रेलटेल कॉर्पोरेशन ऑफ इंडिया लिमिटेड
(भारत सरकार का एक उपक्रम)

**RAILTEL CORPORATION OF INDIA LIMITED**
**(A Govt. of India Undertaking)**

# ELECTRONIC TENDER DOCUMENT

**FOR**

ई-ऑफिस प्रोजेक्ट के संदर्भ  में “डाटा सेंटर (डीसी और डीआर) की सुरक्षा समाधान की आपूर्ति , स्थापना, परीक्षण और कमीशन हेतु” निविदा दस्तावेज

**Tender document for Supply, Installation, Testing & Commissioning of Security Solution for Data Center (DC & DR) against e-Office Project**

**E-निविदा संख्या: RAILTEL/TENDER/OT/CO/DNM/2018-19/Security Solution for DC & DR/476**

**OPEN E-TENDER NO. RAILTEL/TENDER/OT/CO/DNM/2018-19/ Security Solution for DC & DR/476**

निविदा दस्तावेज की कीमत: रु. 11,800/- (टैक्स सहित)
**Cost of Tender Document: Rs. 11,800/- (Including Taxes)**

**Sold to ______________________**

**RailTel Corporation of India Ltd.**
**Plot No. 143, Institutional Area, Sector -44**
**Gurgaon-122003, Ph: 0124-4236085-86, Fax: 0124-4236084**

**E-Tender Notice No.: RAILTEL/TENDER/OT/CO/DNM/2018-19/Security Solution DC & DR /476 Dtd. 02.04.2019**

RailTel Corporation of India Ltd. (RailTel) invites E-Tenders in Two Packet (Part I –Credential/ Techno commercial Bid and Part II - Price Bid) System for **“Tender document for Supply, Installation, Testing & Commissioning of Security Solution for Data Center (DC & DR) against e-Office Project”**.

| | | |
|---|---|---|
| a) | Opening date of Tender downloading | 02.04.2019 |
| b) | Submission date of bids | 25.04.2019 up-to 15:00 hrs. (Online) |
| c) | Opening of bids | 25.04.2019 at 15:30 hrs (Online) |
| d) | Approximate cost of Tender | Rs 22.22 Crore approx (Inclusive All.) |
| e) | Earnest Money (EMD) | Rs 12,61,000/- to be made in favor of RailTel Corporation of India Ltd. in the form of DD payable at New Delhi. |
| f) | Cost of Tender Document is Rs.11,900/- (Including Tax) | |

# Small scale Units registered with NSIC under single point registration scheme are exempted from cost of Tender Documents and EMD.

**Note:** Tender Notice and Tender Document are available on RailTel’s website and can be downloaded from **www.railtelindia.com** or from the e-Tendering portal https://www.ireps.gov.in. For online bid submission the bidder will have to necessarily download an official online copy of the tender documents from IREPS e-portal. All future Information viz. corrigendum /addendum/ amendments etc. for this Tender shall be posted on the e-Tendering Portal only. Printed copy of Tender document will not be sold from RailTel office.

The bidder shall bear all costs associated with the preparation, submission/participation in the bid. Purchaser in no way will be responsible or liable for these costs regardless of the conduct or outcome of the bidding process.

## INDEX

## CHAPTER-1

## OFFER LETTER

RailTel Corporation of India Ltd.
Plot No. 143, Institutional Area,
Opposite-Gold Souk,
Sector-44, Gurgaon-122003

1. I/We ______________________________________________ have read the various conditions detailed in tender documents attached here to and hereby agree to ABIDE BY THE SAID CONDITIONS. I/We also agree to keep this offer open for acceptance for a period of 60 days from the date of submission and in default thereof. I/We will be liable for forfeiture of my/our Earnest Money. I/We offer to supply various equipment at the rates quoted in the attached schedules and hereby bind myself/ourselves to complete the work of **"Tender document for Supply, Installation, Testing & Commissioning of Security Solution for Data Center (DC & DR) against e-Office Project"** within 120 days from the date of issue of Purchase Order. I/We also hereby agree to abide by the Various Conditions of Contract and to carry out the supplies according to the Specifications for materials and works laid down by the RailTel.

2. Earnest Money of Rs………… has been submitted through IREPS portal with the following transaction details:

   The full value of Earnest Money shall stand forfeited without prejudice to any other rights or remedies if, I/We withdraw or modify the offer within validity period or do not deposit the security deposit (Performance Bank Guarantee) within specified days as per tender after issue of Purchase Order/LOA.

SIGNATURE OF SUPPLIER (S)

Date:

CONTRACTOR (S) ADDRESS

SIGNATURE OF WITNESS:

1.

2.

## CHAPTER- 2

## SCHEDULE OF REQUIREMENT

| SOR | | Item Description | UOM | Qty | Unit Rate (All inclusive) (in Rs.) | | Total Cost (in Rs.) | |
|---|---|---|---|---|---|---|---|---|
| | | | | | In fig | In word | In fig | In word |
| **SOR-A** | **1** | Data Centre Router as per technical specification given in Chapter-3A | **Nos** | **04** | | | | |
| | **2** | L3 Switch with redundant power supply as per technical specification given in Chapter-3A | **Nos** | **04** | | | | |
| | **3** | UTM Solution along with other appliances as per technical specification given in Chapter-3A | **Set** | **02** | | | | |
| **SOR-B** | **1** | Core Switch as per technical specification given in Chapter-3A | **Nos** | **04** | | | | |
| | **2** | Internet Firewall as per technical specification given in Chapter-3A | **Nos** | **04** | | | | |
| **Sub Total** | | | | | | | | |
| **SOR-C** | | **Incremental% AMC cost** in addition to 3.5 % mentioned in clause 3.8 of Chapter-3 | **Years** | **05** | | | | |
| | **Grand Total** | | | | | | | |

| Note: | |
|---|---|
| I. | a) Unit rate quoted against SOR above should be CIP destination inclusive of all duties, taxes, insurance and freight etc (with tax break-up as per Performa attached as Annexure-A). The materials as per SOR are required to be delivered within the delivery period as indicated in Bid Data Sheet (BDS, Chapter 5) to the sites as per Annexure-I.<br>b) It shall be the responsibility of Tenderer to transport the equipment to site for Installation & Commissioning. |
| II. | Tenderers should submit the detailed configuration of each type of equipment indicating quantities of various modules/sub modules/cards/Licenses/sub racks including the vacant slots in the sub racks/chassis for further expansion. Detail BOM of each equipment supplied under the contract shall be submitted along with the bid and the same shall be duly vetted by the OEM. |
| III. | The Tenderer shall attach Unit Rate Analysis of Schedule of Requirements (cost of each sub-assembly, card, module, Licenses etc.) in their Price Bid. The quoted Unit Rates should correspond to the referred unit Rate. |

| | |
|---|---|
| IV. | Tenderer must also furnish unit rate of all the supply of items mentioned in the SOR, which will be required for the Solution. These will also form part of the Rate Contract for procurement of items as when required. |
| V. | The tenderer will be fully responsible Supply of Equipment/cards/interfaces and all related items for installation and commissioning of the network including the following:<br>a) Integration with existing Network as required.<br>b) Spares required for Commissioning, maintenance supervision & warranty period shall be maintained by the Contractor at his own cost.<br>c) All necessary cables and connectors and other accessories required for installation. |
| VI. | Tenderer should be an Original Equipment Manufacturer (OEM) or Authorized representative of OEM |
| VII. | The Bidder should have authorization specific to this tender from respective OEM. Bidder has to quote only one OEM against one SOR |
| VIII. | Bidder has to quote for all SOR and evaluation will be done on totality. However, PO for SOR-A and SOR-B will be issued separately. |

*****************

## Annexure-A
## Tax Breakup for SOR

| SOR | | Description | Total Qty | Basic Unit Price (exclusive of all levies and charges) | Pkg & Forwarding Charges | | Freight & Insurance Charges | | CGST/SGST /IGST/UTGST etc. | | Price Per Unit (all inclusive) for delivery at destination (4+6+8+10) | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | % | Amt | % | Amt | % | Amt | % | Amt |
| 1 | | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| SOR-A | 1 | | | | | | | | | | | |
| | 2 | | | | | | | | | | | |
| | 3 | | | | | | | | | | | |
| SOR-B | 1 | | | | | | | | | | | |
| | 2 | | | | | | | | | | | |

## Chapter - 2-A

**These are the Special Instructions to the Bidders for e-Tendering.**

**Note:- E-Tendering Instructions to Bidders terms given in others chapters shall be superseded by the terms given in Chapter-2 A.**

1. **Order of Priority of Contract Documents:**

Where there is any conflict between the various documents in the contract, the following order of priority shall be followed i.e. a document appearing earlier shall override the document appearing subsequently:

a) Agreement
b) Letter of Acceptance of Tender
c) Notice Inviting Tender
d) Bid Data Sheet
e) Schedule of Requirements
f) Instructions to the Bidders
g) Annexure/Appendix to Tender
h) Form of Bid
i) Commercial Terms and Conditions of the Contract
j) Technical Specifications
k) Relevant Codes and Standards
l) Drawings

2. **Submission of Bids only through online process is mandatory for this Tender**

E-Tendering is a new methodology for conducting Public Procurement in a transparent and secured manner. Now, the Government of India has made e-tendering mandatory. Suppliers/ Vendors will be the biggest beneficiaries of this new system of procurement. For conducting electronic tendering, RailTel has decided to use the portalhttps://www.ireps.gov.in, Indian Railways E-Procurement system (IREPS).

Benefits to Suppliers are outlined on the Home-page of the portal. Bidders are advised to visit the IREPS Portal for details related to E-Tender i.e. Registration, FAQ, Helpdesk, Learning Center etc.

3. **Tender Bidding Methodology:**

Sealed Bid System - ‘Single Stage - Two Envelope’: In this, bidder has to submit each the bid (Part I –Credential/ Techno commercial Bid and Part II - Price Bid) in separate envelope “ONLINE”.

**IREPS Helpdesk**

Please visit Helpdesk section on IREPS Portal.

**RailTel Contact-I (for general Information)**

RailTel’s Contact Person /Designation
Rajeev Kumar, Sr. Manager/DNM
Telephone/ Mobile: 9717644419
E-mail ID: rajeevkumar@railtelindia.com

**RailTel Contact-II (for general Information)**

RailTel's Contact Officer
A. K. Sablania, ED/DNM
Telephone/ Mobile: 9717644015
E-mail ID: asablania@railtelindia.com

## 4. Bid related Information for this Tender (Sealed Bid)

The entire bid-submission would be online on IREPS Portal.

Broad outline of submissions are as follows:

a. Submission of Bid Security/ Earnest Money Deposit (EMD)
b. Submission of digitally signed copy of Tender Documents/Addenda
c. Two Packet (Part I –Credential/ Techno commercial Bid and Part II - Price Bid)
d. Online response to Terms & Conditions of Tender.
e. (Optional) Online Submission of modification, substitution bids for technical or financial parts, or withdrawal bid.

**NOTE: Bidder must ensure that the bid must be successfully submitted online as per instructions of IREPS Portal.**

## 5. Offline Submissions:

The bidder is required to submit the following documents offline to RailTel Corporation of India Ltd, Institutional Area, Plot 143, Sector 44, Gurgaon, before due date & time of submission of bids specified in this tender document, in a Sealed Envelope. The envelope shall bear (the tender name), the tender number and the words 'DO NOT OPEN BEFORE' (due date & time).

a. EMD-Bid Security through IREPS Portal.

b. Power of attorney to be submitted in accordance with Clause-36.5, Chapter-4 of Tender Document.

c. In case bidder happens to be an eligible MSME, the documentary evidence for same shall be submitted.

d. Specific authorization addressed to RailTel from the OEM (Parent Company) for Indian Subsidiary (Clause 4.A.14 of Tender Document).

e. System Performance Guarantee (Form no. 2, chapter-6).

f. Deleted.

g. Declaration regarding acceptance of clarification issued from DoT (Clause 15 of Chapter-4, of Tender Document).

h. Complete technical data and particulars of the equipment offered, as specified in the Tender papers together with descriptive literature, leaflets, Drawings, if any, complete with list etc.

i. Passwords of Price Bid file in separate sealed envelope.

**Format for Affidavit as per Form-4 failing which BID WILL BE SUMMARILY REJECTED.**

**NOTE:** The Bidder has to upload the Scanned copy of all above original documents (item-h optional) as Bid-Annexures during Online Bid-Submission.

6. **Submission of Eligibility Criteria related documents:**

Eligibility criteria related documents as applicable shall also be scanned and submitted ONLINE. Copy of these documents shall also be submitted in RailTel before Tender opening date & time. Bids without these off-line submissions are liable to be rejected.

**NOTE: In case of internet related problem at a bidder's end, especially during 'critical events' such as - a short period before bid-submission deadline, during online public tender opening event, during e-auction, it is the bidder's responsibility to have backup internet connections.**

In case there is a problem at the e-procurement/ e-auction service provider's end (in the server, leased line, etc) due to which all the bidders face a problem during critical events, and this is brought to the notice of RailTel by the bidders in time, then RailTel will promptly re-schedule the affected event(s).

7. **Instructions for Tender Document TO THE BIDDERS**

The RailTel Tenders are published on www.railtelindia.com and on IREPS Portalhttps://www.ireps.gov.in/. In addition to submitting the e Tender documents online, they should also submit a Demand Draft drawn in a scheduled bank in favour of "RailTel Corporation of India Ltd, payable at NEW-DELHI, towards the cost of the tender document.

**NOTE:** For online bid submission the bidder will have to necessarily download an official online copy of the tender documents from IREPS portal, and this should be done well before the deadline for bid-submission.

8. **Submission of Offers and Filling of Tender:**

This e-tender should be duly submitted online using the e-Procurement Portal https://www.ireps.gov.in/.For detailed instructions please refer to IREPS Portal.

9. **Fax Quotations & Late Tenders:**

Fax Tender documents and Late/Delayed tenders would not be considered.

10. **Attendance of Representatives for Tender Opening:**

Representatives of bidders desirous to attend the tender opening can do so on production of a proper letter of authority from the respective firm, failing which they may not be allowed to attend the tender opening. Authorized representatives of those firms who have submitted the tender documents alone shall be allowed to attend the tender opening.

11. **Addenda / Corrigenda:**

Addenda / Corrigenda to the tender documents may be issued by RailTel prior to the date of opening of the tenders, to clarify or reflect modifications in the contract terms and conditions or in the design. Such addendum/corrigendum shall be available on IREPS Portal only. Bidders who are unable or unwilling to bring their tenders to conform to the requirements of the RailTel are liable to be rejected.

**12. Ambiguity/ Pre- Bid Clarification Requests:**

If there is any ambiguity or doubt as to the meaning of any of the tender clauses/ conditions or if any additional information required, the matter should immediately be referred to the RailTel in writing through emails to RailTel Contacts defined above.

**13. Bid submission and Opening date**

a. The bid should be submitted online along with Credential/Techno commercial & Price bid document (all documents).

b. Power of attorney in favor of the signatory duly authorizing the signatory shall be submitted in a separate envelope to the tendering authority before the due date and time of submission of the e-Tender.

c. The bidder's bids will be opened at the time & date of opening of the tender given in the Bid Data Sheet (BDS) online simultaneous in presence of such Bidders/ Representatives who choose to be present online. The Tenders/Representatives can also choose to be physically present in the office of RailTel for the Online Public Tender Opening Event.

**d. Bids received after due date and time shall be summarily rejected and shall not be opened.**

## CHAPTER-3-A

### Technical Requirement

The bidder has to carry out following activities: -

1. Supply, Installation, Configuration, performance Tuning & Integration, Performance Testing, Acceptance Testing, Commissioning and Training of the supplied hardware, software, network equipment and network & security software as per Schedule of Requirements.

2. Bidder should have backend tie-ups with the respective OEMs to provide required technical support along with OEM professional services for the supplied Hardware, Software, Network equipment and Network & Security software for their installation, configuration, fine-tuning, integration with existing components and commissioning to meet the functional requirements. OEMs shall also be responsible for successful implementation and system operations.

3. Comprehensive Warranty support services of all supplied Hardware, Network equipment and Cabling for all the supplied Software and Network & Security software valid for a period of 36 months from the Date of System Commissioning or 40 months from the date of delivery to the site (Only in case the delay in system commissioning is on the part of consignee), whichever is earlier.

### A. Scope of Work

- Proposed Secure Data Centre solution should provide integrated protection and dynamic, intelligent control to defend against today's sophisticated attacks.
- solution should establish a true threat management system to detect threats and mitigate risk.
- Secure Data Centre delivers dynamic security capabilities, reduces complexity, and increases flexibility by coordinating security between Firewall, AAA, Network Behavior Anomaly detection and Endpoint.
- With integrated network access control technology, Railtel should be able to\ manually or automatically change users' access privileges (quarantine device) when there's suspicious activity, a threat or vulnerabilities discovered. Devices that are suspected of being infected can be denied access to critical data while their users can keep working on less critical applications.
- Solution should turn security intelligence and response technologies into an integrated operation to see and stop threats wherever and whenever they occur in network.
- The Data Centre Solution should have "Secure tool" should provide application insights and inventory across DC's using auto generated application discovery and dependency mapping for workloads in various Dev, Test, Pre-Prod, Prod and other DC zones. It should provide an always on application blueprint for ever changing application relationships and inter-dependencies.
- It should generate a whitelist policy based on real-time application behaviour and keep the policies up-to-date as applications evolves and more applications are added and modified. The tool should enforce the generated application whitelisted policy consistently across bare-metal, virtual and container workloads. It should track policy compliance.

- The tool should have the capability to track every process executed on the server and map behavior deviations instantaneously to malware execution patterns. It should provide high fidelity alters for both system generated and user defined events.
- It should provide accurate inventory of the installed software packages on the workloads to quickly identify any known vulnerabilities and exposures. It should then provide actions to quarantine or restrict communications based on vulnerabilities or vulnerability score.
- It should provide a always-on traffic search and analysis capability for tracking and monitoring application and network performance on a per flow basis between all DC and external endpoints for real time and historic traffic flow.
- The tool should be quoted as an appliance form factor, Scope should include monitoring and display of each and every process, process ID, Process owner, Process mapping running on the server (Physical / VM form factor). Solution must also display the Top 10 providers and consumers on the dashboard

Note 1: It may kindly be noted that in the specification wherever support for a feature has been asked for, it will mean that the feature should be available without RailTel requiring any other hardware/software/licenses. Thus, all hardware/software/licenses required for enabling the support/feature shall be included in the offer.

Note 2: Bidder should submit the vetted BOM from their respective OEMs.

Note 3: The Bidder should have OEM authorization specific for this tender.

Note 4: Bidder has to provide all type of SFP's of same OEM, Patch Cords and other items required for Installation and Commissioning of complete solution.

