## TECHNICAL SPECIFICATION

1. **Identity and Access Management System**

<table>
<thead>
<tr>
<th>Ser No</th>
<th>Description of Requirements</th>
<th>Compliance (Yes/No)</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The proposed solution should have a central identity manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>The multi data centre authentication/access capability should be such that the session created at one data centre should be synced and respected at a remote data centre while traversing from a locally protected app to a centrally deployed centrally protected application.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Proposed Solution should have a LDAP Directory with Directory Replication Capabilities to maintain a read only copy in remote data centres.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Solution should provide Single Sign On (SSO) with role based access control to users of application.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>The solution implemented should offer customizable landing page which can be accessible over Army Data Network. User once authenticated, the landing page should display the list of all applications authorized to him. On choosing any application, the user should be directed to that application with the correct credentials without having to separately login/ sign in. The page should also allow users to manage own attributes e.g. change password, contact details etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Solution should integrate all websites/ applications deployed over ADN (approx 500) – to incl static/ dynamic websites and applications (predominantly web based)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>The proposed solution should be able to seamlessly integrate with existing Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Solution should have the capability to integrate with Active Directory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>The solution should run in High Availability (HA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Solution should support integration with the applications running across different web/ application sever which will be hosted on different OS such as Windows/ Linux/ Solaris.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>The sys software should be completely scalable to accommodate the changing Nos of users and applications.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>System shall have complete web based administration module</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>The proposed solution should be FIDO Compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Support for interoperability with cross platforms specifically Windows and Linux</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>IDENTIFY and ACCESS MANAGEMENT SOFTWARE provider should be certifying authority under CCA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Support SSL/ TLS of latest version</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Solution should have undergone third party Vulnerability Assessment and Penetration Testing (VAPT) and proof of audit certificate should be produced</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td><strong>IDENTITY MANAGEMENT SOFTWARE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Management of Identity profiles should be central with a single repository of identity data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Entire management of identities should be web based.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Solution should be able to create, update, and delete user accounts across the enterprise environment both manually and automatically.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>The solution should enable assignment of users to single/multiple roles.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>The solution should have a workflow for provisioning/de-provisioning of identities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Solution should provide a graphical interface that allows creating and managing workflows.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Solution should automatically route access requests of users for approval to the destined administrator.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Solution should have ability to delegate approval authority to another person.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Solution should have ability to escalate a request to an alternative approver if the allotted time elapses.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Provisioning solution should provide capability to the approver to provide comments.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Should support withdrawal of non-approved requests</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Solution should be able to generate unique user IDs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Should integrate with PKI to complete user creation process.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Solution should provide auto requisition of PKI token personalization for new users being created</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Should support provisioning/de-provisioning on joining/movement of personnel on transfers and temporary assignment of roles.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>Solution should provide delegated administration.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>Solution should be able to define delegated administration by way of both administration (which users, which resources) and capabilities (full account administration, password administration only, etc.).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>Solution must support web-based self-service in terms of changing passwords, resetting forgotten passwords retrieving forgotten user login etc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>Solution must allow users to view their profile and the resources and the corresponding entitlements they have got access to.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>Must have capability to provision user accounts to target systems and applications.