution should support 2 Million subscribers
8. Solution should support Geo redundancy
9. Solution should support dynamic profiling.
10. Solution should support RADIUS and Diameter.
11. Solution should support integration with OCS (online Charging System)
12. Solution should support customizable handling flow
13. Solution should support all AAA related RFCs.
14. Solution shall support centralized monitoring and reporting system.
15. PTCL intends to provide this solution as a managed services solution to other customers.
16. NFV based solution is preferred.
17. Industry Wayforward for AAA vs PCRF functionality.

DNS High Level Scope

1. The proposed solution should be carrier grade, highly resilient and highly available with auotmated failover.
2. Single Tiered architecture/solution is required with detail design. Proposed solution shall be extremely resilient aganist any type of failure and fault with 100% availability.
3. The proposed solution can support Authoritative & Caching/Recursive DNS functions.
4. The proposed solution should be NFV based.
5. The total capacity of the offered solution must be capable to manage 3 million concurrent subscribers scalable upto 6 million and at least 7.2 million DNS QPS.
6. Solution must be capable of recomended Query per second standard for above-mentioned subscribers.
7. PTCL intends to offer this as a managed services solution to other customers.
8. Solution should support multi-tenant solution.
9. DNS Recursive support for ECS (EDNS Client Subnet).
10. Vendor to provide Solid References within Service Providers customers across the region
11. The solution to handle IPv4 DNS queries (all query types)
12. The solution to handle IPv6 DNS queries (all query types)
13. The solution to working in IPv4, IPv6 and IPv4v6 dual stack mode (all query types).
14. The solution to work as DNS64 (all query types).
15. Solution must support standards-based DNS services.
16. Single management interface for complete solution.
17. Product must support distributed Anycast for DNS.
18. Product must automate common tasks such as glue A record creation to prevent errors
19. Product must automate common tasks such as maintaining synchronization between forward and reverse records
20. Product must support the ability to manage the data hierarchically with over-rides at device/zone/record level
21. Product must support the ability to centrally manage name server groups which can applied to zones
22. Product must support adding the following types of DNS records: A, AAAA, MX, CNAME, DNAME, TXT, SRV, PTR
23. Product must allow adding the following types of zones: Forward Mapping (Authoritative, Forward, Stub), Reverse Mapping (IPv4 and IPv6)
24. Product must support access control lists (ACLs) for Zone Transfers.
25. Product must support access control lists (ACLs) for queries.
26. Product must support access control lists (ACLs) for recursive queries
27. Product must support BIND's views feature
28. Product must support the ability to have records shared between views and zones (similar to the BIND $INCLUDE statement)

29. Product must support the ability to centrally manage, configure and report on compliance with RFC-based and customer-defined hostname checking policies (Strict, Allow Underscore, etc.)
30. Product must support enforcing configurable restrictions on the format of hostnames to comply with RFCs and internal company policies
31. Product must support incremental zone transfers
32. Product must support the ability to delegate administration for individual DNS objects
33. Product must allow for recursive only service.
34. Product must allow for authoritative only service.
35. Product must support the ability view DNS syslog messages
36. Product must support EDNS0
37. Product must support a recent version of BIND 9, at least 9.3.0
38. Product must support an advanced forwarder selection algorithm, such as choosing a forwarder according to roundtrip time
39. Product must support diagnostic capabilities such as DNS query latency monitoring
40. Products must be available in different sizes for queries per second
41. Must support DNS Firewall using industry standards RPZ feeds.
42. Must support vendor supplied and external RPZ feeds.
43. Vendor must provide and support high quality dynamic malware data feed with frequent updates
44. Vendor must be capable to integrate with 3rd party feeds via Response Policy Zones (RPZ)
45. Vendor must have tool that security analysts can use to report on why domains were classified as malicious by the DNSFW/threat feed (Threat Lookup)
46. Vendor must have reporting tool to summarize and report on locally sourced malicious traffic, e.g. Top malicious domains, Top clients that tried to communicate to malicious domains, etc.
47. Must be able to balance GTP tunnels across multiple gateways
48. Must be able to detect GTP availability of gateways and remove broken gateways from the DNS responses.
49. Must provide the hardest security to withstand volumetric and DNS based attacks
50. Must avoid operator error at data entry.
51. Must support role based access control
52. Must provide an audit trail of all moves adds and changes.
53. Support for DSCP
54. Solution must support algorithmic pre-fetching of frequent domains
55. Solution must support retaining the last cached value for a Resources Record when an authoritative DNS is offline
56.
57. Must have the capacity to provide high geographic availability by using Anycast
58. Accepting dynamic DNS updates (DDNS) in real time
59. Detection and mitigation of DNS security attacks, with the ability to alert via SNMP and / or e-mail
60. DNSSEC configuration (signing and maintenance of zone signatures) according to NIST-800-81, with automated mechanisms to eliminate manual operations
61. DDNS updates with GSS-TSIG from Microsoft clients to the DNS server

62. Zone blocking, which allows a single administrator to modify a zone to the time
63. DNS redirection and filtering
64. Host name templates, which allow the rules of those names to be applied
65. Propose solution should be fully compliant with all RFC.

NFV DNS

1. The solution must support virtualized DNS service (aka VNF)
2. A single Management framework must accommodate virtual and physical appliances.
3. Describe the licensing model for virtual deployment.
4. License has to be align with a model based on "Pay as you Grow" and capacity model, independent of number of appliances deployed
5. The solution must be compliant to the ETSI MANO reference standard. Describe the details
6. The solution must support private/hybrid clouds deployment
7. The appliance must support virtualize based on NFV ETSI standards
8. The solutions must offers centralize management with rich FCAPS (Fault, Configuration, Accounting, Performance and Security Management) and software life cycle facilities.
9. The solution has to provide unified management between NFV infrastructure and physical infrastructure.