**SOR-A-1: Router**

| SN | Functional Requirements: |
|---|---|
| 1.1 | The following are the functional requirements to be met by the access router:- |
| 1.2 | The router shall have control processor (Control plane) and switch fabric (forwarding plane) redundancy, and PSU redundancy |
| 1.3 | The Core router must be based on architecture which does hardware based forwarding and switching. The processing engine architecture must be multi-processor based for enhanced performance. The Router should have multi-core Processor @ 2.1 GHz or more |
| 1.4 | The router must support intelligent traffic management and QoS features to allocate network resources on application needs and QoS priorities. |
| 1.5 | The Core router must have onboard support for intelligent traffic measurement and analysis. The router must support flow based traffic analysis feature. |
| 1.6 | The router must have hardware assisted Network Address Translation (NAT) capability as per RFC 1631. |
| 2 | **Router Architecture:** |
| 2.1 | Architecture: The architecture of the router must be modular and redundant. Router should have a dedicated data plane Processor, independent of the control plane Processor. The performance should be at least 100 Gbps or more. |

| | |
|---|---|
| 2.2 | Number of Slots: The router must be chassis based with minimum 3 numbers of Main interface slots. Only the main slots on the router chassis should be considered to comply with this requirement. All the 3 interface slots should be usable from day 1 |
| 2.3 | Router Processor Architecture: The router processor architecture must be multi-processor based and should support hardware accelerated, parallelized and programmable IP forwarding and switching. |
| 2.4 | Processor Redundancy Feature: The router must support processor redundancy (both route processor and switch fabric (forwarding plane)) in 1:1 mode to ensure high-availability of the system. The router in the event of failure of any one processor should switch over to the redundant processor without dropping any traffic flow. There should not be any impact on the performance in the event of active processing engine failure. |
| 2.5 | Hot Swap-ability: The router must support on line hot insertion and removal of cards. Any insertion line card should not call for router rebooting nor should disrupt the remaining unicast and multicast traffic flowing in any way. |
| 2.6 | The router clock must sync to the Network Time Protocol (NTP) server of the Service Provider through the WAN links. |
| 2.7 | The router should have minimum 8GB flash and 8GB DRAM. It should also support DRAM expandable to 64GB DRAM. |
| **3** | **Router Performance Parameter:** |
| 3.2 | Routing Table Size: The router must support 20,00,000 IPv4 and 2,00,000 IPv6 routes entries in the routing table from Day-1. Should support at least 50,000 multicast routes/destinations. |
| 3.3 | The router should support uninterrupted forwarding operation for OSPF, IS-IS routing protocol to ensure high-availability during primary controller card failure. |
| 3.4 | Router should support 26 Gbps of IPSEC performance and 8000 tunnels (internal/external). |
| 3.6 | The Router solution must be a carrier-grade Equipment supporting the following: |
| 3.7 | No single point of failure |
| 3.8 | In-band and out-band management |
| 3.9 | Software rollback feature |
| 3.10 | Graceful Restart for OSPF, BGP, LDP, MP-BGP etc. |
| 3.11 | The proposed router should support modular OS and simply the changes through In-Service OS upgrade mechanism |
| **4** | **Physical Interface Support:** |
| 4.1 | The router line card must support following interface as defined in the IEEE, ITU-T: |
| 4.2 | The router should have Short Haul SFP enabled on all ports. The Router should have at least 8 ports 1GE and 8 Port x10GE from Day-1. The router should have support of 40GE &100GE interfaces for any future upgrade with additional line card hardware in same chassis. |
| 434 | The router should support following interfaces: Channelized E1, Channelized POS STM1, Channelized POS STM16, POS STM 64, Fast Ethernet, Gigabit Ethernet, 10G Ethernet, 40G Ethernet,100G Ethernet, Channelized E1, |
| **5** | **Layer 3 Routing Protocols** |

| | |
|---|---|
| 5.1 | The router must support the IPv4 and IPv6 stack in hardware and software. It must support both IPv4 and IPv6 routing domains separately and concurrently. It must also support the ability to bridge between IPv4 and IPv6 routing domains. |
| 5.2 | The router must support RIPv1 & RIPv2, OSPF, BGPv4 and IS-IS routing protocol. |
| 5.3 | The router should support minimum 6000 VRF instances from day one |
| 5.4 | The Router should support 5 level of MPLS Labels lookup |
| 5.5 | The router should support maximum 64K number of MPLS Labels |
| 5.6 | MPLS OAM - LSP Ping/Trace route for MPLS core |
| 5.7 | Multicast VPN (mVPN) |
| 5.8 | The Router shall support dynamically established spoke-to-spoke VPN capabilities over public networks |
| 5.9 | The Router shall support GRE-based IPsec VPN |
| 5.10 | The Router shall support L2TP |
| 5.11 | The Router shall support for improvement of application performance and availability |
| 5.12 | The Router shall support selection of the best path for each application based upon reachability, delay, loss, jitter, MOS |
| **6** | **IPv6 Support.** |
| 6.1 | Should support IP version 6 in hardware. |
| 6.2 | Should support IPv6 static route, OSPFv3, IS-IS support for IPv6, Multiprotocol BGP extensions for IPv6, IPv6 route redistribution. |
| 6.3 | The router shall support dual stack IPv6 on all interfaces and IPv6 over IPv4 tunneling, IPv6 Multicast protocols – Ipv6 MLD, PIM-Sparse Mode, and PIM – SSM,Pv6 Security Functions – ACL, IPv6 Firewall, SSH over IPv6, MPLS Support for IPv6 - IPv6 VPN over MPLS (6VPE) Inter-AS options, IPv6 VPN over MPLS (6VPE), IPv6 transport over MPLS (6PE) |
| 6.4 | Support for IPv6 security – Access Control lists (standard & extended), SSH over IPv6. |
| 6.5 | The router should support for IPv6 Multicast. |
| 6.6 | Should support IPv6 stateless auto-configuration, IPv6 neighbor discovery and, Neighbor Discovery Duplicate Address Detection. |
| 6.7 | Should support IPv6 Quality of Service |
| 6.8 | Should support IPv6 dual stack |
| 6.9 | Should perform IPv6 transport over IPv4 network (6to4 tunneling). |
| 6.10 | Should support SNMP over IPv6 for management. |
| 6.11 | The router must perform Hardware assisted GRE tunneling as per RFC 1701 and RFC 1702. |
| 6.12 | The router must support router redundancy protocol like VRRP. |
| **7** | **Multicast** |
| 7.1 | The router must support Protocol Independent Multicast Dense Mode (PIM-DM) and Sparse Mode (PIM-SM). |
| 7.2 | The multicast implementation must support Rendezvous Points on both leaf and non-leaf nodes. |
| 7.3 | The multicast implementation must support source specific multicast. |

| | |
|---|---|
| 7.4 | The router must support multiprotocol BGP extensions for multicast. |
| 7.5 | The router must support multicast load balancing traffic across multiple interfaces. |
| 7.6 | The router must support RFC 3618 Multicast Source Discovery Protocol (MSDP). |
| 7.7 | The router must support Any cast Rendezvous Point (RP) mechanism using PIM and Multicast Source Discovery Protocol (MSDP) as defined in RFC 3446. |
| **8** | **Quality of Service:** |
| 8.1 | The router must be capable of doing Layer 3 classification and setting ToS/Diffserve bits on incoming traffic using configured guaranteed rates and traffic characteristics. The marking of the ToS/Diffserve bits should be non-performance impacting. |
| 8.2 | The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, MPLS EXP, DSCP and by some well known application types through Application Recognition techniques or Application Awareness techniques. |
| 8.3 | The router shall support Strict Priority Queuing or Low Latency Queuing to support real time application like Voice and Video with minimum delay and jitter. |
| 8.4 | The QoS policy in the router shall support dual Strict Priority Queue or Low Latency Queue per policy so that voice and video traffic can be put in different queue. |
| 8.5 | The router shall support congestion avoidance through WRED and selective packet discard using WRED through IP Precedence and DSCP. |
| 8.6 | The router shall support cRTP for VoIP. |
| 8.7 | The router should have support for minimum 8 queues per port |
| 8.8 | Scheduling should allow for round robin and weighted round robin. |
| 8.9 | The scheduling mechanism must allow for expedited or strict priority routing for all high priority traffic. |
| 8.1 | The scheduling mechanism must allow for alternate priority routing traffic necessary to keep from starving other priority queues. |
| 8.11 | All network based keep alives (PPP keep alives, OSPF LSAs, BGP updates etc) must be given the highest priority and route before any traffic type |
| 8.12 | The traffic must be able to be prioritized into 8 class types. Class types must be able to be mapped into 1 of 8 bandwidth constraints. Bandwidth Constraints should be assignable to in individual hardware queues. Oversubscription rates for bandwidth constraints should have local significance only. |
| 8.13 | The router shall support 200k queues to offer granular QoS, policing and shaping capabilities. |
| 8.14 | Queuing and Scheduling must be able to be configured on a per physical port or logical port |
| **9** | **Security Feature** |
| 9.1 | The router shall meet the following requirements for security – |
| 9.2 | The router shall support Access Control List to filter traffic based on Source & Destination IP Subnet, Source & Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc) and Port Range etc. |
| 9.3 | The router shall support time based ACL to reflect time based security and QoS policy. |

| | |
|---|---|
| 9.4 | The router shall support unicast RPF (uRPF) feature to block any communications and attacks that are being sourced from Randomly generated IP addresses. |
| 9.5 | The router shall provide Firewall Services that are required for routing purposes for enhanced security to protect the WAN backbone from malicious activities. (Internal or external) |
| 9.6 | The router shall support firewall service in hardware on all interfaces. The firewall performance shall be at least 4 Gbps. |
| 9.7 | The router should have support for Network Address Translation (NAT) and Port Address Translation (PAT) to hide internal IP addresses while connecting to external networks. |
| 9.8 | The router shall support AAA features through RADIUS or TACACS+. |
| 9.9 | The router shall support Control Plane Policing to protect the router CPU from attacks. |
| 9.10 | The router shall provide MD5 hash authentication mechanism for RIPv2, OSPF, IS-IS, BGP and MPLS routing protocols. |
| 9.11 | The Router shall support IKEv1 and IKEv2 (RFC 5996) |
| 9.12 | The Router shall support Suite B Cryptographic Suites for Ipsec (RFC 4869) |
| **10** | **System Management and Administration** |
| 10.1 | Routers should support Configuration rollback |
| 10.2 | Support for accounting of traffic flows for Network planning and Security purposes |
| 10.3 | Should support extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss, RTP-Based VoIP traffic, CRTP |
| 10.4 | Routers should support Software upgrades |
| 10.5 | Routers should support SNMPv2 and SNMPv3 |
| 10.6 | Device should have Console, Telnet, SSH1 and SSH2 support for management |
| **11** | **Built-in trouble shooting** |
| 11.1 | Extensive debugs on all protocols |
| 11.2 | Shall support Secure Shell for secure connectivity |
| 11.3 | Should have to support Out of band management through Console and an external modem for remote management |
| 11.4 | Pre-planned scheduled Reboot Facility |
| 11.5 | Real Time Performance Monitor – service-level agreement verification probes/alert |
| **12** | **Certifications** |
| 12.1 | The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum. |
| 12.2 | The proposed router should be Common Criteria Certified such as EAL3 / NDPP or above. |
| 12.3 | Safety certifications UL 60950-1 |
| 12.4 | EMC certifications FCC Class A. IEC/EN61000-4-2 to 4-6, 4-8, 4-11 and EN55022 & EN55024 |

## SOR-A-2: Switch:

| SN | Technical Specification |
|---|---|
| 1 | **Solution Requirement** |
| 1.1 | The Switch should support non-blocking Layer 2 switching and Layer 3 routing |
| 1.2 | There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy |
| 1.3 | Switch should support the complete STACK of IPv4 and IPv6 services. |
| 1.4 | The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied |
| 1.5 | The switch quoted should be part of latest Gartner's Leader Quadrant for Data Center networking |
| 2 | **Hardware and Interface Requirement** |
| 2.1 | Switch should have the following interfaces: |
| 2.2 | a. 48 x 1G/10G/25G Multi Mode Fiber Interface populated with 48*10G multi-mode interfaces |
| 2.3 | b. 6 x 40G /100G ports fully populated using multimode 40G Trancievers, for uplink connectivity |
| 2.4 | Switch should have console port |
| 2.5 | Switch should have management interface for Out of Band Management |
| 2.6 | Switch should be rack mountable and support side rails if required |
| 2.7 | Switch should have adequate power supply for the complete system usage with all slots populated and used and provide N+1 redundant |
| 2.8 | Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP |
| 2.9 | Switch should have a minimum 40MB buffer of more. |
| 2.1 | Switch should have smart buffering mechanism to classify long lived versus short lived flows and must have capability to dynamically prioritize short lived flows during congestion to avoid packet drop of mission critical traffic. In case of such classification not being supported then the OEM must supply a deep buffer (4GB or higher) switch. |
| 2.1 | Switch should support VLAN tagging (IEEE 802.1q) |
| 2.1 | Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy |
| 2.1 | Switch should support Configuration roll-back and check point |
| 2.1 | Switch should support for different logical interface types like loopback, VLAN, SVI/RVI, Port Channel, multi chassis port channel/LAG etc |
| 3 | **Performance Requirement** |
| 3.1 | Switch should support Graceful Restart for OSPF, BGP etc. |
| 3.2 | Switch should support minimum 512 VRF instances |
| 3.3 | The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure |
| 3.4 | The switch should support hardware based load balancing at wire speed using LACP and multi chassis etherchannel/LAG |
| 3.5 | Switch should support minimum 3.6 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) including the services: |
| | a. Switching |

| | |
|---|---|
| | b. IP Routing (Static/Dynamic) |
| | c. IP Forwarding |
| | d. Policy Based Routing |
| | e. QoS |
| | f. ACL and Other IP Services |
| | g. IPv6 host and IPv6 routing |
| **4** | **Advance Features** |
| **4.1** | Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN /NVGRE |
| **4.2** | Switch should support VXLAN and EVPN or equivalent for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data center |
| **4.3** | Switch should support OpenFlow/Open Day light/Open Stack controller |
| **4.4** | Switch should support VXLAN routing (single pass without any re-circulation) |
| **4.5** | Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically. |
| **5** | **Layer2 Features** |
| **5.1** | Spanning Tree Protocol (IEEE 801.D, 802.1W, 802.1S) |
| **5.2** | Switch should support VLAN Trunking (802.1q) and should support 3900 VLAN |
| **5.3** | Switch should support basic Multicast IGMP v1, v2, v3 |
| **5.4** | Switch should support minimum 64K no. of MAC addresses |
| **5.5** | Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch |
| **5.6** | Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port. |
| **5.7** | Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server |
| **5.8** | Switch should support Jumbo Frames up to 9K Bytes on all available Ports |
| **5.9** | Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities |
| **5.1** | Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures |
| **5.1** | Switch platform should support MAC Sec in hardware |
| **6** | **Layer3 Features** |
| **6.1** | Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface |
| **6.2** | Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing |
| **6.3** | Switch should support MPLS segment routing and VRF route leaking functionality from day 1 |
| **6.4** | Switch should provide multicast traffic reachable using: |
| | a. PIM-SM |
| | b. PIM-SSM |
| | c. Bi-Directional PIM |
| | d. Support Multicast Source Discovery Protocol (MSDP) |
| | e. IGMP v1, v2 and v3 |

| | |
|---|---|
| **7**<br>**7.1** | **Availability**<br>Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy |
| **7.2** | Switch should provide gateway level of redundancy in IPv4 and IPv6 using HSRP/VRRP |
| **7.3** | Switch should support for BFD For Fast Failure Detection as per RFC 5880 |
| **7.4** | **Quality of Service** |
| **7.5** | Switch system should support 802.1P classification and marking of packet using: |
| | a. CoS (Class of Service) |
| | b. DSCP (Differentiated Services Code Point) |
| | c. Source physical interfaces |
| | d. Source/destination IP subnet |
| | e. Protocol types (IP/TCP/UDP) |
| | f. Source/destination TCP/UDP ports |
| **7.6** | Switch should support methods for identifying different types of traffic for better management and resilience |
| **7.8** | Switch should support for different type of QoS features for ream time traffic differential treatment using |
| | a. Weighted Random Early Detection |
| | b. Strict Priority Queuing |
| **7.9** | Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy |
| **7.1** | Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic |
| **8** | **Security** |
| **8.1** | Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail |
| **8.2** | Switch should support control plane i.e. processor and memory protection from unnecessary or DoS traffic by control plane protection policy |
| **8.3** | Switch should support for stringent security policies based on time of day of Layer-2 to Layer-4 |
| **8.4** | Switch should support for external database for AAA using: |
| | a. TACACS+ |
| | b. RADIUS |
| **8.5** | Switch should support DHCP Snooping |
| **8.6** | Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol |
| **8.7** | Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes |
| **8.8** | Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port |
| **8.9** | Switch should support Spanning tree BPDU protection |
| **9** | **Manageability** |

| | |
|---|---|
| **9.1** | Switch should support for embedded RMON/RMON-II for central NMS management and monitoring |
| **9.2** | Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail |
| **9.3** | Switch should provide remote login for administration using: |
| | a. Telnet |
| | b. SSH v2 |
| **9.4** | Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures |
| **9.6** | Switch should support for management and monitoring status using different type of Industry standard NMS using: |
| | a. SNMP v1 and v2 |
| | b. SNMP v3 with encryption |
| | c. Filtration of SNMP using Access list |
| | d. SNMP MIB support for QoS |
| **9.7** | Switch should support for basic administrative tools like: |
| | a. Ping |
| | b. Traceroute |
| **9.8** | Switch should support central time server synchronization using Network Time Protocol NTP v4 |
| **9.9** | Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces |
| **9.10** | Switch should support for predefined and customized execution of script for device mange for automatic and scheduled system status update for monitoring and management |
| **9.1** | Switch should provide different privilege for login in to the system for monitoring and management |
| **9.1** | Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding |
| **10** | **IPv6 features** |
| **10** | Switch should support for IPv6 connectivity and routing required for network reachability using different routing protocols such |
| | a. OSPF v3 |
| | b. BGP with IPv6 |
| | c. IPv6 Policy based routing |
| | d. IPv6 Dual Stack etc |
| | e. IPv6 Static Route |
| | f. IPv6 Default route |
| | g. Should support route redistribution between these protocols |
| **10** | Switch should support multicast routing in IPv6 network using PIMv2 Sparse Mode |
| **10** | Switch should support for QoS in IPv6 network connectivity |
| **10** | Switch should support for monitoring and management using different versions of SNMP in IPv6 environment such as: |
| | a. SNMPv1, SNMPv2c, SNMPv3 |
| | b. SNMP over IPv6 with encryption support for SNMP Version 3 |

| | |
|---|---|
| **11** | Switch should support syslog for sending system log messages to centralized log server in IPv6 environment |
| **11** | Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events |
| **11** | Switch should support for IP V.6 different types of tools for administration and management such as: |
| | a. Ping |
| | b. Traceroute |
| | c. VTY |
| | d. SSH |
| | e. TFTP |
| | f. DNS lookup |
| **11** | All relevant licenses for all the above features and scale should be quoted along with switch |
| **11** | Switch and optics should be from the same OEM |

## SOR-A-3: UTM:

## The Component Required for UTM Solution

| SN | Component | Qty |
|---|---|---|
| 1 | Next Generation Firewall | 4 |
| 2 | Network Behavior Analysis | 2 |
| 3 | Network Access Control & Authentication | 2 |
| 4 | Anti-Malware Protection for Endpoint | 2 |