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>Must have out-of-box connectors available for target systems to carry out user provisioning and reconciliation operations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>The proposed solution should more then 15 Factors of Authentication based on policies defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Should have connector development framework to extend support to additional target systems for which out of box connectors are not available.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>Should have capability to allow administrators to define and enforce global password policy that includes password composition rules like - minimum length, minimum password age, warn after expires, disallow past passwords</td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>Should support complex password rules including maximum repeated characters, minimum numeric characters, alphanumeric characters, uppercase &amp; lowercase characters etc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>Should support validation of password provided against the defined password policy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>As part of forgotten password, the solution should have support to challenge the user for security answers to the questions that must have been configured at the time of user creation or self-registration. The manager of the user whose password is being reset must be notified of this password reset.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>Solution should allow users to manage their own passwords.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>Should have ability to synchronize passwords for multiple systems to the same value to reduce the number of different passwords to be remembered by the user.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>Should support delivery of password-change success/failure status to requestor using mechanisms like email</td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>Users should be able to update personal attribute information, such as address, cell phone number, etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>Solution should provide a web based front-end for help-desk administrators to use.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>Solution should provide a password exclusion list and allow restriction of using old passwords.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>Solution should support Role Based Access Control (RBAC).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>Solution should report on who had access to what on a given date.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>Solution should support the creation of custom audit policies (eg. Separation of Duties) that can be applied during access scans.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>Solution should support reporting grouped by the following: by administrator (accounts created, accounts modified, accounts deleted, password changes, complete audit history per administrator, administrative capabilities per administrator) 1. By platform or application (users per platform, provisioning history per platform, who performed the provisioning actions on target platform) 2. By workflow (requests made by user, requests approved by approver, requests denied by approver, requests escalated, delegation of approvals including to whom and for what period of time) 3. By user (audit history per user, accounts/privileges by user, self-service activity by user)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>Should support reports related to access policy, request, certification, approval, role, organization, password, resource &amp; entitlement, user.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>Should support reports like list of all the rogue accounts existing in a resource, list all orphaned accounts etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>Should support SSL/TCS digital certificate based secure encrypted communication.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>Solution should not impose a physical or logical limitation on creation of number of users, while concurrency factor will drive the proposed hardware.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>Solution should have the capability of configuring applications for single factor as well as multi factor authentication.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>The solution should support all types of web browsers like Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td><strong>ACCESS MANAGEMENT SOFTWARE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>Should have capability to provide centralized logout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>Must support integration with PKI Technologies to support certificate based authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>PKI and Digital Certificates is mandatory requirement for Ensure Legal Non-Repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>Must support OSCP based live certification validation from the CA Authority under CCA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>66</td>
<td>Should support Certificate Validation against CRL Export Dump</td>
<td></td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>Must give administrators complete visibility and control over real-time user session data including ability to search for and terminate specific sessions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>Must support delegated administration at each datacenter location to have visibility on local users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>Should allow administrators to enforce constraints on session lifetime idle timeout max number of concurrent sessions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>Should be compatible with a variety of web/app servers including Apache, IIS, IBM HTTP, Oracle HTTP, Node JS, Tomcat, Jboss, Weblogic, Websphere</td>
<td></td>
<td></td>
</tr>
<tr>
<td>71</td>
<td>Should have support to log authentication success and failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>72</td>
<td>Behavioral and Risk based Parameter Detection for user-login to provoke authentication layers in line with real-time adjusted risk profile.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>Identity and Access Management Software provider should be certifying authority under CCA.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>74</td>
<td>Support SSL/TLS of latest version</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## 2. HCI Server