## Technical Specification:

| SN | Feature | Technical Specification |
|---|---|---|
| 1 | Industry recommendations | The Firewall solution offered must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant for Enterprise Firewall published by Gartner from last 3 years |
| 2 | Hardware Architecture | Chassis based security appliance should provide firewall, AVC and IPS functionality from day one |
| | | Chassis platform should support at least 6 * 10G Gigabit ports and should be scalable to additional 8 * 40G in future. Solution should support 100G (QSFP28) Interfaces. |
| | | The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 256 GB of RAM |
| | | Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats. |
| | | The proposed solution shouldn't use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet. |
| | | Proposed firewall should not consume more than 3 RU of rack space |

| | | |
|---|---|---|
| 3 | Performance & Scalability | Should support 40 Gbps of NGFW (FW, AVC and IPS) real-world / production performance and should be scalable to 80 Gbps in future without replacing hardware. |
| | | Firewall should support atleast 25,000,000 concurrent sessions with application visibility turned on or more |
| | | Firewall should support atleast 300,000 connections per second with application visibility turned on or more |
| | | Firewall should have integrated redundant hot-swappable power supply |
| | | Firewall should have integrated redundant hot-swappable fan tray / modules |
| 4 | NG Firewall Features | Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc. Firewall should support Next-Gen IPS (NGIPS) from day one. The same Firewall should support Advanced Malware Protection (AMP) for Networks, and URL Filtering. |
| | | Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat |
| | | Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality |
| | | Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6 |
| | | Should support Multicast protocols like IGMP, PIM, etc |
| | | Should support capability to integrate with other security solutions (AAA) to receive contextual information like security group tags/names |
| | | Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance. |
| | | Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance. |
| | | Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware. |
| | | Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency |
| | | Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention. |

| | | |
|---|---|---|
| | | Should support more than 25,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy |
| | | Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports. |
| | | Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events. |
| | | Should be capable of detecting and blocking IPv6 attacks. |
| | | The solution should be able to identify, decrypt and evaluate both inbound and outbound SSL traffic on-box |
| | | Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control |
| | | Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines. |
| | | The solution must provide IP reputation feed that comprised of several regularly updated collections of poor repuration of IP addresses determined by the proposed security vendor |
| | | Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist |
| | | Should must support DNS threat intelligence feeds to protect against threats |
| | | The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection. |
| | | The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.). |
| | | Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location |
| | | The detection engine should support the capability of detecting variants of known threats, as well as new threats |
| | | The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. |
| | | Should support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly |
| 5 | URL Filtering Features | Should support URL threat intelligence feeds to protect against threats |
| | | Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web |

| | | |
|---|---|---|
| | | traffic and enforces policies on more than 280 million of URLs in more than 80 categories. |
| | | Should support safe search for YouTube EDU enforcement |
| 6 | DNS Security | The proposed solution must d mandatorily support recursive DNS analysis and must have a minimal impact with the existing DNS infrastructure |
| | | The solution must offer several deployment options: either via an internal forwarder, or pointing the forwarder of the existing authoritative DNS to the recursive service, or pointing the DNS configured on the Internal Proxy to the recursive service, without any additional physical hardware. |
| | | The solution must be able to detect and block malware using protocols different from HTTP/HTTPS. |
| | | The solution must be able to protect at least from the following categories of malware: botnets, exploit kits, drive-by, phishing. |
| | | The solution must be able to prevent infections, blocking the DNS requests towards malware distribution domains or drive-by domains, and contain the pre-existing infections, blocking the DNS requests towards command and control infrastructures. |
| | | In order to allow the malware detection on a global scale, the network utilized to build the threat intelligence must process at least 80 billion DNS requests/day coming from at least 60 million daily users. |
| | | The analysis algorithms must make use multi-layer predictive detectors. As a mere example, these include (but are not limited to):<br>§ Analysis of DNS co-occurrences,<br>§ Analysis of Domains based on Natural Language Processing algorithms.<br>§ Detection of DGA via perplexity and entropy.<br>§ Detection of DNS traffic peaks<br>§ Soundwave analysis applied to DNS traffic<br>§ BGP anomalies detection. |
| | | The solution should support ability to enforce Web filtering policies, based on 62 categories. It must be possible to enforce the Web filtering policy independently form the security policy. |
| | | The solution must have ability to Protect against phishing threats automatically leveraging global network data and predictive intelligence to discover internet infrastructure used to host phishing sites. |
| | | The network used to deliver the DNS security service must have experienced an uptime of at least 99.9% over the last 10 years. |
| | | The solution must have ability to block over 200 apps and automatically enable app settings and policy configuration. |
| 7 | Management | The management platform must be accessible via a web-based interface and ideally with no need for additional client software |

| | | |
|---|---|---|
| | | The management platform must be a dedicated OEM appliance and VM running on server will not be accepted |
| | | The management appliance should have 2 x 10G port and integrated redundant power supply from day one |
| | | The management platform must be able to store record of 15000 user or more |
| | | The management platform must provide a highly customizable dashboard. |
| | | The management platform must domain multi-domain management |
| | | The management platform must provide centralized logging and reporting functionality |
| | | The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows |
| | | The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication. |
| | | Should support troubleshooting techniques like Packet tracer and capture |
| | | Should support REST API for monitoring and config programmability |
| | | The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV. |
| | | The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG). |
| | | The centralized management platform must not have any limit in terms of handling logs per day<br>Solution should be able to provide insights of hosts/user on basis of indication of compromise, any license required for this to be included from day one |
| | | The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports. |
| | | The management platform support running on-demand and scheduled reports |
| | | The management platform must risk reports like advanced malware, attacks and network |
| | | The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools. |
| 8 | Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement | |
| **B** | **Technical Requirement: Network Behavior Analysis Specification:** | |
| **SN** | **Minimum Requirement Specification** | |

| | |
|---|---|
| 1 | Solution should provide a full-featured Network threat analyzer capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter FW/IPS). This includes the ability to establish “normal” traffic baselines through flow analysis techniques and the ability to detect deviations from normal baselines. |
| 2 | Should have an automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts. |
| 3 | Should capture signature / heuristics based alerts and block the same |
| 4 | Should Identify the source of an attack and should not block legitimate users |
| 5 | Should identify worms through techniques such as identifying the use of normally inactive ports or identification of network scanning activities |
| 6 | The solution should be capable of detecting denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks including floods of all types (ICMP, UDP, TCP SYN, TCP NULL, IP NULL etc.), identify the presence of botnets in the network, identify DNS spoofing attack etc. |
| 7 | Solution should detect common events like Scanning, Worms, Unexpected application services (e.g., tunneled protocols, backdoors, use of forbidden application Protocols), Policy violations, etc. |
| 8 | Solution should provide application insights and inventory across data center using auto generated application discovery and dependency mapping for workloads in various environments like dev, test, Pre-Prod, Prod and other zones in datacenter. It should provide an always-on application blueprint for ever changing application relationships and inter-dependencies. |
| 9 | Solution should generate a whitelist policy based on real-time application behavior and keep the policies up-to-date as applications evolves and more applications are added and modified. It should enforce the generated application whitelisted policy consistently across bare-metal, virtual and container workloads. It should track policy compliance. |
| 10 | Should utilize Anamoly detection methods to identify attacks such as zero-day exploits, self-modifying malware, attacks in the ciphered traffic or resource misuse or misconfiguration. |
| 11 | Solution should Integrates with Microsoft Active Directory, RADIUS, and DHCP to provide user Identity information in addition to IP address information throughout the system & allow groups based on Identity or Active Directory workgroup & Provides full historical mapping of User Name to IP address logins in a searchable format |
| 12 | Should support the capability to instruct network security devices such as firewalls to block certain types of traffic or route it to quarantine VLANS |
| 13 | Should support the capability to alert the admin and provide mitigation action like quarantine or block the endpoint or custom scripts like ACL push or block the further spread of the malware/worm while allowing legitimate traffic to continue |
| 14 | The system should be able to monitor flow data between various VLANS |
| 15 | Should support the capability to identify network traffic from high risk applications such as file sharing, peer-to-peer, etc. |

| | |
|---|---|
| 16 | Should support the capability to link usernames to IP addresses for suspected security events. |
| 17 | Should support the capability to extract user defined fields (including source and destination IPs, source and destination MAC address, TCP/UDP ports or ICMP types and codes, no. of packets and no. of bytes transmitted in a session, timestamps for start and end of session etc.) from captured packet data and then utilize fields in correlation rules. |
| 18 | Should support the capability Application profiling in the system and should also support custom applications present or acquired by the bank/customer |
| 19 | Solution should be compatible with a virtual environment. |
| 20 | Solution should support capability to quarantine / remediate endpoint |
| 21 | Solution should be able to identify potential DDOS attacks originating from behind proxies. |
| 22 | Solution should be able to identify anomalies related to VOIP protocols over data network |
| 23 | Solution should have the capability to track every process executed on the server and map behaviour deviations instantaneously to malware execution patterns. It should provide high fidelity alters for both system generated and user defined events. |
| 24 | Solution should provide accurate inventory of the installed software packages on the workloads in real time to quickly identify any known vulnerabilities and exposures. It should then provide actions to quarantine or restrict communications based on vulnerabilities or vulnerability score. |
| 25 | It should provide a always-on traffic search and analysis capability for tracking and monitoring application and network performance on a per flow basis between all DC and external endpoints for real time and historic traffic flow. |
| 26 | Solution should be dedicated network behaviour analysis solution and not a subset of SIEM or Forensic analysis |
| 27 | Solution should support built-in firewalling support, rejecting all packets by default (transparent to pings and port scans) |
| 28 | Dashboard should have the facility to be configured according to user profile |
| 29 | System should support event forwarding for SMTP, SYSLOG & SNMP for high risk issues |
| 30 | The solution must allow analysis by grouping of network segments such as User VLAN, Management VLAN, Server Farms etc. |
| 31 | Solution should be able to track user's activities locally and remote network sites and should be able to report usage behavior across the entire network. |
| 32 | The solution should support the identification of applications tunneling on other ports |
| 33 | Solution should be able to collect security and network information of servers and clients without the usage of agents |
| 34 | Solution include capability to monitor and display of each and every process, process ID, Process owner, Process mapping running on the server (Physical / VM form factor). |

| | |
|---|---|
| 35 | Solution should be capable of simulating "what if" scenario with existing policy in data center workload on past traffic or new policy on current / old traffic and validate the result before applying the policy on the production network. |
| 36 | Solution should provide contextual search capability with actionable insight for faster troubleshooting and anamoly detection |
| 37 | The solution should be able to conduct de-duplication of redundant flow identified in the network to improve performance |
| 38 | The solution should have the ability to statefully reassemble uni-directional flows into bi-directional conversations; handling de-duplication of data and asymmetry |
| 39 | The solution should support all forms of flows including but not limited to cisco netflow, juniper jflow, sflow, ipfix for udp etc. |
| 40 | The solution should be able to combine/stitch the flow records coming from different network devices like routers/switches/firewall that are associated with a single conversation and present them as a single bi-derectional flow record |
| 41 | The solution should be able to stitch flows into conversations even when the traffic is NATted by the firewall; clearly showing the original and translated IP address |
| 42 | The solution should be able to leverage external threat feeds for information about known detection methods/fingerprints for Phishing, Botnets, Malware, Spyware, Connections to bad reputation Nations and Dark IP |
| 43 | Solution should support detection methods/fingerprints for Web crawler identification, location based threats & GEO IP based threats |
| 44 | The solution should be able to integrate with various SIEMs available in the market like RSA, Splunk, HP, etc |
| 45 | Solution should collect telemetry information from every packet in the data center without sampling along witht support of long term data retention. |
| 46 | Solution should analys each and every flow in different dimension i.e. location, time of transaction, network and application latency, source and destination ports and IP, Session duration etc to find out application anomaly in data center |
| 47 | **Network performance** |
| 48 | Solution should provide application bandwidth utilization graph for various applications which should include bandwidth consumption for top hosts and trends on network bandwidth utilization. |
| 49 | Dashboard should have the facility to be configured according to user profile |
| 50 | Solution should probe the network in a manner so that impact on network performance is minimal. |
| 51 | Should support both in line and/or offline modes. |
| 52 | The tool should have a system for interactive event identification and rule creation |
| 53 | Devices / applications those do not support flows, the solution should be capable to generate its own flows for monitoring. |
| 54 | Solution should have facility to assign risk and credibility rating to events. |
| 55 | Solution should include 100 license for Data Center workload for montioring and policy enforcement |
| 56 | Solution should support traffic rate up to 10 Gbps |

| | |
|---|---|
| 57 | Proposed flow collectors should have the ability to scale from 20000 flows per second to 80000 flows per second |
| 58 | Proposed solution should be a dedicated appliance based solution |
| C | **Technical Requirement: Network Access Control & Authentication Specification:** |
| SN | **Minimum Requirement Specification** |
| 1 | The Solution should provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA); profiling; posture/health check; and guest management services on a single platform. |
| 2 | Solution should have concurrent capacity for 2000 endpoints out of 50000 endpoint users from day one with scaling upto 50000 concurrent end point endpoints. |
| 3 | It should allow organisation to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise |
| 4 | Solution should enables administrators to centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console, greatly simplifying administration by providing consistency in managing all these services. |
| 5 | Provides complete guest lifecycle management by empowering sponsors to on-board guests |
| 6 | Should helps organisations to identify the number of endpoints that have a specified application installed and these applications should be classified into 13 categories |
| 7 | Solution should be dedicated appliance based |
| 8 | Proposed solution should include two appliances to be configured in Active/Standby |
| 9 | Should support consistent policy in centralized and distributed deployments that allows services to be delivered where ever required |
| 10 | Solution should delivers customizable self service portals as well as the ability to host custom web pages to ease device and guest on-boarding, automate endpoint secure access and service provisioning, and enhance the overall end-user experience inside business-defined workflows |
| 11 | Should enforces security policies by blocking, isolating, and repairing non-compliant machines in a quarantine area without requiring administrator attention |
| 12 | Should support Identity source sequences which defines the order in which the solution will look for user credentials in the different databases. Solution should support the following databases:<br>•Internal Users, Internal Endpoints, Active Directory, LDAP, RSA, RADIUS Token Servers, Certificate Authentication Profiles |
| 13 | Support password settings for internal users and admin users, option should be available to choose if the password can contain any dictionary word or its characters in reverse order |
| 14 | Support allows Organisation to configure the AD and LDAP server with IPv4 or IPv6 address |
| 15 | Should utilizes standard RADIUS protocol for authentication, authorization, and accounting (AAA). |

| | |
|---|---|
| 16 | Supports a wide range of 802.1x authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST), and EAP-Transport Layer Security (TLS). |
| 17 | Solution should support TACACS+ to simplify device administration and enhance security through flexible, granular control of access to network devices |
| 18 | TACACS+ device administration should support:<br>i. Role-based access control<br>ii. Flow-based user experience<br>iii. Per Command level authorization with detailed logs for auditing |
| 19 | Solution should support capability to customize TACACS+ Services by specifying customer TACACS+ port number |
| 20 | Solution should support capability to create different network device groups so that administrator can create:<br>i. Different policy sets for IOS/OS or wireless controller OS<br>ii. Different for firewall<br>iii. Differentiate base on location of device |
| 21 | Solution should be able to create TACACS+ profile like Monitor, Priviledge level, default, etc to control the initial login session of device administrator. |
| 22 | solution should be able to create TACACS+ authorization policy for device administrator containing specific lists of commands a device admin can execute. Command sets should support; exact match, case sensitive, ? (any character), * (matches any), etc and support stacking as well |
| 23 | solution must support TACACS+ in IPv6 network |
| 24 | Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect |
| 25 | Solution should be able to integrate with MDM vendors like: Airwatch, Good, Mobileiron, Zenprise,etc |
| 26 | Should support full guest lifecycle management, whereby guest users can access the network for a limited time, either through administrator sponsorship or by self-signing via a guest portal. Should include guest portal customize from day one |
| 27 | Solution should have capability to establish user identity, location, and access history, which can be used for compliance and reporting. |
| 28 | Solution should have capability to collect endpoint attribute data via passive network telemetry, querying the actual endpoints, or alternatively from the infrastructure via device sensors on switches. |
| 29 | Solution should have profiling capabilities integrated into the solution in order to detect headless host. The profiling features leverage the existing infrastructure for device discovery. Should support the use of attributes from the following sources or sensors:<br>* Profiling using MAC OUIs<br>* Profiling using DHCP information<br>* Profiling using RADIUS information<br>* Profiling using HTTP information<br>* Profiling using DNS information / Nessus<br>* Profiling using NetFlow information / Onguard Agent<br>* Profiling using SPAN/Mirrored traffic |
| 30 | Should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, smartphones, and tablets. |

| | |
|---|---|
| 31 | Solution should support receiving updated endpoint profiling policies and the updated OUI database as a feed from the OEM database. |
| 32 | Solution should support the following endpoint checks for compliance for windows endpoints:<br>Check process, registry, file & application<br>Check operating system/service packs/hotfixes<br>Check firewall product is running<br>check for Antivirus installation/Version/ Antivirus Definition Date<br>check for Antispyware installation/Version/ Antispyware Definition Date<br>Check for windows update running & configuration |
| 33 | Should be a persistent client-based agent or clientless to validate that an endpoint is conforming to a company's posture policies. |
| 34 | Allows administrators to quickly take corrective action (Quarantine, Un-Quarantine, or Shutdown) on risk-compromised endpoints within the network. |
| 35 | Should support integration with 3rd party vulnerability assessment tools like Rapid7, Tenable/Nessus, etc |
| 36 | Should allows to create read-only administrative users who can view the configurations on GUI, but cannot create, update, or delete data |
| 37 | Should allow viewing the summary of the reports that are exported by the users in the last 48 hours along with the status. |
| 38 | Should support troubleshooting & Monitoring Tools |
| 39 | Includes a built-in web console for monitoring, reporting, and troubleshooting to assist help-desk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network. |
| **D** | **Technical Requirement: Anti-Malware Protection for Endpoint Specification:** |
| 1 | **Minimum Requirement Specification** |
| 2 | The bidder shall propose dedicated endpoint based solution to protect systems Advanced Targeted Attacks and APT's |
| 3 | The proposed solution shall work on a signature-less mechanism to stop threats without relying on a database to be present at the endpoint |
| 4 | The proposed solution shall work as an independent module without relying on other endpoint and network systems for any of its functionality |
| 5 | The proposed solution shall be capable of working along with all leading endpoint AV vendors without needing to replace them |
| 6 | The proposed solution shall utilize layered and defense in depth approach, wherein the solution cannot be of the same make as existing endpoint AV |
| 7 | The proposed endpoint solution should support detecting of all malware types, both known and unknown. The movement of all known and unknown malware should be tracked and reported across the endpoints. |
| 8 | The proposed endpoint solution should be able to support continuous and root cause analysis to help in triaging of security incidents. |
| 9 | Security vendor should have a dedicated research organisation that is focus on vulnerability research and should actively contribute to discoveries of new vulnerabilities exploited in the wild. |