<table>
<thead>
<tr>
<th>SI No</th>
<th>Description of Requirement</th>
<th>COMPLIANCE (YES / NO)</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hyper-Converged Solution for Cloud</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(a)</td>
<td>Analyst Ratings</td>
<td>The bidder shall propose Hyper Converged Integrated System from vendors placed in the leader's wave in the Forrester Wave: Hyperconverged Infrastructure (HCI). (The bidder will submit the supporting documents for the proposed solution listed in The Forrester Wave Report.)</td>
<td></td>
</tr>
<tr>
<td>(b)</td>
<td>Analyst Ratings</td>
<td>The bidder shall propose Hyper Converged Integrated System from vendors placed in the leader's quadrant in the Gartner Magic Quadrant report latest. (The bidder will submit the supporting documents for the proposed solution listed in Gartner Magic Report latest)</td>
<td></td>
</tr>
<tr>
<td>(c)</td>
<td>Benchmarks</td>
<td>Should have a Validated by LoginVSI Benchmark for Cloud for both Citrix XenDesktop and Vmware Horizon View environments.</td>
<td></td>
</tr>
<tr>
<td><strong>HARDWARE AND PERFORMANCE REQUIREMENTS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(d)</td>
<td>Offered Hyper-Converged Capacity</td>
<td>The offered appliance shall be based on modular building blocks of up to one compute node. Each block shall be built using a 2U modular chassis / enclosure housing the compute with respective storage capacity. Each of the Server nodes should be individually serviceable, without shutting down the other Server nodes</td>
<td></td>
</tr>
<tr>
<td>(e)</td>
<td>Hardware Support</td>
<td>Solution must be x86 infrastructure agnostic and available to be deployed on a choice of atleast 3 server OEMs</td>
<td></td>
</tr>
<tr>
<td>(f)</td>
<td>Hyper-Converged Infrastructure</td>
<td>Proposed solution must be based on converged IT infrastructure platform that integrates storage, compute, networking, hypervisor, real-time deduplication, compression, and optimization along with powerful data management, data protection, and disaster recovery capabilities in a standard x86 server building block.</td>
<td></td>
</tr>
<tr>
<td>(g)</td>
<td>Functionality</td>
<td>Proposed hardware must be capable to Deduplicate, Compress &amp; Optimize ALL data inline, in real-time, across all storage tiers: All handled with fine data granularity of 8KB data blocks</td>
<td></td>
</tr>
<tr>
<td>(h)</td>
<td>Hardware Specifications</td>
<td>Each Compute Block must come with the following specifications: Dual Intel Intel® Xeon® Gold 5120 Processor or higher Use of All SSD Drives for Caching and Persistent storage. Minimum 5<em>1.92TB SSD for data storage Minimum 256GB of DDR4 RAM at 2400 Mhz or above 2</em>40GbE NIC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Resiliency</td>
<td>Proposed solution must be able to support multiple points of failure with no loss of function or data.</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>During a single component failure (of any type) production services are not affected / degraded in anyway</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Solution will be deployed as a stretched cluster with Zero RTO. Solution should support stretched cluster deployment in a near site metro DC deployment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Each node should have dedicated non-shared dual-PSU's and should be able to sustain single power supply failure. Solution should not utilize micro-server architecture with shared PSU's and other components.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Must be able to sustain minimum of simultaneous 2-HDDs failures per node without DU/DL</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Must be able to sustain minimum of simultaneous 1-HDDs failures in each node of a cluster and across all nodes in the cluster without DU/DL</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Must be able to sustain one node failure in the cluster</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Must be able to sustain 1 NIC port failure</td>
<td></td>
</tr>
</tbody>
</table>

### SOFTWARE AND FUNCTIONALITY REQUIREMENTS

#### (k) Common Features Included

<table>
<thead>
<tr>
<th></th>
<th>The proposed solution must be able to provide enhanced functionality by including the following available without compromise in function or performance in both Hybrid as well as All Flash Nodes:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Global dedupe, compression and optimization with minimum impact to production workloads and guaranteed CPU and RAM available to user applications</td>
</tr>
<tr>
<td></td>
<td>VM-centric policy-based backup/recovery/DR</td>
</tr>
<tr>
<td></td>
<td>WAN-optimized data protection for VM mobility</td>
</tr>
<tr>
<td></td>
<td>Unlimited real time data Deduplication Function - licenses Included</td>
</tr>
<tr>
<td></td>
<td>Unlimited real-time data Compression Function -licenses Included</td>
</tr>
<tr>
<td></td>
<td>Unlimited capacity Backup Function- Included</td>
</tr>
<tr>
<td></td>
<td>Should include licenses for multi-site deployments of atleast 3 sites</td>
</tr>
</tbody>
</table>

#### (l) Global Unified Management

<table>
<thead>
<tr>
<th></th>
<th>Proposed solution must be able to support the following Global Unified Management features</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VM-centric management through a single pane of glass via the virtualization manager</td>
</tr>
<tr>
<td></td>
<td>Programmatic interface to enable automated tasks like failover / failback</td>
</tr>
<tr>
<td></td>
<td>The ability for a single administrator to manage all aspects of the Hyper-convergence from within the Virtualization Manager for all sites</td>
</tr>
<tr>
<td></td>
<td>Leverage existing investment of servers for hosting VMs and applications while taking advantage of the functionality of the solution</td>
</tr>
<tr>
<td></td>
<td>Globally manage Backup Policies per Datastore or per VM</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>VM-Centricity and Mobility</strong></td>
<td>Proposed solution must be able to support the following VM-Centricity and Mobility feature</td>
</tr>
<tr>
<td></td>
<td>Backups for specific VMs</td>
</tr>
<tr>
<td></td>
<td>Ability to Move specific VMs between datacenters</td>
</tr>
<tr>
<td></td>
<td>Cloning specific VMs</td>
</tr>
<tr>
<td></td>
<td>VM-level backup instead of forcing protection at the datastore or protection domain level</td>
</tr>
<tr>
<td><strong>Data Protection</strong></td>
<td>Proposed solution must be able to support the following Data Protection features</td>
</tr>
<tr>
<td></td>
<td>Backup functionality as a feature instead of a separate server / software license</td>
</tr>
<tr>
<td></td>
<td>Backup must be an independent copy of source Virtual Server and must allow restore of deleted or corrupted source Virtual Server</td>
</tr>
<tr>
<td></td>
<td>Backup to disk functionality as a feature instead of a separate license or appliance</td>
</tr>
<tr>
<td></td>
<td>Replication across separate datacenter as a feature instead of a separate server / software license.</td>
</tr>
<tr>
<td></td>
<td>Replication across separate datacenters should be optimized with minimum additional overheads. Data should not need to be rehydrated before being transferred to target datacenter.</td>
</tr>
<tr>
<td></td>
<td>The ability to carry simultaneous out bi-directional replication between two data centers</td>
</tr>
<tr>
<td></td>
<td>The ability to replicate Any-to-Any in a Mesh Data Center deployment of more than 3 DC's</td>
</tr>
<tr>
<td></td>
<td>The ability to define backup policy per datastore, a group of VMs or specific VM</td>
</tr>
<tr>
<td></td>
<td>Data Protection should have RPO of 10 minutes for local backups</td>
</tr>
<tr>
<td></td>
<td>The ability to execute backup tasks during office hours without impacting to production workloads</td>
</tr>
<tr>
<td></td>
<td>Data loss protection against a minimum of 2 simultaneous local hard disks failures per node</td>
</tr>
<tr>
<td></td>
<td>Data loss protection against a minimum of 1 simultaneous local hard disc failures in all nodes of the cluster</td>
</tr>
<tr>
<td></td>
<td>Data loss protection against single node failure in cluster</td>
</tr>
<tr>
<td><strong>Data Recovery</strong></td>
<td>The proposed solution must be able to provide backup reports for audit purpose</td>
</tr>
<tr>
<td></td>
<td>Proposed solution must be able to support the following Data Recovery features</td>
</tr>
<tr>
<td></td>
<td>Data recovery should be indepent of source Virtual Server</td>
</tr>
<tr>
<td></td>
<td>Solution should provide a backup catalog to allow any Virtual Server to be recovered to any specific point-in-time</td>
</tr>
<tr>
<td></td>
<td>Data recovery process should be simple with an RTO in minutes</td>
</tr>
<tr>
<td><strong>Disaster Recovery</strong></td>
<td>Proposed solution must be able to support the following Disaster Recovery features</td>
</tr>
<tr>
<td></td>
<td>The solution must provide a simple failover operation</td>
</tr>
</tbody>
</table>
The solution must allow creation of a Runbook to automate recovery of Virtual Servers.

The solution must allow changing of IP address of recovered Virtual Servers to match target datacenter.

The solution should allow changing Virtual Server settings (example vCPU, vRAM, VMSwitch) if required.

The solution must allow the option to test DR failover to separate network with no impact to production workloads.

The solution should have feature to assist in failback process to Primary datacenter.