| | |
|---|---|
| 10 | Software footprint should be small <50MB and should support interactive and/or silent install. Total of 50000 Licenses should be factored for this End Points. Solution should have concurrent capacity for 2000 endpoints out of 50000 endpoint users from day one with scaling upto 50000 concurrent end point endpoints. |
| 11 | Endpoint software should be easy to deploy and support (not limited to) deployment through 3rd party systems management tools |
| 12 | Root cause analysis on a suspected machines should include the following capability: |
| 13 | - Sequential and chronological trace of events with details including host, username, IP, client application involved |
| 14 | - Details should highlight which file/process/services that affected |
| 15 | Proposed endpoint software should support malware tracking and provide visualization at the network level: systems and users affected, patient zero, and method/point of entry. |
| 16 | Proposed system should support continuous and persistent monitoring of files to detect polymorphic and time bound malware whenever they start turning bad and shall not be only an on-demand scan mechanism |
| 17 | Proposed endpoint software should be capable to block CnC communications and dropper activity and contain the spread of malware |
| 18 | Remediation at endpoints for incident response should include (and not limited to): |
| 19 | - Track and capture files on suspected machine with option for lookups on suspected devices |
| 20 | - Block of files / process / services that are showing malicious behaviors |
| 21 | - Dropper detection and blocking of downloads via URL / sites |
| 22 | - Submit suspected malicious files for further analysis |
| 23 | The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quanratining the entire user machine from network which would affect business productivity of the user |
| 24 | The proposed solution shall have the capability to work with Indicators of Compromise (IOC's) |
| 25 | The proposed solution shall provide the capability to write/upload custom IOC's |
| 26 | The proposed solution shall provide details to enable forensic analysis of incidents |
| 27 | The solution shall be capable of working in Windows, Windows Server &Linux operating systems |
| 28 | The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints |
| 29 | The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition |
| 30 | The proposed solution should not be dependent on a network sandbox for its detection as it takes up bandwidth and affects productivity and shall provide the option of choosing which files to be submitted for sandboxing, to administrator |
| 31 | The proposed solution should be able to do a threat hunting across all endpoints and quarantine the specific malicious file |

| | |
|---|---|
| 32 | The proposed endpoint solution should run as is and not require any system changes at OS level like enabling Volume Shadow copy Service, disabling admin access or any other user level change |
| 33 | Solution should allow Users to chose to preview the new Policy UI. |
| 34 | - Track and capture files on suspected machine with option for lookups on suspected devices |
| 35 | - Block of files / process / services that are showing malicious behaviors |
| 36 | - Dropper detection and blocking of downloads via URL / sites |
| 37 | - Submit suspected malicious files for further analysis |
| 38 | The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quanratining the entire user machine from network which would affect business productivity of the user |
| 39 | The proposed solution shall have the capability to work with Indicators of Compromise (IOC's) |
| 40 | The proposed solution shall provide the capability to write/upload custom IOC's |
| 41 | The proposed solution shall provide details to enable forensic analysis of incidents |
| 42 | The solution shall be capable of working in Windows, Windows Server & Linux operating systems |
| 43 | The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints |
| 44 | The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition |
| 45 | The proposed solution should not be dependent on a network sandbox for its detection as it takes up bandwidth and affects productivity and shall provide the option of choosing which files to be submitted for sandboxing, to administrator |
| 46 | The proposed solution should be able to do a threat hunting across all endpoints and quarantine the specific malicious file |
| 47 | The proposed endpoint solution should run as is and not require any system changes at OS level like enabling Volume Shadow copy Service, disabling admin access or any other user level change |
| 48 | Solution should allow Users to chose to preview the new Policy UI. |

## SOR-B-1: Core Switch:

| SN | Feature Set |
|---|---|
| **1** | **Fabric Definition** |
| 1.1 | Proposed fabric must be the Close architecture defined using Spine, Leaf and VXLAN + ISIS or VXLAN + EVPN Protocol |
| 1.2 | Fabric should have achieved following functionalities: |
| 1.3 | **Flexibility :** Should allow workload mobility anywhere in the DC, across the DC |
| 1.4 | **Robustness :** while dynamic mobility is allowed on any authorized location of the DC, the failure domain is contained to its smallest zone |
| 1.5 | **Performance:** full cross sectional bandwidth (any-to-any) – all possible equal paths between two endpoints are active |

| | |
|---|---|
| 1.6 | **Deterministic Latency :** fix and predictable latency between two endpoints with same hop count between any two endpoints, independently of scale |
| 1.7 | **Multi-site design:-** The fabric should support a Multi-Site/Multi-Fabric design to interconnect separate availability zones (fabrics), each deployed either as a single pod or multiple pods (a Multi-Pod design) |
| 1.8 | **Business Continuance-** The fabric should be able to deploy applications across data center fabrics representing separate availability zones, to ensure that any network-level failures or configuration or policy definition errors that occur in one availability zone will not ever be propagated to the application’s workloads running in a separate availability zone |
| 1.9 | **Scalability:** add as much Leaf as needed to achieve desired scale in terms of number of servers while maintaining the same oversubscription ratio everywhere inside the fabric. |
| **2** | **Hardware and Interface Requirement** |
| 2.1 | Fabric Connectivity should have the following properties: |
| 2.2 | Leaf switches to Spine connectivity should use uplink port using line rate 40G/100G . |
| 2.3 | In case of Fixed Spine Switches must be scalable to 32 numbers 40/100 G ports in the same chassis and should be populated Equipped with 32* 40G Multimode QFP28 Multimode from day 1 to support desired Leaf Scale.<br>Each Leaf should connect to Each Spine using minimum 6 x 40G/100 G ports connectivity |
| 2.4 | All switches including Spine and leafs should be of line rate including access and uplink ports non-blocking |
| **3** | **Fabric Features** |
| 3.1 | Fabric must support various Hypervisor encapsulation including VXLAN and 802.1q natively without any additional hardware/software or design change. |
| 3.2 | Fabric must be created based on hardware based VXLAN + ISIS or VXLAN + EVPN architecture. |
| 3.3 | Fabric must auto discover all the hardware and auto provision the fabric based on the policy. |
| 3.4 | The fabric architecture must be based on hardware VXLAN overlays to provide logical topologies that are abstracted from the physical infrastructure with no performance degradation. Fabric must support VXLAN Switching/Bridging and VXLAN Routing. |
| 3.5 | Fabric must provide open programmable interface using python SDK, JSon SDK, XMLS or COBRA etc. from the Central Management appliance / SDN Controller for programming/configuring the entire fabric. |
| 3.6 | Fabric must provide open scripting interface using Bash / powershell / NetConf/YANG from the central management appliance / SDN Controller for configuring the entire fabric. |
| 3.7 | Fabric must support Role Based Access Control in order to support Multi - Tenant environment. |
| 3.8 | Fabric must integrate with different virtual machine manager viz. VmwarevCenter, Microsoft Hyper-V with System Center and manage virtualize networking from the single pane of Glass - Fabric Controller/SDN Controller |

| | |
|---|---|
| 3.9 | Fabric must support provide default gateway redundancy |
| 3.10 | Fabric must integrate with best of breed L4 - L7 Physical and virtual appliances and manage using single pane of glass - Fabric Controller / SDN Controller |
| 3.11 | Fabric must provide deeper visibility into the fabric in terms of latency and packet drop between any two endpoints on the fabric |
| 3.12 | Fabric must act as single distributed layer 2 switch, Layer 3 router and Stateless distributed firewall etc |
| 3.13 | Fabric must provide REST APIs from the Central management appliance/SDN Controller in order to integrate with best of breed Management, Monitoring, Hypervisor and Cloud automation & Orchestration software. |
| **4** | **Fabric Layer 2, Layer 3 and Misc. Features** |
| 4.1 | Fabric must support Layer 2 features like LACP, STP /RSTP /MSTP, VLAN Trunking, LLDP etc |
| 4.2 | Fabric must support multi chassis ether channel/MLAG i.e. Host connects to two different Leaf switches and form ether channel using LACP/NIC Teaming on Host |
| 4.3 | Fabric must support Jumbo Frame up to 9K Bytes on 1G/10G/25G/40G/100G ports |
| 4.4 | Fabric must support Layer 2 Multicast i.e. IGMP v1, v2 and v3 |
| 4.5 | Fabric must support IP v4 and IP v6 FHRP using HSRP or VRRP |
| 4.6 | Fabric Must support IP v4 and IP v6 Layer 3 routing protocol OSPF and BGP |
| 4.7 | Fabric must support IP v6 dual stack |
| 4.8 | Fabric must support traffic redistribution between different routing protocol |
| 4.9 | Fabric must support IP v4 and IP v6 management tools like - Ping, Traceroute, VTY, SSH, TFTP and DNS Lookup |
| 4.10 | Fabric must support IP v4 and IP v6 SNMP V1 / V2 / V3 |
| 4.11 | Fabric must support RMON/RMON-II for monitoring |
| 4.12 | Fabric must support integration with the centralized Syslog server for monitoring and audit trail |
| 4.13 | Fabric must support NTP |
| **5** | **Fabric Security Features** |
| 5.1 | Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle - attack, Replay Attack, Data Disclosure, Denial of Service |
| 5.2 | Fabric must provide RBAC policies and support AAA using Local User authentication, External RADIUS, External TACACS+, External LDAP, External AD |
| 5.3 | Fabric must support VM attribute based zoning and policy |
| 5.4 | Fabric must support Micro Segmentation for the Virtualize and Non - Virtualize environment |
| 5.5 | Fabric must support true multi - tenancy |
| 5.6 | Fabric must be accessible using CLI over SSH and GUI using HTTP/HTTPS |

| | |
|---|---|
| 5.7 | Fabric must support SNMP v2/3 with HMAC-MD5 or HMAC-SHA authentication and DES encryption. |
| 5.8 | Fabric must act as a State-less distributed firewall with the logging capability |
| 5.9 | Fabric must be capable to provide services of L 4 - L7 services using physical or virtual appliances i.e. Firewall, ADC, IPS etc. |
| **6** | **Fabric Scale and Performance** |
| 6.1 | Fabric should support scale up and scale out without any service disruption |
| 6.2 | Fabric must support for 512 VRF/Private network/tenants without any additional component or upgrade or design change |
| 6.3 | Fabric must integrate with minimum 3 Virtual Machine Manager (i.e. vCenter, SCVMM, OpenStack etc.) of different Hypervisors simultaneously and scalable to 5 in future with or without common orchestrator |
| 6.4 | Fabric must be capable of connecting up to 200 physical servers. |
| 6.5 | Fabric must be capable of integrating minimum of 8 nos. of L4 - L7 services physical or virtual appliances (i.e. Firewall, ADC, IPS etc.) and scale up to 16 nos. of L4 - L7 Services appliances. |
| 6.6 | Spine Switches must be scalable to 32 numbers 40/100 G ports in the same chassis and should be populated from day 1 to support desired Leaf Scale. Each Leaf should connect to Each Spine using minimum 4 x 40G/100 G ports connectivity |
| **7** | **Fabric management** |
| 7.1 | Fabric must provide Centralized Management Appliance or SDN Controller - Single pane of glass for managing, monitoring and provisioning the entire Fabric. |
| 7.2 | Fabric must Auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy using Centralized Management appliance or SDN Controller. |
| 7.3 | Centralized management appliance or SDN Controller must manages and provision rules on L4 - L7 Services physical or virtual appliance as well as integrate with Virtual Machine manager. |
| 7.4 | Centralized management appliance or SDN Controller should not participate in Data plane and control plane path of the fabric. |
| 7.5 | Centralized management appliance or SDN Controller must provide necessary report for compliance and audit. |
| 7.6 | Centralized management appliance or SDN Controller must communicate to south bound devices using open standard protocol i.e. OPFLEX / OPENFLOW / OVSDB etc. or using Device APIs. |
| 7.7 | Centralized management appliance or SDN Controller communication with the south bound devices must be encrypted |
| 7.8 | Centralized management appliance or SDN Controller must communicate with the south bound devices using more than one path i.e. in-path connectivity and out of band management connectivity |
| 7.9 | Centralized management appliance or SDN Controller provide dynamic device inventory of the Fabric as well as current network topology of the fabric. It must also validate the cabling connectivity and generate alarms in case of wrong or faulty connectivity. |

| | |
|---|---|
| 7.10 | Centralized management appliance or SDN Controller must run in "N + 1" redundancy to provide availability as well as function during the split brain scenario |
| 7.11 | In Event of all Centralized management appliances or SDN Controllers fails, the fabric must function without any performance degradation and with the current configuration. |
| 7.12 | Centralized management appliance or SDN Controller must support multi tenancy from management perspective and also provide Role Based Access Control per tenant for the tenant management. |
| 7.13 | Centralized management appliance or SDN Controller must support TACACS+, RADIUS, LDAP or Local Authentication. It must also provide an integration with the Syslog servers. |
| 7.14 | The proposed solution must be able to analyze real time data about the network which includes any metadata, configurations, policies, device states or protocol states and then run automated checks to identify potential errors, misconfigurations and network misbehaviors. |
| 7.15 | The proposed solution must be able to verify configurations before been committed to be adherent to configuration best practices and if any check/verification failure occurs then system must notify it to the admin via a suitable mechanism |
| 7.16 | The proposed solution must be able to analyse configuration/polocies across all devices in the fabric and then verify information such as<br>Two endpoints will be able to communicate with each other with the defined configuration/policies.<br>a. Two different sets of endpoints will be able to communicate with each other with the defined configuration/policies.<br>b. Tenants defined are indeed isolated as per configuration/policy across the entire fabric |

| Spine (40/100G Fibre) Switch Specification | |
|---|---|
| SN | Item Description |
| 1 | Solution Requirement - Spine Switch |
| 1.1 | The Switch should support non-blocking Layer 2 switching and Layer 3 routing |
| 1.2 | There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy |
| 1.3 | Switch should support the complete STACK of IPv4 and IPv6 services. |
| 1.4 | The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied |
| 1.5 | The switch quoted should be part of latest Gartner's Leader Quadrant for Data Center networking |
| 2 | Hardware and Interface Requirement |
| 2.1 | Switch should have the following interfaces: |
| | a. Minimum 36 ports support 40/100 Gbps QSFP28 ports. The switch should be populated with 32* 40G Multimode fiber transreceivers for downlink connectivity & 4*100G ports with multimode 100G Transrecievers, for uplink connectivity |
| 2.2 | Switch should have console port |
| 2.3 | Switch should have management interface for Out of Band Management |
| 2.4 | Switch should be rack mountable and support side rails if required |

| | |
|---|---|
| **2.5** | Switch should have adequate power supply for the complete system usage with all slots populated and used and provide N+1 redundant |
| **2.6** | Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP |
| **2.7** | Switch should have a minimum 40MB buffer of more. |
| **2.8** | Switch should have smart buffering mechanism to classify long lived versus short lived flows and must have capability to dynamically priortise short lived flows during congestion to avoid packet drop of mission critical traffic. In case of such classification not being supported then the OEM must supply a deep buffer (4GB or higher) switch. |
| **2.9** | Switch should support VLAN tagging (IEEE 802.1q) |
| **2.10** | Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy |
| **2.11** | Switch should support Configuration roll-back and check point |
| **2.12** | Switch should support for different logical interface types like loopback, VLAN, SVI/RVI, Port Channel, multi chassis port channel/LAG etc |
| **3** | **Performance Requirement** |
| **3.1** | Switch should support Graceful Restart for OSPF, BGP etc. |
| **3.2** | Switch should support minimum 512 VRF instances |
| **3.3** | The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure |
| **3.4** | The switch should support hardware based loadbalancing at wire speed using LACP and multi chassis etherchannel/LAG |
| **3.5** | Switch should support minimum 7 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) including the services: |
| | a. Switching |
| | b. IP Routing (Static/Dynamic) |
| | c. IP Forwarding |
| | d. Policy Based Routing |
| | e. QoS |
| | f. ACL and Other IP Services |
| | g. IPv6 host and IPv6 routing |
| **4** | **Advance Features** |
| **4.1** | Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN /NVGRE |
| **4.2** | Switch should support VXLAN and EVPN or equivalent for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data center |
| **4.3** | Switch should support OpenFlow/Open Day light/Open Stack controller |
| **4.4** | Switch should support VXLAN routing (single pass without any re-circulation) |
| **4.6** | Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically. |
| **5** | **Layer2 Features** |
| **5.1** | Spanning Tree Protocol (IEEE 801.D, 802.1W, 802.1S) |
| **5.2** | Switch should support VLAN Trunking (802.1q) and should support 3900 VLAN |
| **5.3** | Switch should support basic Multicast IGMP v1, v2, v3 |
| **5.4** | Switch should support minimum 64K no. of MAC addresses |

| | |
|---|---|
| **5.5** | Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch |
| **5.6** | Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port. |
| **5.7** | Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server |
| **5.8** | Switch should support Jumbo Frames up to 9K Bytes on all available Ports |
| **5.9** | Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities |
| **5.10** | Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures |
| **5.11** | Switch platform should support MAC Sec in hardware |
| **6** | **Layer3 Features** |
| **6.1** | Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface |
| **6.2** | Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing |
| **6.3** | Switch should support MPLS segment routing and VRF route leaking functionality from day 1 |
| **6.4** | Switch should provide multicast traffic reachable using: |
| | a. PIM-SM |
| | b. PIM-SSM |
| | c. Bi-Directional PIM |
| | d. Support Multicast Source Discovery Protocol (MSDP) |
| | e. IGMP v1, v2 and v3 |
| **7** | **Availability** |
| **7.1** | Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy |
| **7.2** | Switch should provide gateway level of redundancy in IPv4 and IPv6 using HSRP/VRRP |
| **7.3** | Switch should support for BFD For Fast Failure Detection as per RFC 5880 |
| **8** | **Quality of Service** |
| **8.1** | Switch system should support 802.1P classification and marking of packet using: |
| | a. CoS (Class of Service) |
| | b. DSCP (Differentiated Services Code Point) |
| | c. Source physical interfaces |
| | d. Source/destination IP subnet |
| | e. Protocol types (IP/TCP/UDP) |
| | f. Source/destination TCP/UDP ports |
| **8.2** | Switch should support methods for identifying different types of traffic for better management and resilience |
| **8.3** | Switch should support for different type of QoS features for ream time traffic differential treatment using |
| | a. Weighted Random Early Detection |
| | b. Strict Priority Queuing |

| | |
|---|---|
| **8.4** | Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy |
| **8.5** | Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic |
| **9** | **Security** |
| **9.1** | Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail |
| **9.2** | Switch should support control plane i.e. processor and memory protection from unnecessary or DoS traffic by control plane protection policy |
| **9.3** | Switch should support for stringent security policies based on time of day of Layer-2 to Layer-4 |
| **9.4** | Switch should support for external database for AAA using: |
| | a. TACACS+ |
| | b. RADIUS |
| **9.7** | Switch should support DHCP Snooping |
| **9.8** | Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol |
| **9.11** | Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes |
| **9.12** | Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port |
| **9.13** | Switch should support Spanning tree BPDU protection |
| **10** | **Manageability** |
| **10.1** | Switch should support for embedded RMON/RMON-II for central NMS management and monitoring |
| **10.2** | Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail |
| **10.3** | Switch should provide remote login for administration using: |
| | a. Telnet |
| | b. SSH v2 |
| **10.6** | Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures |
| **10.7** | Switch should support for management and monitoring status using different type of Industry standard NMS using: |
| | a. SNMP v1 and v2 |
| | b. SNMP v3 with encryption |
| | c. Filtration of SNMP using Access list |
| | d. SNMP MIB support for QoS |
| **10.8** | Switch should support for basic administrative tools like: |
| | a. Ping |
| | b. Traceroute |
| **10.9** | Switch should support central time server synchronization using Network Time Protocol NTP v4 |

| | |
|---|---|
| **10.10** | Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces |
| **10.11** | Switch should support for predefined and customized execution of script for device mange for automatic and scheduled system status update for monitoring and management |
| **10.12** | Switch should provide different privilege for login in to the system for monitoring and management |
| **10.13** | Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding |
| **11** | **IPv6 features** |
| 11.1 | Switch should support for IPv6 connectivity and routing required for network reachability using different routing protocols such |
| | a. OSPF v3 |
| | b. BGP with IPv6 |
| | c. IPv6 Policy based routing |
| | d. IPv6 Dual Stack etc |
| | e. IPv6 Static Route |
| | f. IPv6 Default route |
| | g. Should support route redistribution between these protocols |
| 11.2 | Switch should support multicast routing in IPv6 network using PIMv2 Sparse Mode |
| 11.3 | Switch should support for QoS in IPv6 network connectivity |
| 11.4 | Switch should support for monitoring and management using different versions of SNMP in IPv6 environment such as: |
| | a. SNMPv1, SNMPv2c, SNMPv3 |
| | b. SNMP over IPv6 with encryption support for SNMP Version 3 |
| 11.5 | Switch should support syslog for sending system log messages to centralized log server in IPv6 environment |
| 11.6 | Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events |
| 11.7 | Switch should support for IP V.6 different types of tools for administration and management such as: |
| | a. Ping |
| | b. Traceroute |
| | c. VTY |
| | d. SSH |
| | e. TFTP |
| | f. DNS lookup |
| 11.8 | All relevant licenses for all the above features and scale should be quoted along with switch |
| 11.9 | Switch and optics should be from the same OEM |

## SOR-B-2: Internet Firewall:

| SN. | Specifications |
|---|---|
| **1** | **Industry Certifications and Evaluations** |
| 1.1 | The Firewall solution offered must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant for Enterprise Firewall published by Gartner from last 3 years |
| **2** | **Hardware Architecture** |
| 2.1 | The appliancebased security platform should be capable of providing firewall, application visibility, and IPS functionality in a single appliance |
| 2.2 | The appliance should have at least 8 * 1 GE and 8*10G ports from day one |
| 2.3 | The appliance hardware should be a multicore CPU architecture with a hardened operating system |
| **3** | **Performance & Scalability** |
| 3.1 | Should support at least 10 Gbps of NGFW Real world performance (includes FW, Application Visibility & IPS) from day one |
| 3.2 | NG Firewall should support at least 4,00,0000 concurrent sessions |
| 3.3 | NG Firewall should support at least 50,000 connections per second |
| 3.4 | NG Firewall should support at least 1024 VLANs |
| **4** | **High-Availability Features** |
| 4.1 | Firewall should support Active/Standby or Active/Active failover |
| 4.2 | Firewall should support 802.3ad functionality for the failover control & date interfaces for provide additional level of redundancy |
| 4.3 | Firewall should support redundant interfaces to provide interface level redundancy before device failover |
| 4.4 | Firewall should support 802.3ad functionality to increase the bandwidth for a segment. |
| 4.5 | Firewall should have integrated redundant power supply without any external adaptors |
| **5.** | **Firewall Features** |
| 5.1 | Solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance. |
| 5.2 | Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously |
| 5.3 | Firewall should support operating in routed & transparent mode |
| 5.4 | Should support Static, RIP, OSPF, OSPFv3 and BGP/BGPv6 |
| 5.5 | Firewall should support manual NAT and Auto-NAT, static NAT, dynamic NAT, dynamic pat |
| 5.6 | Firewall should support Nat66 (IPv6-to-IPv6), Nat44 (IPv4 to IPv4) and IPv6 to IPv4 to IPv6 for translation/tunneling functionality. |
| 5.7 | Firewall should support Multicast protocols like IGMP, PIM, etc. |
| 5.8 | Should support security policies based on security group in source or destination fields or both |
| 5.9 | Should support capability to receive contextual user information like username, IP address, authentication status, location and device information from 3rd party vendors |

| | |
|---|---|
| 5.10 | Should support capability to limit bandwidth on basis of apps / groups, Networks / Geo, Ports, etc. |
| 5.11 | Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.). |
| 5.12 | Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports. |
| 5.13 | Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events. |
| 5.14 | Should be capable of detecting and blocking IPv6 attacks. |
| 5.15 | Deleted. |
| 5.16 | Solution should support the capability to configure the access policy on the basis of IP Address, User ID/Group, VLAN, Network, Objects, Device type, Location, Ports, Protocols, etc. |
| 5.17 | Solution must provide IP reputation feed that comprised of several regularly updated collections of poor reparation of IP addresses determined by the proposed security vendor |
| 5.18 | Solution must support IP reputation intelligence feeds from in-house/third party and custom lists of IP addresses including a global blacklist. |
| 5.19 | Should support URL and DNS threat intelligence feeds to protect against threats |
| 5.20 | Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic. |
| 5.21 | Deleted. |
| 5.22 | Should support more than 3000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness. |
| 5.23 | Should support the capability (by purchasing license) of providing network-based detection of malware by checking the disposition of unknown files in the cloud using the SHA-256 file-hash as they transit the network and capability to do dynamic analysis on premise (if required in future) on purpose built-appliance |
| 5.24 | NGFW OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection. |
| 5.25 | The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.). |
| 5.26 | Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location |
| 5.27 | The detection engine should support the capability of detecting variants of known threats, as well as new threats |
| 5.28 | The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Identify and explain each type of detection mechanism supported. |
| **6.** | **VPN features** |
| 6.1 | Firewall should support RFC 6379 based Suite-B Cryptography Suites/algorithms like AES-GCM/GMAC support (128-, 192-, and 256-bit keys) |
| 6.2 | Firewall should support latest IKEv2 standards. |

| | |
|---|---|
| 6.3 | Should support pre-shared keys & Digital Certificates for VPN peer authentication |
| 6.4 | Should support perfect forward secrecy & dead peer detection functionality |
| 6.5 | Should support Nat-T for IPsec VPN |
| **7.** | **Regulatory Compliance** |
| 7.1 | Firewall shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment. |
| 7.2 | Firewall shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements. |
| **8.** | **Evaluation Compliance** |
| 8.1 | Firewall/ Firewall's Operating System should be tested and certified for EAL 4/NDPP or above under Common Criteria Certification or FIPS Level 2 Certifications |
| 8.2 | Firewall/ Firewall's Operating System should be USGv6/IPv6 Certified/IPv6 logo ready |
| **9** | **Management** |
| 9.1 | The management platform must be accessible via a web-based interface and ideally with no need for additional client software |
| 9.2 | The management platform must provide a highly customizable dashboard. |
| 9.3 | Deleted. |
| 9.4 | The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication. |
| 9.5 | Should support REST API for monitoring and config. programmability |
| 9.6 | Should support troubleshooting techniques like Ping, Trace route, etc. |
| 9.7 | The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV. |
| 9.8 | The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG). |
| 9.9 | The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports. |
| 9.10 | The management platform should support risk reports like advanced malware, attacks and network |
| 9.11 | The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools. |

***********************

# CHAPTER-3-B

## INSPECTION AND INSTALLATION, TESTING & COMMISSIONING

1. TESTS AND MEASUREMENTS

All equipment's shall be subjected to tests as per technical specification and requirement specified in Chapter-3, Part-A, at manufacturer facility/premises and a test report for each equipment duly signed by the testing authority and accepted by suitable authority shall be submitted along with the equipment.

1.1 TEST CATEGORIES

1.1.1 The following tests shall be conducted for acceptance of the equipment and the system before final acceptance of the system.

i) Factory Acceptance Testing (FAT)
ii) Pre-commissioning test (after installation) for total integrated system.
iii) Site Acceptance Testing (SAT)
i) Trial Run / Field Trials.

Under exceptional circumstance, if it is not feasible to conduct Factory Acceptance Testing (FAT) at manufacturing facility, the equipment shall be accepted on the basis of certified manufacturer test report. In that case preliminary inspection of the equipment shall be arranged by the vendor at a suitable facility within India and detail inspection at site as per mutually agreed testing procedure. Exemption of inspection at factory premises (FAT) will be at the sole discretion of RailTel.

1.1.2 These tests shall be carried out on all equipment supplied by tenderer including those supplied by sub-vendors, if any. Tenderer shall arrange all necessary test instruments, manpower, test-gear, accessories etc.

1.1.3 All technical personnel assigned by Tenderer shall be fully conversant with the system specifications and requirements. They shall have the specific capability to make the system operative quickly and efficiently and shall not interfere or be interfered by other concurrent testing, construction and commissioning activities in progress. They shall also have the capability to incorporate any minor modifications/suggestions put forward by Purchaser/Engineer.

1.1.4 Test Plan: The Contractor shall submit to Purchaser 'Test Plans' well in advance of commencement of actual testing in each of the above mentioned test categories.

The plans shall include:

1.1.4.1 System/Equipment functional and performance description (in short) and Tests to be conducted and purpose of test.

1.1.4.2 Test procedures (including time schedule for the tests) and identification of test inputs details and desired/expected test results

1.1.5 Test Report: The observations and test results obtained during various tests conducted shall be compiled and documented to produce Test Reports by Tenderer. The Test Reports shall be given for each equipment/item and system as a whole. The report shall contain the following information to a minimum:

1.1.5.1 Test results

1.1.5.2 Comparison of test results and anticipated/expected (as per specifications) test result as given in test plans and reasons for deviations, if any.

1.1.5.3 The data furnished shall prove convincingly that:

a. The system meets the Guaranteed Performance objectives
b. Mechanical and Electrical limits were not exceeded.
c. Failure profile of the equipment during the tests are well within the specified limits.

1.1.6 Failure of Cards/Components:

Till the system is accepted by the Purchaser, a log of each and every failure of cards/components shall be maintained. It shall give the date and time of failure, description of failed component/ card with serial no., lot no. etc, circuit, module, component designation, effect of failure of component on the system/ equipment, cause of failure, date and time of repair, mean time to repair etc. Repair/modification done at any point of time at one site shall be carried out by Tenderer at all the sites. Detailed documentation for the same shall be submitted to Purchaser for future reference.

If the malfunction and/or failures of a unit/module/sub-system/equipment repeat during the test, the test shall be terminated and Tenderer shall replace the necessary component or module to correct the deficiency. Thereafter, the tests shall commence all over again from the start.

If after the replacement the equipment still fails to meet the specification, Tenderer shall replace the equipment with a new one and tests shall begin all over again. If a unit/ subsystem/module have failed during the test, the test shall be suspended and restarted all over again only after the Tenderer has placed the Equipment back into acceptable operation. Purchaser’s approval shall be obtained for any allowable logical time required to replace the failed component/unit/module/sub-system.

1.1.7 Re-adjustments

No adjustments shall be made to any equipment/cards during the acceptance tests. If satisfactory test results cannot be obtained unless readjustments are made, Tenderer shall carry out only those readjustment needed to ready the equipment/system for continuance of tests. A log of all such adjustments shall be kept giving date and time, equipment, module, circuit, adjustments, reasons, test result before and after adjustment etc. Fresh acceptance tests shall be conducted after the readjustments have been completed.

## 1.2 FACTORY ACCEPTANCE TESTING (FAT)

Factory acceptance tests shall be carried out after review and approval of FAT procedure/documents as per bid requirements and review of Pre-Factory acceptance results & shall be conducted at the manufacturing facilities from where the respective equipment/subsystems are offered. The factory acceptance testing shall be conducted in the presence of the Purchaser/Engineer. The tests shall be carried out on all equipment/items including those supplied by Sub-vendors and factory acceptance certificates shall be issued. The factory tests shall include but not be limited to:

1.2.1 Equipment Testing:

1.2.1.1 Mechanical checks to the equipment for dimensions, inner and outer supports, finishing, welds, hinges, terminal boards, connectors, cables, painting etc.

1.2.1.2 Electrical checks including internal wiring, external connections to other equipment etc.

1.2.1.3 Check for assuring compliance with standards mentioned in the specifications.

1.2.1.4 Individual check on each/module/sub-assembly in accordance with the modes and diagnostics programs of the Tenderer

1.2.1.5 Checks on power consumption and heat dissipation characteristics of various equipment.

1.2.1.6 Environment testing and other laid down tests in Type Tests plan of the specification of the equipment.

1.2.1.7 Functional testing

1.2.1.8 Any other test not included in FAT document but relevant to the project as desired by the Purchaser/Engineer at the time of factory acceptance testing.

All equipment’s materials fittings and components will be subject to inspection by the purchaser or his representative at the manufacturer’s factory/tenderer works before dispatch and no materials shall be dispatched until these are inspected and/or approved.

Under exceptional circumstance, if it is not feasible to conduct Factory Acceptance Testing (FAT) at manufacturing facility, the equipment shall be accepted on the basis of certified manufacturer test report. In that case preliminary inspection of the equipment shall be arranged by the vendor at a suitable facility within India and detail inspection at site as per mutually agreed testing procedure. Exemption of inspection at factory premises (FAT) will be at the sole discretion of RailTel.

1.2.2 System Integration Testing

Functional and performance test should be conducted for the complete system/ all major equipment constituting the system (including the equipment supplied by sub-vendors, as applicable) simulating the complete network with appropriate network elements. All equipment shall be connected using the same cables (interfaces/components) as will be used during final installation so that the system can be tested in its final configuration. This testing shall be conducted at the manufacturing facility of the main equipment.

1.3 INSTALLATION:

After successful completion of Factory Acceptance Test or acceptance report of equipment on the basis of certified manufacturer test report, equipment shall be sent to site for installation.

All equipment shall be checked for completeness as per the specifications of equipment required for a particular station. Installation shall be carried out in accordance with the installation manuals and approved installation drawings in the best workmanship.

The contractor shall be responsible for ensuring that the work throughout are executed in the most substantial, proper and workmanlike manner with the quality of material and workmanship in strict accordance with the specifications and as per sound industrial practices and to the entire satisfaction of the RailTel.

If during installation and commissioning any repairs are undertaken, the maintenance spares supplied with equipment shall not be used for the repair. Tenderer shall arrange his own spare parts for such activities till such time the system has been finally accepted by the Purchaser. A detailed report & log of all such repairs shall be made available by the Tenderer to Purchaser/Engineer and shall include cause of faults and repair details, within two weeks of fault occurrence.

Tenderer shall supply all installation materials required for proper installation of the equipment. These shall include but not be limited to, all connectors, inter-bay and inter-equipment cables, power/earthing cables, connectors, anchoring bolts, nuts, screws, washers etc. as needed.

The bidder has to ensure that installation of equipment shall be done as to present neat and clean appearance in accordance with approved installation document drawings. All inter bay, power supply and other cables shall be routed through wall mounted cable trays. No cable shall be visible. Equipment installed at one of the site shall be made as model site and Tenderer shall take approval from Purchaser/engineer on various aspects etc.

1.4 PRE-COMMISSIONING

On completion of installation of equipment, the correctness and completeness of the installation as per Manufacturer's manual and approved installation documents shall be checked by the Tenderer on his own.

A list of Pre-Commissioning tests (same as approved by the Purchaser/Engineer for Site Acceptance Testing) and activities shall be prepared by Tenderer and the test shall be carried out by the Tenderer on his own. After the tests have been conducted to the Tenderer own satisfaction, the Tenderer shall provide the test results for review by Purchaser/Engineer and then offer the system for Site Acceptance Testing.

During pre-commissioning, if any fault occurs to any equipment or system, Tenderer shall identify the same and provide report/history of all faults to the Purchaser.

Tenderer shall ensure that the spares meant for operation and maintenance are not used during installation and commissioning.

1.5 SITE ACCEPTANCE TESTING (SAT)

On completion of Pre-commissioning, site acceptance testing shall be conducted on the system as per approved SAT procedures and its constituents by the Tenderer under the presence of Purchaser/Engineer.

The tests shall include, but not be limited to the following:

1.5.1 Checks for proper installation as per the approved installation drawings for each equipment/item and system as a whole.
1.5.2 Guaranteed performance specifications of individual equipment/item.
1.5.3 Self diagnostics test on individual equipment
1.5.4 Tests on metering and alarm panels
1.5.5 Tests on remote alarm transmission and reception
1.5.6 System tests on per hop basis and END TO END for the ring/link, all complete.

1.6 PROVISIONAL ACCEPTANCE CERTIFICATE (PAC)

On installation of the equipment, the contractor shall certify and advise Railtel Supervisor where equipment has been installed, in writing that the installation is (i) completed (ii) ready for satisfactory commercial service and (iii) ready to be handed over. After successful completion of Site Acceptance Testing, a report (SAT) shall be forwarded to ED/DNM. Provisional Acceptance Certificate (PAC) will be issued by ED/DNM. PAC will not be held back for want of minor deficiencies not affecting the functioning of the equipment. Deficiencies, if any, pointed at the time of issuance of PAC, will be rectified by the contractor within one month.

1.7 TRIAL RUN/FIELD TRIALS

Upon conclusion of the site acceptance testing, the Tenderer shall keep the facilities commissioned for one month for 'TRIAL RUN/FIELD TRIALS'. During this period Tenderer shall provide all specialist Engineers & Technicians including experts at the NMS to maintain the total log, incidents, failures & for assisting site engineer & for total co-ordination. However, the normal operation and maintenance of the system shall be performed by the personnel of the Purchaser trained for the purpose.

If during 'TRIAL RUN/FIELD TRIALS' any defect is noted in the system, the Tenderer shall rectify, replace the same to the satisfaction of Purchaser/Engineer. The decision to repeat the final test or restart the 'Trial / Field Trials' shall be of Purchaser/Engineer depending upon the severity of the defect.

During trial run / field trial, if any fault occurs to any equipment of system, Tenderer shall identity and rectify the same and provide report, history of all faults to the Purchaser.

Ideally, during the 'TRIAL RUN / FIELD TRIALS', no shutdown of the system due to failure of equipment, power supply etc. should happen. A record of all failures shall be kept for each manned/unmanned station and the availability of the system on per hop and end to End basis shall be calculated, accordingly and results submitted to Purchaser/engineer. If the system fails to come up to the guaranteed performance, the Tenderer, within a period of thirty (30) days shall take any and all corrective measures and resubmit the system for another 'Trial Run' of trial period. All modifications, changes, corrective measures, labour etc. shall be at the cost of the Tenderer. In case the date of completion for the second trial run exceeds the time schedule for the project, he shall be liable to pay liquidated damages. If the system fails to reach the guaranteed performance even after the second trial run, the Purchaser shall be free to take any action as he deems fit against the Tenderer and to bring the system to the guaranteed performance with the help of third party at the expense of the Tenderer.

## 1.8 FINAL ACCEPTANCE CERTIFICATE (FAC)

The final acceptance of the works completed shall take effect from the date of successful completion of 12 months after issue of PAC provided in any case that the contractor has complied fully with his obligations in respect of each item under the contract. The Final Acceptance Certificate of all regions against the contract shall be issued by ED/DNM. Notwithstanding the issue of Final Acceptance Certificate, the contractor and the purchaser shall remain liable for fulfillment of any obligation incurred under the provision of the contract prior to the issue of Final Acceptance Certificate which remains unperformed at the time such certificate is issued and for determining the nature and extent of such obligation the contract shall be deemed to remain in force between the parties hereto.

## 1.9 QUALITY ASSURANCE

1.9.1 Tenderer shall submit the details of Quality Assurance program followed by them beginning with raw materials, active, passive and fabricated components, units, sub-assemblies, assemblies, wiring, interconnections, structures etc. to finished product. Tenderer shall obtain and forward the Quality Assurance Program for equipment supplied by Sub-vendor, if any.