(q) **Private Cloud License**

The Proposed solution must be offered with cloud-ready operating system that is ideal for highly virtualized and software defined datacenter environments.

It must include Shielded Virtual Machines, software defined networking, Storage Spaces Direct, and Storage Replica; customers receive rights to unlimited Operating System Environments (OSEs).

The proposed solution must provide following features:
- Computing environment: The virtual machine includes the same basic parts as a physical computer, such as memory, processor, storage, and networking.
- Disaster recovery and backup, Optimization.
- Solution must have features such as live migration, storage migration, and import/export to move or distribute a virtual machine.
- It must offer a remote connection tool for use with both Windows and Linux.
- The solution should have Secure boot and shielded virtual machines that protects against malware and other unauthorized access to a virtual machine and its data.
- The solution must give virtual machine direct and exclusive access to some PCIe hardware devices. Using a device in this way bypasses the virtualization stack, which results in faster access.
- The solution must prevent a virtual machine's excessive activity from degrading the performance of the host or other virtual machines.
- A virtual machine can be used as a host and create virtual machines within that virtualized host.
- The solution must have option to set up Remote direct memory access (RDMA) on network adapters bound to a virtual switch, regardless of whether switch embedded teaming (SET) is also used.
- The solution must have features to make it harder for virtualisation administrators and malware on the host to inspect, tamper with, or steal data from the state of a shielded virtual machine.
### 3. Core Switch

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Specifications</th>
<th>Compliance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Architecture</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Shall be 19” Rack Mountable</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The switch should have dual hot-swappable power supplies</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch shall have minimum 24 x 1/10G SFP+ ports, populated with 8x10G SR, 8x1G SX and 8x1G BaseT transceiver.</td>
<td>Yes / No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 RJ-45 serial console port</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 RJ-45 out-of-band management port</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Should have minimum 2GB SDRAM and 512 MB flash and 13 MB Packet buffer size</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Shall have switching capacity of minimum 480 Gbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Shall have up to 350 million pps switching throughput</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Switch should support minimum 64000 MAC address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Software Defined Networking (SDN) Capability</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OpenFlow protocol capability to enable software-defined networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Features</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The switch should support HTTP redirect function</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The switch should support User role to defines a set of switch-based policies in areas such as security, authentication, and QoS. A user role can be assigned to a group of users or devices, using switch configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Quality of Service (QoS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The switch should support Advanced classifier-based QoS to classifies traffic using multiple match criteria based on Layer 2, 3, and 4 information and apply QoS policies such as setting priority level and rate limit to selected traffic on a per-port or per-VLAN basis</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The switch should support Layer 4 prioritization to enable prioritization based on TCP/UDP port numbers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The switch should support Class of Service (CoS) to set the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The switch should support Port-based rate limiting to provide per-port ingress/egress-enforced increased bandwidth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The switch should support Classifier-based rate limiting to use an access control list (ACL) to enforce increased bandwidth for ingress traffic on each port</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The switch should support Reduced bandwidth to provides per-port, per-queue egress-based reduced bandwidth</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The switch should support Remote intelligent mirroring to mirror selected ingress/egress traffic based on an ACL, port, MAC address, or VLAN to a local or remote switch anywhere on the network</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The switch should support Remote monitoring (RMON), Extended RMON (XRMON), and sFlow v5 to provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The switch should support Traffic prioritization allows real-time traffic classification into eight priority levels that will mapped to eight queues</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><strong>Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The switch should allow assignment of descriptive names to ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The switch should leverage RADIUS to link a custom list of CLI commands to an individual network administrator's login for an audit trail documents activity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The switch should support Multiple configuration files to store easily to the flash image</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The switch should support Dual flash images to provide independent primary and secondary operating system files for backup while upgrading</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The switch should have Out-of-band Ethernet management port to enable management over a separate physical management network and keeps management traffic segmented from network data traffic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The switch should support Unidirectional Link Detection (UDLD)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6</th>
<th><strong>Connectivity</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The switch should support Jumbo frames on Gigabit Ethernet and 10-Gigabit Ethernet ports</td>
<td></td>
</tr>
<tr>
<td><strong>The switch should support following IPv6 feature</strong></td>
<td></td>
</tr>
<tr>
<td>IPv6 host: enables switch management in an IPv6 network</td>
<td></td>
</tr>
<tr>
<td>Dual stack (IPv4 and IPv6): transition IPv4 to IPv6, supporting connectivity for both protocols</td>
<td></td>
</tr>
<tr>
<td>MLD snooping: forward IPv6 multicast traffic to the appropriate interface</td>
<td></td>
</tr>
<tr>
<td>IPv6 ACL/QoS: support ACL and QoS for IPv6 traffic</td>
<td></td>
</tr>
<tr>
<td>IPv6 routing: support static, RIPv3, OSPFv3 routing protocols</td>
<td></td>
</tr>
<tr>
<td>6in4 tunneling: support encapsulation of IPv6 traffic in IPv4 packets</td>
<td></td>
</tr>
<tr>
<td>Security: provide RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7</th>
<th><strong>Performance</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The switch should support Selectable queue configurations to allow for increased performance by selecting the number of queues and associated memory buffering that best meet the requirements of the network applications</td>
<td></td>
</tr>
<tr>
<td>The switch should support Energy-efficient Ethernet (EEE) support: reduces power consumption in accordance with IEEE 802.3az</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8</th>
<th><strong>Resiliency and high availability</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The Switch should support stacking up to 9 Switch and support up to 336 Gb/s of stacking throughput. The Switch support Ring, chain, and mesh stacking topologies. Stacking not required from day-1.</td>
<td></td>
</tr>
<tr>
<td>The Switch should support Virtualized switching to provide simplified management as the switches appear as a single chassis when stacked</td>
<td></td>
</tr>
<tr>
<td>The switch should support Virtual Router Redundancy Protocol (VRRP)</td>
<td></td>
</tr>
<tr>
<td>The switch should support Nonstop switching and routing</td>
<td></td>
</tr>
<tr>
<td>The switch should support IEEE 802.3ad Link Aggregation Protocol (LACP) and support up to 144 trunks, each with up to 8 links (ports) per trunk</td>
<td></td>
</tr>
</tbody>
</table>
The switch should support IEEE 802.1s Multiple Spanning Tree