1.9.2 The Purchaser/engineer reserves the right to inspect and test each equipment at all stages of production and commissioning of the system. The inspection and testing shall include but not be limited to raw materials. Components, sub-assemblies, prototypes, production units, guaranteed performance specifications etc.

1.9.3 For inspection and testing, Tenderer shall arrange all that is required e.g. quality assurance personnel, space, test instruments etc. for successful carrying out of the testing by the Purchaser/Engineer, at Tenderer cost, at the Manufacturer's works/tenderer premises/site.

1.9.4 Purchaser/Engineer shall have free entry and access to any and all parts of the Manufacturer's facilities associated with manufacturing and testing of the system at any given time.

1.9.5 It shall be explicitly understood that under no circumstances shall any approval of the Purchaser/Engineer relieve the Tenderer of his responsibility for material, design, quality assurance and the guaranteed performance of the system and its constituents.

1.9.6 Tenderer shall invite the Purchaser/Engineer, at least 7 days in advance, of the date at which system shall be ready for Inspection and Testing. All relevant documents and manuals approved Engineering drawings etc. shall be available with the Purchaser/Engineer well in advance of the start of Inspection and Testing.

1.9.7 Purchaser or his representative shall, after completion of inspection and testing to their satisfaction, issue factory acceptance certificates to release the equipment for shipment. No equipment shall be shipped under any circumstances unless a factory acceptance certificate has been issued for it, unless agreed otherwise by Purchaser/Engineer.

****************

# CHAPTER-3-C

## TRAINING, VENDOR DATA REQUIREMENT, DOCUMENTATION, AND DESIGN GUIDELINES

### 1. TRAINING

Tenderer shall train personnel of Purchaser/engineer in all aspects of offered system.

The training course shall be conducted at the manufacturing facilities from where the respective equipment/subsystems are manufactured/ offered or in India if the firm can arrange full fledged training facilities in case their manufacturing facilities are located outside India.

It shall be explicitly understood, that Purchaser's/Engineer's personnel shall be fully associated during Engineering, Installation, Testing and Commissioning activities and this opportunity shall be taken by Tenderer to impart on the job training in addition to the above training course.

Tenderer offer excludes costs of transportation, lodging and boarding of the trainees which shall be arranged by the Purchaser.

The training course to be conducted at the manufacturing facilities shall be designed to train the trainees in all aspects of System engineering, equipment operation, installation and functional details, theory of operation of equipment, trouble shooting and familiarization with the equipment at card and component level. All equipment used for training shall be identical to those quoted and supplied for site installation in hardware and software versions.

Tenderer shall provide comprehensive documentation, course material, manuals, literature etc. as required for proper training of personnel at his own cost. Consolidated and comprehensive documentation shall be available to each participant. After the completion of course, all such materials shall become the property of the PURCHASER. Tenderer shall update the course material of manuals in case there are any changes owing to revision/modifications in equipment/system specifications.

Tenderer shall, prior to start of training, send complete training program including details of each course, duration, subject matter etc. The Purchaser/Engineer reserves their right to suggest any additions/deletions in the program, which shall be incorporated by the Tenderer at no additional cost.

### 2. VENDOR DATA REQUIREMENT AND DOCUMENTATION

One set of Documentation shall be supplied with each system. In addition, 12 more sets of full documents shall be supplied. All documents and manuals shall be in English language only.

The following documents for the complete system shall be supplied and approved by Purchaser/Engineer in order to start inspection:

a. System description, System configuration diagram & Connectivity diagram

b. Detail technical manual of each type of equipment

c. Equipment interconnection diagram including details of various interfaces, signaling protocols used at each stage.

d. Layout of equipment and space requirements for each station.

e. Installation manual including installation procedure and commissioning.

f. Supervisory configuration, alarm list, operator interface etc.

g. Maintenance manual of each type of equipment containing:

   i. Preventive maintenance procedures.

ii. Trouble shooting/repairs procedures including failure analysis shall provide exhaustive information about repairs including but not limited to removal, reinsertion of components and cards, repairs, adjustments, tuning, calibration, tools required for a particular operation, test points, including turnaround time for repair and the details of the maintenance support service center to be furnished in the bid and all other maintenance related details.

iii. Expansion possibilities of the system without causing deterioration in the system performance.

iv. Any other data, document not specifically mentioned, but required for the satisfactory testing, installation and commissioning, operation and maintenance of the system shall be provided.

v. Documents to be supplied after trial runs but before System commissioning (Acceptance of the System by Purchaser/Engineer).

3. DESIGN GUIDELINES

i) Equipment shall conform to the similar housing standards and shall preferably be integrated in one 19”/21” rack.

ii) All equipment shall have sufficient number of alarms and supervisory indications and shall be provided with self-diagnostic facilities. All alarms and monitoring & diagnostic facilities shall be built-in & shall be displayed on the front panel of the equipment for ease of maintenance. It shall be possible to transmit these indications, parameters to the control station /NMS on real time basis.

iii) The healthy/unhealthy condition of the units shall be displayed by different color LEDs/Lamps.

iv) For important switches, the maintenance personnel shall provide controls on the front panel with suitable safeguard to avoid accidental operation. Manual changeover should be performed by more than one sequential operating procedure to avoid accidental operation.

v) All equipment shall be immune to EMI; RFI interference generated by any nearby source & shall meet the latest international standards in this regard.

vi) The equipment shall be capable of functioning with minimum maintenance and shall be preferred to have no requirement of any preventive maintenance.

vii) All patch cords shall be provided with connectors matching to the cable used and shall have identification markings.

viii) All sub-assemblies or modules, switches and controls and the circuit components shall be so mounted as to permit their replacement without appreciable disturbance to other components.

ix) If the vendor is not using distributed power supply system on individual module basis then the Power supply cards shall be duplicated (1+1). However one standalone power supply card shall be able to run the system for its entire lifetime.

x) All equipment sub racks, housings shall be provided with antistatic wristbands, if required for safe handling of Cards.

xi) The equipment should have modular design and should be configurable in number of operational modes to perform complex and different network functions without need of any additional software.

*****************

## CHAPTER 4

## COMMERCIAL TERMS & CONDITIONS

### 1. Offer letter and Validity of offer

1.1. The bidder shall complete the offer letter (Chapter 1) and the Price Schedule (Chapter 2) furnished in the tender documents, indicating the goods to be supplied, description of the goods, associated technical literature, quantity and prices etc.

1.2. The offer should remain valid for a minimum period from the date of opening of tender including the date of opening as indicated in Bid Data Sheet (BDS) Chapter 5.

### 2. Warranty

2.1. The warranty would be valid for a period as indicated in Bid Data Sheet (BDS) Chapter 5. The supplier shall warrant that stores to be supplied shall be new and free from all defects and faults in material, workmanship and manufacture and shall be of the highest grade and consistent with the established and generally accepted standards of materials of the type ordered and shall perform in full conformity with the specifications and drawings. The supplier shall be responsible for any defects that may develop under the conditions provided by the contract and under proper use, arising from faulty materials, design or workmanship such as corrosion, inadequate quantity of material to meet equipment requirements, inadequate contact protection, deficiencies in design and/ or otherwise and shall remedy such defects at his own cost when called upon to do so by the Purchaser who shall state in writing in what respect the stores are faulty.

2.2. If it becomes necessary for the contractor to replace or renew any defective portion/portions of the supplies under this clause, the provisions of the clause shall apply to the portion/portions of the equipment so replaced or renewed or until the end of the above-mentioned period or twelve months, whichever may be later. If any defect is not remedied within a reasonable time of 30 days, the Purchaser may proceed to do the work at the contractor’s cost, but without prejudice to any other rights which the Purchaser may have against the contractor in respect of such defects

2.3. Replacement under warranty clause shall be made by the contractor free of all charges at site including freight, insurance and other incidental charges.

### 2.4. Warranty Support

2.4.1. Material for repair during Warranty Period shall be handed over /taken over to contractors engineer at RailTel Data Center Gurgaon/Secunderabad or nearest RailTel PoP.

2.4.2. During the warranty period, the contractor shall be responsible to the extent expressed in this clause for any defects that may develop under the conditions provided for by the contract and under proper use, arising from faulty materials, design or workmanship in the plant, or from faulty execution of the plant by the contractor but not otherwise and shall remedy such defects at his own cost when called upon to do so by the Purchaser Engineer who shall state in writing in what respect the portion is faulty.

2.4.3. During the free warranty maintenance period contractor should stabilize the working of the system. Purchaser has the right to extend the period of supervision of the maintenance free of cost till the system stabilizes and works satisfactorily for a reasonable period of time. If during the time any equipment etc. is to be added or deficiencies are to be rectified to make the system work trouble free the same also will have to be done by the contractor at no cost to RailTel as to make good all the deficiencies.

2.4.4. In case of hardware failure the replacement must be given in next business day If the Bidder fail to replace as per below mentioned duration, the following penalties will be imposed. It will be calculated on quarterly (3 month) basis and maximum penalties will be 10 % of the cost of Equipment per year.

2.4.5. Replacement Services

During warranty and AMC period, if the Bidder fails to replace /Equipment card/Part in next business day, the following penalties will be imposed.

| **Equipment** | **Duration of repair** | **Deduction/Penalties** |
|---|---|---|
| All Modules and accessories | More than 1 days and up to 7 days | 2% of the cost of affected part/module |
| All Modules and accessories | More than 7 days and up to 15 days | 10% of the cost of affected part/module |
| All Modules and accessories | More than 16 days and up to 30 days | 25% of the cost of affected part/module |
| All Modules and accessories | More than 30 days | 100% of the cost of affected part/module |

Note:

a. In event of that bidder fails on both service SLA and replacement services the maximum aggregate penalties would be limited to equipment cost.

b. OEM should provide facility to RailTel for direct fault case open on TAC Support in case emergency.

### 2.5. Maintenance Supervision

2.5.1. After the proposed network is commissioned and placed in service and after Provisional Acceptance Certificate (PAC) is issued, the contractor shall be responsible for proper maintenance supervision of the network free of cost for a period of twelve months from the Successful commissioning of the solution.

2.5.2. To summarize, the total period of warranty as per BDS in Chapter-5, will comprise of first 12 months of Maintenance Supervision (after issue of PAC) extendable by RailTel for reasons as explained, as per para 2.5 above, posts which FAC will stand issued.

## 3. Long Term Maintenance Support

3.1 Tenderer (OEM) shall provide maintenance support after successful completion of the warranty obligations for a minimum period of 5 years. The long term maintenance support shall be comprehensive and include all hardware and software of equipment supplied against this contract. RailTel should be extended the benefits of periodical software patches/updates made by OEM on the system from time to time for equipment security/performance without any additional cost to RailTel.

3.2 Tenderer/OEM (through its Indian subsidiary), shall be paid @ 3.5% of supply cost per annum towards Long Term Maintenance Support after completion of warranty period, to undertake repairs/replacements of all type of module/ card/assembly/ subassembly and update/upgrade of software released during this period and /or which may fail in the network after the warranty. Only incremental cost in % over and above this, if perceived by the OEM and Tenderer, may be indicated in Schedule of Requirement and shall be added to the equipment cost towards evaluation of tender. If however the tenderer feels that his AMC Cost is less than 3.5% per annum, he should give suitable discount in equipment pricing. For AMC he will be paid @ 3.5% per annum only. If the Tenderer quotes a higher base rate for AMC, he will be paid at his quoted rate per annum and five years differential cost shall be added to offered cost for evaluation. AMC would have to be valid for minimum period of 5 years after the warranty.

In case tenderer quotes AMC rates lower than 3.5%, no advantage will be given to him for evaluation purposes. In case the tenderer wins the contract his cost will be reduced by differential (w.r.t. 3.5%) AMC rates & he will be paid accordingly. AMC charges to him, however be paid only @ 3.5% per annum.

3.3 Separate agreement for AMC (Long term Maintenance Support) before expiry of warranty period shall be entered with OEM/the authorized partner of OEM by RailTel. A fresh Bank Guarantee @10% of issued LOA/PO value valid for 64 months (4 months beyond the AMC period of 5 years) from the date of issue of LOA shall be required to be submitted by OEM/ Tenderer for due fulfillment of long term maintenance support obligation.

3.4 Quarterly payment for AMC Charges would be made by RailTel after successful completion of AMC Services of that quarter and on the certificate furnished by concerned RailTel representative of the CNOC.

Note: The acceptance of the above clause is mandatory and specific acceptance from OEM is required to be enclosed as per Form no.3. Any deviation / non acceptance will lead to rejection of the bid summarily

## 4. Delivery Period

The materials as per SOR are required to be delivered within period as indicated in Bid Data Sheet (BDS, Chapter 5) to the site /transported to different locations which will be provided by RailTel to the successful bidder.

## 5. Payment Terms

5.1 Payment shall be made in Indian Currency (Rs) 75% payment of the value of the supply items would be made on receipt of material by the consignee (at site / the stores) duly inspected and on submission of the following documents subject to any deductions or recovery which RailTel may be entitled to make under the contract:

- Invoice (GST)
- Delivery Challan/e-way bill.
- Packing list.
- Factory Test Report/Certified manufacturer Test Report
- Purchaser's Inspection certificate
- Consignee receipt
- Warranty certificate of OEM
- Insurance certificate
- Certificates duly signed by the firm certifying that equipment/ materials being delivered are new and conform to technical specification.

5.2 15% payment of the value of Supply items of the PO shall be made by RailTel on successfully Installation & Commissioning at site, 5% payment of value of Supply items of the PO on issue of Provisional Acceptance Certificate (PAC) and the last 5% payment of the value of Supply items of the PO shall be made by RailTel on issue of Final Acceptance Certificate (FAC) which will be issued by ED/DNM.

5.3 15% payment of value of supply items of the PO which could not be installed within 90 days due to site readiness or other reason on account of RailTel will be made with approval of ED/DNM and remaining (5% + 5%) on issue of PAC and FAC.

5.4 RailTel shall make payments after the submission of invoice with required documents as per contract. Accounting/Bill passing unit for SOR for supplies is Corporate Office. All Bills shall be submitted to the ED/DNM for certifying and verification and onwards submission to Finance of RailTel Corporate Office for releasing the payment.

5.5 Deleted.

5.6 The breakup of taxes has to be furnished and same should be reflected in the bills so that any CENVAT/input credit can be availed by RailTel.

5.7 Payment of Services Items

5.7.1 Payment of service items shall be made in Indian Currency (INR) only. 90% payment of SOR item towards “Installation, Testing & Commissioning" shall be made by Corporate Office on successful Installation, testing & commissioning, 5% on issue of PAC and final 5% on issue of Final Acceptance Certificate.

5.7.2 Payments for Resident Engineer will be paid on quarterly basis after satisfactory go ahead from competent authority.

5.7.3 Payment of SOR item towards “AMC " would be paid quarterly by the Corporate Office after satisfactory completion of AMC Services of that quarter and on certificate furnished by DC Team.

## 6. Performance Bank Guarantee (Security Deposit)

6.1 The successful bidder has to furnish security deposit in the form of Performance Bank guarantee @ 10% of issued PO/ LOA value, the same should be submitted within 30 days of issue of LOA/PO, failing which a penal interest of 15% per annum shall be charged for the delay period i.e. beyond 30 (thirty) days from the date of issue of LOA/PO. This PBG should be from a Scheduled Bank and should cover warranty period plus three months for lodging the claim. The performance Bank Guarantee will be discharged by the Purchaser after completion of the supplier's performance obligations including any warranty obligations under the contract.

6.2 The earnest money shall be released on submission of PBG. The Performa for PBG is given in Chapter 6 Form No. 1. If the delivery period gets extended, the PBG should also be extended appropriately.

6.3 The Performance Bank Guarantee (security deposit) will bear no interest.

6.4 This PBG would be released after satisfactory completion of contract including warranty period and only after submission of 10 % PBG towards AMC.

6.5 A separate advice of the BG will invariably be sent by the BG issuing bank to the RailTel’s Bank through SFMS and only after this the BG will become acceptable to RailTel. It is therefore in interest of bidder to obtain RailTel’s Bank IFSC code, Its branch and address and advise these particulars to the BG Issuing bank and request them to send advice of BG through SFMS to the RailTel’s Bank.

## 7. Taxes & Duties

7.1 The price quoted in the offer should be firm, fixed indicating the break up and inclusive of all taxes and duties like import, custom, anti-dumping, CGST, IGST, SGST, UTGST etc. The offer should be inclusive of packing, forwarding, freight up to destination, insurance charges.

7.2 Bidder shall issue valid tax invoice to RailTel for availing proper credit of CGST/SGST/IGST/UTGST in case of award of contract. GST will not be reimbursed in the absence of valid tax invoice.

7.3 For all the taxable supplies made by the vendor, the vendor shall furnish all the details of such taxable supplies in the relevant returns to be filled under GST act.

7.4 If the vendor fails to comply with any of the above, the vendor shall pay to purchaser any expense, interest, penalty as applicable under the GST act.

7.5 In case of incorrect reporting of the supply made by the vendor in the relevant return, leading to disallowance of input credit to purchaser, the vendor shall be liable to pay applicable interest under the GST act to the credit of purchaser. The same provisions shall be applicable in case of debit/credit notes.

7.6 Tenderer shall quote all-inclusive rates, but there shall be break up of basic price and all type of applicable taxes such as SGST/CGST/IGST/UTGST along with respective HSN/SAC code under GST law (Including tax under reverse charges payable by the recipient).

7.7 Wherever the law makes it statutory for the purchaser do deduct any amount towards GST at sources, the same will be deducted and remitted to the concerned authority.

7.8 The imposition of any new tax and/or increase/ in the aforesaid taxes, duties, levies, after the last stipulated date for the receipt of tender including extensions if any and the bidder there upon necessarily and properly pays such taxes/levies/cess, the bidder shall be reimbursed the amount so paid, provided such payments, if any, is not, in the opinion of RailTel attributable to delay in execution of work within the control of bidder. The bidder shall within a period of 30 days of the imposition of any such tax or levy or cess, give a written notice thereof to RailTel that the same is given pursuant to this condition, together with all necessary information including details of input credit relating thereto. In the event of no payment/default payment of any of the above taxes, RailTel reserves the right to withhold the dues/payments of bidder and make payment to states/central government authorities as may be applicable. However, if the rates are reduced after the last stipulated date for receipt of tender, bidder has to pass on the benefits to RailTel.

7.9 In case of imported equipment:
Anti-Dumping duty if applicable on the equipment proposed to be supplied by OEM/Tenderer as per extant instructions of Ministry of Commerce/Finance Government of India, has to be borne by the tenderer and shall be deducted from the amount payable to the bidder at the time of making payment to the firm, if this duty amount is paid to custom Authority by RailTel.

7.10 Inter se position of the offers will be determined on total unit rate on CIP destination basis which will include basic rate, custom duty, CGST, SGST, IGST, UTGST, freight, Insurance and any other charges or cost quoted by the tenderer, including GST payable on reverse charge by RailTel, whenever applicable.

7.11 In regards to works contract, the tenderer should have registration no. for GST in respective state where work is to be executed and shall furnish GST registration certificate on award of LOA.