The switch should enable loop-free and redundant network topology without using Spanning Tree Protocol; allows a server or switch to connect to two switches using one logical trunk for redundancy and load sharing

The switch should provide easy-to-configure link redundancy of active and standby links

9 **Layer 2 switching**

The switch should support IEEE 802.1ad QinQ

The switch should support VLAN and tagging and support the IEEE 802.1Q standard and 4096 VLANs simultaneously

The switch should support IEEE 802.1v protocol VLANs

The switch should support MAC-based VLAN

The switch should support Rapid Per-VLAN Spanning Tree (RPVST+)

The switch should dynamically load balances across multiple active redundant links to increase available aggregate bandwidth and allow concurrent Layer 3 routing

The switch should support GVRP and MVRP

10 **Layer 3 services**

The switch should support Loopback interface address

The switch should support Route maps

The switch should support User datagram protocol (UDP) helper function

The switch should support DHCP server

The switch should support Bidirectional Forwarding Detection (BFD) to enable link connectivity monitoring and reduces network convergence time for static routing, OSPFv2, and VRRP

11 **Layer 3 routing - Should support from Day-1**

The switch should support Static IP routing for both IPv4 and IPv6 networks

The switch should support OSPFv2 for IPv4 routing and OSPFv3 for IPv6 routing

The switch should support Policy-based routing

The switch should support Border Gateway Protocol (BGP)

The switch should support RIPv1, RIPv2, and RIPvng routing

12 **Security**

The switch should support Source-port filtering

The switch should support RADIUS/TACACS+

The switch should support Secure shell

The switch should support Secure Sockets Layer (SSL)

The switch should support Port security

The switch should support MAC address lockout

The switch should support Detection of malicious attacks

The switch should support Secure FTP

The switch should support Switch management logon security

The switch should support Secure management access to deliver secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3

The switch should support ICMP throttling

The switch should support Identity-driven ACL

The switch should support STP BPDU port protection

The switch should support Dynamic IP lockdown
The switch should support DHCP protection
The switch should support Dynamic ARP protection
The switch should support STP root guard
The Switch should secure management interfaces such as SNMP, Telnet, SSH, SSL, Web, and USB at the desired level
The Switch should display a customized security policy when users log in to the switch
The switch should support CPU protection
The switch should provide filtering based on the IP field, source/destination IP address/subnet and source/destination TCP/UDP port number on a per-VLAN or per-port basis
The switch should support IEEE 802.1X
The switch should support Web-based authentication
The switch should support MAC-based authentication
authenticates client with the RADIUS server based on client's MAC address
The switch should support Concurrent authentication modes to enable a switch port to accept up to 32 sessions of 802.1X, Web, and MAC authentication
The switch should support Private VLAN

13 Convergence
The switch should support IP multicast snooping (data-driven IGMP)
The switch should support LLDP-MED (Media Endpoint Discovery)
The switch should support IP multicast routing including PIM sparse and dense modes to route IP multicast traffic
The switch should support Auto VLAN configuration for voice
The switch should support RADIUS VLAN
The switch should support Local MAC Authentication to assign attributes such as VLAN and QoS using locally configured profile that can be a list of MAC prefixes

14 Environmental Features
Shall support IEEE 802.3az Energy-efficient Ethernet (EEE) to reduce power consumption
Operating temperature of 0°C to 45°C
Safety and Emission standards including EN 60950; IEC 60950; VCCI Class A; FCC Class A

15 Warranty and Support
The below Warranty shall be offered directly from the switch OEM.
Software upgrades/updates shall be included as part of the warranty

4. UTM
<table>
<thead>
<tr>
<th>S. No</th>
<th>Specification</th>
<th>Compliance (Yes/No)</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a)</td>
<td>Network security appliance should support “Stateful” policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
(b) The proposed vendor must have a track record of continuous improvement in threat detection (IPS) and must have successfully completed NSS Labs’ NGFW Methodology v7.0 testing with a minimum exploit blocking rate of 99%.

(c) OEM should be in Leaders quadrant of Gartner’s – in Enterprise Firewall Magic Quadrant as per the latest report.

(d) Appliance shall be ICSA certified for Firewall, IPS & Gateway AntiVirus functionalities.

### Hardware & Interface requirements

(a) 14 x 1GE RJ45 inbuilt interfaces, 12 x 1GE SFP interface slots from day one

(b) The Appliance should have USB & Console Ports

### Performance and Availability

(a) The Firewall should be on multiprocessor architecture with minimum 20Gbps of Firewall throughput & support of 3,500,000 concurrent sessions, and 200,000 new sessions per second from day one and Firewall Latency should not be more than 3μs

(b) Minimum IPS throughput of 4500 Mbps for real world traffic or enterprise mix traffic

(c) Minimum Threat Prevention Throughput (measured with Application Control and IPS and Anti-Malware enabled) of 3000 Mbps for real world traffic or enterprise mix traffic

(d) IPSec VPN throughput: minimum 10 Gbps

(e) Simultaneous VPN tunnels: 1000

(f) Proposed solution must support minimum 3.2 Gbps of SSL Inspection throughput

(g) Proposed solution must support minimum 10 virtual firewall from day one

### Routing Protocols

(a) Static Routing

(b) Policy Based Routing

(c) The Firewall should support dynamic routing protocol like RIP, OSPF, BGP, ISIS

### Firewall Features

(a) Firewall should provide application inspection for LDAP, SIP, H.323, SNMP, FTP, SMTP, HTTP, DNS, ICMP, DHCP, RPC, SNMP, IMAP, NFS etc

(b) IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP

(c) Allows secure deployment of next-generation IPv6 networks, as well as hybrid environments that require simultaneous, dual stack support of IPv4 and IPv6

(d) The firewall should support transparent (Layer 2) firewall or routed (Layer 3) firewall Operation

(e) The Firewall should support ISP link load balancing.