## 8. Insurance

8.1 The Contractor shall take out and keep in force a policy or policies of insurance from the date, the delivery of material starts (including the transit portion) against all liabilities of the Contractor or the Purchaser. The contractor shall take out and keep in force a Policy or policies of Insurance for all materials covered in schedule of requirement irrespective of whether used up in the portion of work already done or kept for the use in the balance portion of the work until such material are provisionally handed over to RailTel. The goods will be issued by purchaser to supplier and risk of goods shall remain with supplier until the issue of PAC by RailTel. Insurance policy has to be kept valid by the contractor till issue of PAC by RailTel.

8.2 The Contractor should insure the stores brought to site, against risks as required under the Emergency Risk (Goods) Insurance Act in force from time to time up to contract value.

8.3 It may be noted that the beneficiary of the insurance policy should be RailTel or the policies should be pledged in favor of RailTel. The contractor shall keep the policy/policies current till the equipment are handed over to the purchaser. It may also be noted that in the event of contractor's failure to keep the policy current and alive, renewal of policy will be done by purchaser for which the cost of the premium plus 20% of premium shall be recovered from the contractor.

## 9. Liquidated Damages

The timely delivery is the essence of this tender. Liquidated damages will be applicable at the rate of half percent per week or part thereof for undelivered portion of SOR subject to a maximum of 10% of the cost of Purchase order for any reason whatsoever attributed to failure of tenderer. RailTel will have the right to cancel the order, place order on alternative source besides levying the liquidated damages as above.

## 10. Transportation

The rates quoted should be CIP destination. The destination shall be defined POP / nominated office of RailTel in the proposed sections which shall be indicated by RailTel's representative.

## 11. Statutory Deduction

These will be made at source as per the rules prevalent in the area of work.

## 12. Qualification Criteria

Qualifying criteria under this clause lays down minimum acceptable qualifications in various areas to ensure that qualified tenderer has necessary experience, technical expertise, equipment and financial and human resources to successfully complete the project. Bids from bidder not meeting these qualification criteria shall be summarily rejected.

### 12.1 Technical Capability

12.1.1 The Tenderer/bidder should be an Original Equipment Manufacturer (OEM) or Authorized partner of OEM specifically authorized by OEM for bidding in this tender (as indicated in Bid Data Sheet (BDS) Chapter 5). The OEM should have proven facilities for Engineering, manufacture, assembly, integration and testing of offered system and basic facilities with respect to space, Engineering, Personnel, Test equipment, Manufacture, Training, Logistic Supports for at least past three years in the country from where the proposed equipment are planned to be supplied.

12.1.2 The Tenderer/bidder should have supplied and provision of similar offered equipment's of security solution commercially with satisfactory working as indicated in Bid Data Sheet (BDS) Chapter 5 to Government/PSUs/Telecom Service Providers/Public Listed Company during the last three years from the date of opening of tender.

12.1.3 The Bidder should have registered office in India for a minimum period of 3 years as on originally scheduled date of bid opening.

12.1.4 The Bidder should have authorization from respective OEMs and should submit the vetted BOM from their respective OEMs.

12.1.5 Each OEM can authorize up to a maximum of three (3) authorized partners to bid the tender.

12.1.6 The Bidder or their promoters having equity stake or operating partnership in bidder, should not be holding valid License for Telecom service provider/ISP/NLD, Services License of Government of India for Telecom Operation.

12.1.7 RailTel reserves the right: -

a) To verify, if so desired, the correctness of documentary evidence furnished by the tenderer.

b) To verify the successful operation and performance of qualifying projects and tenderer shall arrange permission for the same.

c) To carry out capability assessment of the bidder(s) including referral to in-house information.

d) RailTel shall not be responsible for any delay in the receipt of tenders and reserves the right to accept/reject any or all tenders without assigning any reason.

12.1.8 The bidder shall furnish documentary proof of backend support including software upgrades and availability of spares for a period of 5 years from the respective OEMs of the products offered.

12.1.9 The tenderer/OEM should submit the details of supply of offered equipment executed as indicated in Bid Data Sheet (BDS) Chapter 5, along with certificates from the original user for whom the project was undertaken certifying the date of award of contract, date of completion, and the present working state of the system which should clearly bring out performance of the equipment. The certificates are to be submitted in original or their true copies duly signed by the tenderer.

### 12.2 Financial Criteria

12.2.1 The bidder should be a company registered under the Companies Act, 1956/2013 or a partnership firm registered under Indian Partnership Act 1932 or Limited Liability Partnership Act 2008 with registered office in India and in operation for at least 3 years from the date of opening of tender and should have their registered offices in India.

Valid documentary proof of:

- Certificate of Incorporation
- Certificate of Commencement of Business.
- Certificate consequent to change of name, if applicable
- Copy of Memorandum of Association.

12.2.2 The company must be registered with appropriate authorities for all applicable statutory duties/taxes.

12.2.3 Valid documentary proof of:

a) Income Tax registration/PAN number

b) GSTIN Number

12.2.4 Income Tax returns for the last three years.

12.2.5 The tenderer should present at least one (1) project worth at least INR 7.78 Crore showcasing supply, design, installation, testing, commissioning, implementation and operations projects for Data Center solutions commercially in India in the last 3 years.

Copy of work orders supported with relevant documentary evidences for the same and the completion certificates by the client. Documentary evidence should clearly indicate the nature of systems implemented for each project

12.2.6 The sum total of the turnover (i.e. revenue from operations) during the last preceding 3 financial years (i.e. current year and three previous financial years) from the date of opening of tender should be a minimum of the value as indicated in Bid Data Sheet (BDS) Chapter 5.

12.2.7 Tenderer should produce Audited Balance Sheet and Income statement of all the preceding three financial years.

12.2.8 The tenderer shall furnish such documents as to establish the financial soundness of their company. The latest balance sheet audited or certified by a neutral agency shall be furnished.

12.2.9 In the event of foreign Original Equipment Manufacturer (OEM), Indian Subsidiary is allowed to participate with the experience and financial credential of parent company with specific authorization for doing so from the OEM. The specific authorization addressed to RailTel should be submitted by the tenderer.

## 13. System Performance Guarantee

13.1 The tenderer shall give unqualified and unconditional guarantee that when the equipment / material supplied by him is installed and commissioned at site, it shall achieve the desired objective and that in the event of performance of the system when installed not complying with the end objective or with the specifications, he shall provide further inputs to enable the RailTel to realize the end objectives with full compliance of the specifications contained in these documents. No additional payment will be made to the contractor for supply of any additional goods and service required in this regard.

13.2 This certificate in the Proforma given in Chapter 6 Form No. 2, shall accompany the final offer. Absence of this certificate which will form part of the agreement shall disqualify the tenderer automatically.

## 14. Evaluation of Offer

14.1 For the purpose of relative ranking of offers, all-inclusive value for entire supply, supervision of installation, testing & commissioning and warranty period support, training, AMC shall be taken into account.

14.2 Additional features offered by the bidder, over and above the ones asked for in the tender documents, shall not be considered for evaluation of bids.

14.3 The tenderer should make available the offered products, if desired during technical evaluation of offered equipment for testing and benchmarking at any testing facility approved by RailTel.

14.4 The bidders should quote for all items & the offer will be evaluated in totality. The bidders should indicate brand name, type/model number of the products offered. Optional items will be considered for evaluation of offers. The equipment should be supplied as per Technical Specifications given in Chapter-3.

### 15. Security Considerations & Security Agreement

15.1 While evaluating the tender, regards would be paid to National Defence and Security considerations.

15.2 The directives issued from time to time by the Department of Telecommunications (DoT), Ministry of Communications and IT or any other Ministry of Govt. of India on security considerations shall be applicable to the present tender. Accordingly, as per the extent amendment of the National Long Distance (NLD) Service License Agreement for Security related concerns for expansion of Telecom Services in various zones of the country issued vide Department of Telecommunication, Ministry of Communication and IT, Govt. of India's letter no. 10-54/2010-CS-III (NLD) dated: 31.05.2011, the successful tenderer/OEM shall comply with the provisions stated in the above mentioned directive of DoT and shall have to enter into an agreement with RailTel as per the template agreement between Telecom Service Provider and the vendor of equipment, product and services (available on DoT website). The tenderer must submit a declaration along with their bid.

15.3 The Network is being provided primarily to meet the requirement of Indian Railways. Accordingly, the network shall take into consideration the National Security requirement and National Security aspects indicated by the Indian Railways~~.~~

### 16. Purchaser's Right to Vary Quantities

The purchaser shall be at liberty to enhance or reduce the quantity mentioned in the purchase order as indicated in Bid Data Sheet (BDS) Chapter 5 without assigning any reasons. The bidder shall comply with such modifications unconditionally provided these are made before completion of the deliveries under the purchase order. Any such change in quantity shall have no impact on the rates mentioned in the purchase order for any such item.

### 17. Purchaser's Right to accept any offer / Bid and to reject any or all offer/ Bid

The Purchaser reserves the right to accept or reject any offer / bid, and to annul the bidding process and reject all offers / bids, at any time prior to award of order without assigning any reason whatsoever and without thereby incurring any liability to the affected bidder or bidders on the grounds for the Purchaser's action.

### 18. Execution of Purchase Order

18.1 The successful bidder has to submit the copy of the Purchase order duly signed on each page including Annexures & will submit the Performance Bank Guarantee as per Clause no. 6 for due fulfillment of the PO.

18.2 If the successful bidder fails to submit the accepted copy of PO and required PBG within 30 days from the date of issue, it shall constitute a breach of the agreement affected by the acceptance of the tender in which case the full value of the earnest money accompanying the tender shall stand forfeited without prejudice to any other rights or remedies. The

Tenderer shall also submit the inspection plan, Implementation plan etc, within 30 days period.

18.3 In the event of any tenderer, whose tender is accepted, refuses to execute the PO as herein before provided, RailTel may determine that such tenderer has abandoned the Purchase Order and thereupon his tender and acceptance thereof shall be treated as cancelled and RailTel shall be entitled to forfeit the full amount of the Earnest Money and to recover the damages for such default.

## 19. Annulment of Award

Failure of the successful bidder to comply with the requirement of various clauses of tender document shall constitute sufficient ground for the annulment of the award and forfeiture of EMD in which event the Purchaser may make the award to any other bidder at the discretion of the Purchaser or call for new offers/ bids.

## 20. Earnest Money Deposit (EMD)/ Bid Security

20.1 The tenderer shall furnish a sum as given in Bid Data Sheet (BDS) Chapter 5 as Earnest Money through IREPS Portal.]

20.2 The EMD may be forfeited if a bidder withdraws his offer or modifies the terms and conditions of the offer during validity period and in the case of a successful bidder, if the bidder fails to accept the Purchase order and fails to furnish performance bank guarantee (security deposit) in accordance with clause 6.

20.3 Offers not accompanied with Earnest Money shall be summarily rejected.

20.4 Earnest Money of the unsuccessful bidder will be discharged / returned as promptly as possible but not later than 30 days after the expiry of the period of offer / bid validity prescribed by the Purchaser.

20.5 The successful bidder’s EMD will be discharged upon the bidder’s acceptance of the purchase order satisfactorily and furnishing the performance bank guarantee in accordance with clause 6.

20.6 Earnest Money will bear no interest.

## 21. Preference to make in India

Preference to make in India will be applicable as per (i) Ministry of Commerce and Industry / Department of Industrial Policy and Promotion (Public procurement Section) notification No. P-45021/2/2017-PP (BE-II) dt. 28.05.2018 and (ii) Ministry of Communication/ Department of telecommunications notification number 18-10/2017-IP dt. 29.08.2018 or any latest notification issued by Government of India.

## 22. Offer/ Bid Prices

22.1 The bidder shall give the prices indicating all levies and taxes, packing forwarding, freight and insurance etc. The basic unit price and all other components of the price need to be individually indicated against the goods it proposes to supply under the tender document as per schedule given in Chapter 2. The price shall be quoted in Indian Rupees or in any major foreign currency for the imported items (FOR/CIP destination).

22.2 The breakup of price of each item of SOR in terms of basic Unit price, Excise duty, Sales Tax, Freight, Custom Duty, Forwarding, Packing, Insurance and any other Levies/charges already paid or payable by the tenderer shall be quoted in the SOR Chapter 2. Any changes in statutory duties/taxes after opening of technical bid will be to RailTel's account within the contracted delivery period.

22.3 All prices and other information like discounts etc. having a bearing on the price shall be written both in figures and in words in the prescribed offer form (SOR). In case of difference in words and figures, the amount written in words will be taken into consideration. In the event of any discrepancy between total unit cost and total cost, the value shown in total unit cost will be taken for evaluation purpose.

22.4 Fall Clause: - The tenderer shall undertake that in case the tenderer offers same type of material at a lower price to any other purchaser including Central/State/ Government Organization or Public Sector Undertaking, during the validity of purchase order, the equal benefit of lower prices will be passed on to RailTel. The tenderer will submit an undertaking to this effect while claiming the payment.

## 23. Clause wise Compliance

Clause wise compliance statement of the Technical Specifications (Chapter 3) and Commercial Terms & Conditions (Chapter 4) shall be enclosed with the offer along with the technical literature of the material and other documents in support of relevant clauses.

## 24. Inspection

24.1 Pre-shipment / pre-dispatch inspection shall be carried out at manufacturer's / tenderer's works/site by RailTel's authorized representative. At least part of the material should be offered for inspection within 60 days of issue of confirmed Purchase Order. Traveling, lodging & boarding expenses of RailTel's representative and charges for 3rd party inspection if any shall be borne by RailTel but necessary facilities to carry out tests/witness inspection shall be provided by the manufacturer/ tenderer, free of cost. Under exceptional circumstance, if it is not possible to carry out pre-dispatch inspection at manufacturer's premises, Exemption for the same shall be obtained from competent authority.

24.2 Along with inspection call, the tenderer/manufacturer shall submit details of test procedures, test programme, test parameters together with permitted values, etc. and their Quality Assurance Plan.

24.3 In case material fails during inspection, the fresh lot of material shall be offered without any extra cost, by the manufacturer/tenderer. In such a case, total cost of re-inspection including travel, lodging & boarding of the inspecting officials shall be to manufacturer's/ tenderer's account.

## 25. Force Majeure

25.1 If during the Agreement, the performance in whole or in part, by either party, of any obligation under this is prevented or delayed, by reason beyond the control of the parties including war, hostility, acts of the public enemy, civic commotion, sabotage, Act of State or direction from Statutory Authority, explosion, epidemic, quarantine restriction, strikes and lockouts (as are not limited to the establishments and facilities of the parties), fire, floods, earthquakes, natural calamities or any act of GOD (hereinafter referred to as EVENTS), provided notice of happenings of any such EVENT is given by the affected party to the other, within twenty one (21) days from date of occurrence thereof, neither party shall have any such claims for damages against the other, in respect of such non-performance or delay in performance. Provided service under this Agreement shall be resumed as soon as practicable, after such EVENT comes to an end or ceases to exist.

25.2 In the event of a Force Majeure, the affected party will be excused from performance during the existence of the Force Majeure. When a Force Majeure occurs, the affected party after notifying the other party will attempt to mitigate the effect of the Force Majeure as much as possible. If such delaying cause shall continue for more than sixty (60) days from the date of the notice stated above, the party injured by the inability of the other to perform shall have the right, upon written notice of thirty (30) days to the other party, to terminate this Agreement. Neither party shall be liable for any breach, claims, damages against the other, in respect of non-performance or delay in performance as a result of Force Majeure leading to such termination.

## 26. Settlement of Disputes

26.1 Any dispute or difference whatsoever arising between the parties out of or relating to the construction, meaning, scope, operation or effect of this contract or the validity or the breach thereof shall be settled by arbitration in accordance with the Arbitration and Conciliation Act, 1996 as amended and the award made in pursuance thereof shall be binding on the parties. The venue of such arbitration or proceedings thereof shall be New Delhi.

26.2 All arbitration proceedings shall be conducted in English. Recourse against any Arbitral award so rendered may be entered into court having jurisdiction or application may be made to such court for the order of enforcement as the case may be.

26.3 The Arbitral Tribunal shall consist of the sole Arbitrator appointed by mutual agreement of the parties.

26.4 Each of the parties agree that notwithstanding that the matter may be referred to Arbitrator as provided herein, the parties shall nevertheless pending the resolution of the controversy or disagreement continue to fulfill their obligation under this Agreement so far as they are reasonably able to do so.

## 27. Governing Laws

The Purchase Order shall be interpreted in accordance with the laws of India. The courts at New Delhi shall have exclusive jurisdiction to entertain and try all matters arising out of this contract.

## 28. Termination for Default

The purchaser may, without prejudice to any other remedy for breach of contract, by written notice of default, sent to the Tenderer, terminate this contract in whole or in part.

28.1 If the tenderer fails to deliver any or all of the goods within the time period(s) specified in the contract.

28.2 If the tenderer fails to perform any other obligation(s) under the contract; and

28.3 If the tenderer, in either of the above circumstance(s) does not remedy his failure within a period of 30 days (or such longer period as the Purchaser may authorize in writing) after receipt of the default notice from the Purchaser.

28.4 In case of any of the above circumstances the RailTel shall pay the supplier for all products and services delivered till point of termination as per terms and conditions of the contract.

However, any recovery and losses occurred to RailTel will be recovered from Contractor up to the value of contract.

## 29. Risk & Cost

If the contractor fails to deliver the equipment or honor the contractual commitment within the period fixed for such delivery in the contract, the Purchaser may terminate the Purchase contract in whole or in part, the Purchaser may proceed to purchase, upon such terms and in such manner as it deems appropriate, goods similar to those undelivered at no risk and cost to contractor. However, the security deposit of tenderer shall be forfeited/ Performance Bank Guarantee shall be encashed. The failed tenderer shall not be permitted to take part in the tender for balance work.

## 30. Termination for Insolvency

The purchaser may at any time terminate the Purchase order by giving written notice to the tenderer, without compensation to the tenderer, if the tenderer becomes bankrupt or otherwise insolvent as declared by the competent court provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Purchaser.

## 31. Rates during Negotiation

The tenderer/s shall not increase his/their quoted rates including payment terms in case the RailTel Administration negotiates for reduction of rates. Such negotiations shall not amount to cancellation or withdrawal of the original offer and the rates originally quoted will be binding on the tenderer/s.

## 32. Clarification Requests

It is solicited that the written queries/ clarifications may be sent to the RailTel's office latest by date as indicated in the Bid Data sheet (BDS) through e-mail to rajeevkumar@railtelindia.comwith copy to asablania@railtelindia.com (in word format) & hard copy by post. All relevant clarifications sought will be addressed during the pre-bid meeting scheduled as per BDS.

## 33. Submission of Offers

33.1 All offers in the prescribed forms should be submitted before the time and date fixed for the receipt of the offers.

33.2 In case the schedule of requirement quoted by tenderer is incomplete with reference to tender document, the offer is liable to be rejected.

33.3 ATTESTATION OF ALTERATION: No scribbling is permissible in the tender documents. Tender containing erasures and alterations in the tender documents are liable to be rejected. Any correction made by the tenderer/ tenderers in his/their entries must be signed (not initialed) by him/them.

33.4 The tenderer shall submit his tender in sealed cover on specified date & time as mentioned in BDS Chapter 5. Each copy of the tender shall be complete in all respects. The copies should be marked "tender name & no". The original tender paper purchased from this office or down loaded from the RailTel web site shall be returned duly signed on each page along with the original offer.

33.5 The offer shall be submitted in two packet. Both Bids Credential Bid (Techno-Commercial Bid) & Price Bid shall be sealed in separate envelopes and both envelopes put in one large envelope. Both envelopes should bear the Tender No., its description and date of closing/opening. The bid shall consist of following documents:-

33.5.1 Offer Letter complete.
33.5.2 Schedule of Requirements with quantities but with prices blanked out (this will be a replica of price bid with prices blanked out).
33.5.3 Earnest Money in prescribed form.
33.5.4 Audited balance sheet duly attested by Notary Public.
33.5.5 Constitution of Firm and Power of Attorney.
33.5.6 Clause wise compliance to tender conditions.
33.5.7 Copies of purchase orders and other documents in support of meeting qualifying criteria.
33.5.8 Complete technical data and particulars of the equipment offered, as specified in the Tender papers together with descriptive literature, leaflets, Drawings, if any, complete with list etc.
33.5.9 Documentary proof of equipment being proven and working for more than 6 months in India or outside India along with user certificate and Contact Details of user/firm.
33.5.10 Technical proposal of tenderer in conformity with system design or alternative proposal of the tenderer, if any.
33.5.11 System Performance Guarantee as per Chapter 6 Form no. 2
33.5.12 The manufacturer claiming to qualify under the scope of rules for PMA (Preferential Market Access) must submit the declaration of VA (Value Addition) as required under the issued notification for the specified period (2015-16,2016-17 & 2017-18).
33.5.13 Any other information desired to be submitted by the tenderer.
33.5.14 NIL Deviation certificate.

## 34. Constitution of Firm and power of Attorney

34.1 Any individual(s) signing the tender or other documents connected therewith should specify whether he is signing:-

34.1.1 As sole proprietor of the concern or as attorney of the sole Proprietor.
34.1.2 As a partner or partners of the firm.
34.1.3 As a Director, Manager or Secretary in the case of Limited Company duly authorized by a resolution passed by the Board of Directors or in pursuance of the authority conferred by Memorandum of Association.

34.2 In the case of a firm not registered under the Indian Partnership Act, all the partners or the attorney duly authorized by all of them should sign the tender and all other connected documents. The original Power of Attorney or other documents empowering the individual or individuals to sign should be furnished to the Purchaser for verification, if required.

34.3 The RailTel will not be bound by Power of Attorney granted by the tenderer or by the changes in the composition of the firm made subsequent to the execution of the contract agreement.

34.4 In case where the Power of Attorney partnership deed has not been executed in English, the true and authenticated copies of the translation of the same by Advocate, authorized translators of Courts and Licensed Petition Writers should be supplied by the Contractor(s) while tendering for the work.

34.5 The duly notorised Power of Attorney shall be submitted in original or duly signed.

## 35. Opening of Bids:

35.1 Bids received form the Bidders shall be opened on due date and time. The opening of the Bids shall be carried out in the physical presence of the designated representatives of RailTel and the Bidders. However, this RFP does not mandate the physical presence of the Bidders. The absence of the physical presence of the Bidders shall in no way affect the outcome of the evaluation of the Bids. During bid opening, only two authorized representatives of each bidder shall be allowed to be present.

35.2 RailTel shall subsequently examine and evaluate the Bids in accordance with the provisions set out in this Chapter.

35.3 To facilitate evaluation of Bids, RailTel may, at its sole discretion, seek clarifications in writing from any Bidder regarding its Bid.

## 36. Non-Transferability & Non-Refund ability

The tender documents are not transferable. The cost of tender paper is not refundable.

## 37. Errors, Omissions & Discrepancies

The Contractor(s) shall not take any advantage of any mis-interpretation of the conditions due to typing or any other error and if in doubt, shall bring it to the notice of the purchaser without delay. In case of any contradiction only the printed rules, and books should be followed and no claim for the mis-interpretation shall be entertained.

## 38. Wrong Information by Tenderer

If the tenderer/s deliberately gives/give wrong information in his/their tender which creates/create circumstances for the acceptance of his/their tender the RailTel reserves the right to reject such tender at any stage.

## 39. The envelope shall be addressed to the Purchaser at the following address:

Executive Director/DNM
RailTel Corporation of India Ltd.
Plot No. 143, Institutional Area,
Opposite-Gold Souk,
Sector-44, Gurgaon-122003

**Note: The envelope shall bear name of the tender, the tender no. and the words “DO NOT OPEN BEFORE” (due date).**

**40**. Offer / Bid should be delivered to the above address so as to reach up to 15:00 Hrs of due date. The offers / bids shall be opened at 15:30 Hrs on the same day in the above office in the presence of those representatives of the bidders who choose to be present. Offers / Bids received after due date and time shall be dealt as per extant rules.

In case the date of opening happens to be a holiday, the tender will be received and opened at the same time on the next working day.

## 41. Limitation of Liability

Provided the following does not exclude or limit any liabilities of either party in ways not permitted by applicable law:

41.1 The Supplier shall not be liable to the Purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the Supplier to pay liquidated damages to the Purchaser; and

41.2 The aggregate liability of the Supplier to the Purchaser, whether under the Contract, in tort or otherwise, shall not exceed the total Contract Price, provided that this limitation shall not apply to any obligation of the Supplier to indemnify the Purchaser with respect to intellectual property rights infringement.

## 42. Credential Verification

42.1 The tenderer shall submit along with the tender document, documents in support of his/their claim to fulfill the eligibility criteria as mentioned in the tender document. Each page of the copy of documents/ certificates in support of credentials, submitted by the tenderer, shall be self-attested/digitally signed by the tenderer or authorized representative of the tendering firm. Self-attestation shall include signature, stamp and date (on each page). Only those documents which are declared explicitly by the tenderer as “documents supporting the claim of qualifying the laid down eligibility criteria”, will be considered for evaluating his/their tender.

42.2 The tenderer shall submit a notarized affidavit on a non-judicial stamp paper stating that they are not liable to the disqualified and all their statements/documents submitted alongwith bid are true and factual. Standard format of the affidavit to be submitted by the bidder is available in Chapter-6 of this tender document (Form No. 4). Non-submission of an affidavit by the bidder shall result in summary rejection of his/their bid and it shall be mandatory incumbents upon the tenderer to identify, state and submit the supporting documents duly self-attested by which they/he is qualifying the Qualification Criteria mentioned in the tender document. It will not be obligatory on the part of the RailTel to scrutinize beyond the submitted document of tenderer as far as his qualification for the tender is concerned.

a. The RailTel reserves the right to verify all statements, information and documents submitted by the bidder in his tender offer, and the bidder shall, when so required by the RailTel, make available all such information, evidence and documents as may be necessary for such verification. Any such verification or lack of such verification, by the RailTel shall not relieve the bidder of its obligations or liabilities here under nor will it affect any rights of the RailTel thereunder.

b. In case of any wrong information submitted by the tenderer, the contract shall be terminated, Earnest Money Deposit (EMD), Performance Guarantee (PG) and Security Deposit (SD) of contract forfeited and agency barred for doing business on entire RailTel for 5 (five) years.

## 43. Mandatory updation of Labour Data on Railway’s shramikkalyan portal:

43.1 Contractor is to abide by the provisions of Payment of Wages Act & Minimum Wages act in terms of clause 54 and 55 of Indian Railways General Condition of Contract. In order to ensure the same, an application has been developed and hosted on website ‘www.shramikkalyam.indianrailways.gov.in’. Contractor shall register his firm/company etc. and upload requisite details of labour and their payment in this portal. These details shall be available in public domain. The Registration/updation of Portal shall be done as under:

(a) Contractor shall apply for onetime registration of his company/firm etc. in the Shramikkalyam portal with requisite details subsequent to issue of Letter of Acceptance.

Engineer shall approve the contractor's registration on the portal within 7 days of receipt of such request.

(b) Contractor once approved by any Engineer, can create password with login ID (PAN No.) for subsequent use of portal for all LoAs issued in his favour.

(c) The contractor once registered on the portal, shall provide details of his Letter of Acceptance (LoA)/Contract Agreements on shramikkalyan portal within 15 days of issue of any LoA for approval of concerned engineer. Engineer shall update (if required) and approve the details of LoA filled by contractor within 7 days of receipt of such request.

(d) After approval of LoA by Engineer, contractor shall fill the salient details of contract labours engaged in the contract and ensure updating of each wage payment to them on shramikkalyam portal on monthly basis.

(e) It shall be mandatory upon the contractor to ensure correct and prompt uploading of all salient of engaged contractual labour & payments made thereof after each wage period.

43.2 While processing payment of any 'On Account bill' or 'Final bill' or release of 'Advances' or Performance Guarantee/Security deposit', contractor shall submit a certificate to the Engineer or Engineer's representatives that "I have uploaded the correct details of contract labours engaged in connection with this contract and payments made to them during the wage period in Railway's Shramikkalyam portal at 'shramikkalyam.indianrailways.gov.in ' till________Month________Year."

*******************************************

## CHAPTER- 5

## BID DATA SHEET (BDS)

The section consists of provisions that are specific to various Clauses of the tender document COMMERCIAL TERMS & CONDITIONS Chapter 4.

| Clause | Description |
|---|---|
| Clause 1.2 | Validity of offer<br>60 days. |
| Clause 2 | Warranty<br>36 months from the Date of System Commissioning (PAC) or 40 months from the date of delivery (Only in case the delay in system commissioning is on the part of consignee) whichever is earlier. |
| Clause 4 | Delivery Period<br>Delivery and supervision of installation and commissioning within 120 days of issue of LOA/PO. |
| Clause 12.1.1 | **Technical Capability**<br>The Tenderer/bidder should be an Original Equipment Manufacturer (OEM) or Authorized partner of OEM specifically authorized by OEM for bidding in this tender. The OEM should have proven facilities for Engineering, manufacture, assembly, integration and testing of offered system and basic facilities with respect to space, Engineering, Personnel, Test equipment, Manufacture, Training, Logistic Supports for at least past three years in the country from where the proposed equipment are planned to be supplied. |
| Clause 12.1.2 | The Tenderer/bidder should have supplied and provision of similar offered security solution with satisfactory working as to Government/PSUs/ Telecom Service Providers/Public Listed Company during the last three years from the date of opening of tender. |
| Clause 12.2.1 | **Financial Criteria**<br>i) The tenderer should present at least one (1) project worth at least INR 7.78 Crore showcasing supply, design, installation, testing, commissioning, implementation and operations projects for Data Center solutions commercially in India in the last 3 years.<br>Copy of work orders supported with relevant documentary evidences for the design parameters as mentioned in criteria 4 and the completion certificates by the client.<br>Documentary evidence should clearly indicate the nature of systems implemented for each project |

| Clause | Description |
|---|---|
| | ii) The sum total of the turnover (i.e. revenue from operations) during the last preceding 3 financial years from the date of opening of tender should be Minimum of Rs. 33.33 Cr. |
| Clause 16 | Purchaser's Right to Vary Quantities<br>Up to a maximum extent of +/- 30% of SOR quantity. |
| Clause 20 | Earnest Money Deposit (EMD)/ Bid Security<br>Rs. **12,61,000**/- (Rs. Twelve Lakh Sixty One Thousand only) |
| Clause 32 | Clarification Requests<br>Last date of Submission of Clarification<br>Date: 09.04.2019 |
| Clause 32 | Pre Bid Meeting<br>Scheduled on Date: 12.04.2019 at 15:00 Hrs at RailTel Corporate Office Gurgaon. |
| Clause 33 | Last Date of Submission of Offer<br>Date: 25.04.2019<br>Time: 15:00 hours<br>Venue: same as above |
| Clause 35 | Date of Opening of Tender<br>Date: 25.04.2019<br>Time: 15:30 hours<br>Venue: same as above |

**********************

# CHAPTER- 6
## Form No. 1
## PROFORMA FOR PERFORMANCE BANK GUARANTEE BOND
## (On Stamp Paper of Rs one hundred)

**(To be used by approved Scheduled Banks)**

1. In consideration of the RailTel Corporation of India Limited, having its registered office at 6th Floor, IIIrd Block, Delhi Technology Park, Shastri Park,Delhi-110053 (Herein after called RailTel) having agreed to exempt ………………………………………………………………(Hereinafter called "the said Contractor(s)") from the demand, under the terms and conditions of an Purchase Order No.………………………………dated……………made between……………………………and……………………………………….. for (hereinafter called " the said Agreement") of security deposit for the due fulfillment by the said Contractor (s) of the terms and conditions contained in the said Agreement, on production of a Bank Guarantee for Rs. ………………………(Rs ………….. only). We ……………………………… (indicate the name of the Bank) hereinafter referred to as "the Bank") at the request of ……………. ……………. Contractor(s) do hereby undertake to pay the RailTel an amount not exceeding Rs. ……………. against any loss or damage caused to or suffered or would be caused to or suffered by the RailTel by reason of any breach by the said Contractor(s) of any of the terms or conditions contained in the said Agreement.

2. We, …………………………………………………………… Bank do hereby undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from the RailTel stating that the amount is claimed is due by way of loss or damage caused to or would be caused to or suffered by the RailTel by reason of breach by the said Contractor(s) of any of terms or conditions contained in the said Agreement or by reason of the Contractor(s) failure to perform the said Agreement. Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs . ………………………

3. We, ……………………………………….. bank undertake to pay to the RailTel any money so demanded notwithstanding any dispute or disputes raised by the Contractor(s) / Tenderer(s) in any suit or proceedings pending before any court or Tribunal relating thereto our liability under this present being, absolute and unequivocal. The payment so made by us under this Bond shall be a valid discharge of our liability for payment there under and the Contractor(s) / Tenderer(s) shall have no claim against us for making such payment.

4. We, ………………………………………… Bank further agree that the Guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Agreement and that it shall continue to be enforceable till all the dues of the RailTel under or by virtue of the said Agreement have been fully paid and its claims satisfied or discharged or till RailTel certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said Contractor(s) and accordingly discharges this Guarantee. Unless a demand or claim under the Guarantee is made on us in writing on or before the ……. ……….. We shall be discharged from all liability under this Guarantee thereafter.

5. We,…………………………………………… (indicate the name of Bank) further agree with the RailTel that the RailTel shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the Agreement or to extend time of to postpone for any time or from time to time any of the powers exercisable by the RailTel against the said contractor(s) and to forbear or enforce any of the terms and conditions relating to the said Agreement and we shall not be relieved from our liability by reason of any such variation, or extension to the said Contractor(s) or for any forbearance, act or omission on the part of RailTel or any indulgence by the RailTel to the said Contractor(s) or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have affect of so relieving us.

This Guarantee will not be discharged due to the change in the Constitution of the Bank or the Contractor(s) / Tenderer(s).

(indicate the name of Bank) lastly undertake not to revoke this Guarantee during its currency except with the previous consent of the RailTel in writing.

**Dated the day of 2019**

for ………………………………………………..

(indicate the name of the Bank)

Witness

1. Signature
Name

2. Signature
Name

Form No. 2
PROFORMA FOR THE SYSTEM PERFORMANCE GUARANTEE
(On Stamp Paper of Rs. One hundred)

The Director,
RailTel Corporation of India Limited

I / We ………………………………………………………………… hereby guarantee that the design on the basis of which we have submitted our tender no. ………………………………… has been carefully made to conform to the end objectives in the tender documents and to technical specification therein. We further guarantee that in the event of the performance of the system, when installed, not complying with the end objectives or with the specifications contained in the tender documents, we shall provide further inputs to enable the RailTel to realize the end objectives contained in these documents without any additional payment for any additional equipment which may be required in this regard. We further guarantee that all the expenses for providing the additional inputs under the System Guarantee will be borne by us. We further guarantee that these additional inputs will be provided by us to make the system workable within 1 month from the date on which this guarantee is invoked by the Purchaser. The guarantee is valid for a period of one year from the date of commissioning of the system.

(Signature of Firm's Authorized Officer)

Seal

Signature of witness:

1. …………………….

2. …………………….

Form No. 3

PROFORMA FOR THE LONG TERM MAINTENANCE SUPPORT
(To be signed by the O.E.M.)

To

The Director,
RailTel Corporation of India Limited

I / We ……………………………………………………………………. hereby confirm and accept that against RailTel Tender No. ……………………………………….. , there is a requirement of Long Term Maintenance Support as per Clause 3. We confirm that Long Term Maintenance Support shall be met by us directly or through Authorized partner, as the case may be based on contracts. I / We have gone through the requirement mentioned in the Tender document and shall provide services for the offered supply items.

(Signature of Firm's Authorized Officer)
Seal

Signature of witness:

1. …………………

2. ………………….

**Form No. 4**

FORMAT FOR AFFIDAVIT TO BE UPLOADED BY TENDERER ALONGWITH THE TENDER DOCUMENTS

(To be executed in presence of Public notary on non-judicial stamp paper of the value of Rs. 100/-. The paper has to be in the name of the tenderer) **

I…………………………. (Name and designation)** appointed as the attorney/authorized signatory of the tenderer (including its constituents),
M/s ____________________________(hereinafter called the tenderer) for the purpose of the Tender documents for the work of ______________________________ as per the tender No. _______________ of (RailTel Corporation of India Ltd.), do hereby solemnly affirm and state on the behalf of the tenderer including its constituents as under:

1. I/we the tenderer (s), am/are signing this document after carefully reading the contents.

2. I/we the tenderer(s) also accept all the conditions of the tender and have signed all the pages in confirmation thereof.

3. I/we hereby declare that I/we have downloaded the tender documents from RailTel/TCIL website www.railtelindia.com/www.tcil-india-electronictender.com. I/we have verified the content of the document from the website and there is no addition, no deletion or no alternation to be content of the tender document. In case of any discrepancy noticed at any stage i.e. evaluation of tenders, execution of work or final payment of the contract, the master copy available with the RailTel Administration shall be final and binding upon me/us.

4. I/we declare and certify that I/we have not made any misleading or false representation in the forms, statements and attachments in proof of the qualification requirements.

5. I/we also understand that my/our offer will be evaluated based on the documents/credentials submitted along with the offer and same shall be binding upon me/us.

6. I/we declare that the information and documents submitted along with the tender by me/us are correct and I/we are fully responsible for the correctness of the information and documents, submitted by us.

7. I/we undersigned that if the certificates regarding eligibility criteria submitted by us are found to be forged/false or incorrect at any time during process for evaluation of tenders, it shall lead to forfeiture of the tender EMD besides banning of business for five years on entire RailTel. Further, I/we (insert name of the tenderer)** _______________ and all my/our constituents understand that my/our constituents understand that my/our offer shall be summarily rejected.

8. I/we also understand that if the certificates submitted by us are found to be false/forged or incorrect at any time after the award of the contract, it will lead to termination of the contract, along with forfeiture of EMD/SD and Performance guarantee besides any other action provided in the contract including banning of business for five years on entire RailTel.

DEPONENT

SEAL AND SIGNATURE
OF THE TENDERER

VERIFICATION

I/We above named tender do hereby solemnly affirm and verify that the contents of my/our above affidavit are true and correct. Nothing has been concealed and no part of it is false.

DEPONENT

SEAL AND SIGNAURE
OF THE TENDERER

Place:
Dated:

**The contents in Italics are only for guidance purpose. Details as appropriate, are to be filled in suitably by tenderer. Attestation before Magistrate/Notary Public.

END of Tender Document

*************