(f) Firewall should support link aggregation functionality to group multiple ports as single port.

(g) Firewall should support minimum VLANS 2048

(h) Firewall should support static NAT, policy based NAT and PAT
### Firewall Requirements

- **Firewall should support IPSec data encryption**
- **It should support the IPSec VPN for both site-site and remote access VPN**
- **Firewall should support IPSec NAT traversal.**
- **Support for standard access lists and extended access lists to provide supervision and control**
- **Control SNMP access through the use of SNMP and MD5 authentication.**
- **Firewall system should support virtual tunnel interfaces to provision route-based IPSec VPN**
- **The Firewall should have integrated solution for SSL VPN**
- **Should support LDAP, RADIUS, Windows AD, PKI based Authentication & should have integrated 2-Factor Authentication server support & this two factor authentication can be used for VPN users for accessing internal network from outside and for Local users accessing internet from inside the network and for administrative access to the appliance or all of them**
- **The solution should have basic server load balancing functionality as an inbuilt feature**
- **Licensing should be a per device and not user or IP based (should support unlimited users)**

### Integrated IPS Features Set

- **IPS should have DDoS and DoS anomaly detection and protection mechanism with threshold configuration.**
- **Support SYN detection and protection for both targets and IPS devices.**
- **The device shall allow administrators to create Custom IPS signatures**
- **Should have a built-in Signature and Anomaly based IPS engine on the same unit**
- **Signature based detection using real time updated database & should have minimum 10000+ IPS signature database from day one**
- **Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)**
- **Signature updates do not require reboot of the unit.**
- **Configurable IPS filters to selectively implement signatures based on severity, target (client/server) and operating systems**
- **IPS Actions: Default, monitor, block, reset, or quarantine**
- **Should support packet capture option**
- **IP(s) exemption from specified IPS signatures**
- **Should support IDS sniffer mode**

### AntiVirus & AntiBot

- **Firewall should support antimalware capabilities , including antivirus, botnet traffic filter and antispyware**
- **Solution should be able to detect and prevent unique communication patterns used by BOTs i.e. information about botnet family**
| (c) | Solution should be able to block traffic between infected host and remote operator and not to legitimate destination |
| (d) | Should have antivirus protection for protocols like HTTP, HTTPS, IMAPS, POP3S, SMTPS protocols etc. |
| (e) | Solution should have an option of packet capture for further analysis of the incident |
| (f) | Solution should uncover threats hidden in SSL links and communications |
| (g) | The AV should scan files that are passing on CIFS protocol |
| (h) | The proposed system shall provide ability to allow, block attachments or downloads according to file extensions and/or file types |
| (j) | The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy. |

**Other support**

| (a) | Should support features like Web-Filtering, Application-Control & Gateway level DLP from day one |
| (b) | The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should support over 250 million webpages in 72+ categories and 68+ languages without external solution, devices or hardware modules. |
| (c) | Should support detection over 3,000+ applications in multiple Categories: Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others) |
| (d) | The product must supports Layer-7 based UTM/Firewall virtualization, and all UTM features should be supported in each virtual firewall like Threat Prevention, IPS, Web filter, Application Control, content filtering etc. |
| (e) | QoS features like traffic prioritization, differentiated services., Should support for QoS features for defining the QoS policies. |
| (f) | It should support the VOIP traffic filtering |
| (g) | Appliance should have identity awareness capabilities |
| (h) | The firewall must support Active-Active as well as Active-Passive redundancy. |
| (j) | Solution must support VRRP clustering protocol. |

**Management & Reporting functionality**

| (a) | Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI. |
| (b) | Support accessible through variety of methods, including console port, Telnet, and SSHv2 |
Support for both SNMPv2 and SNMPv2c, providing in-depth visibility into the status of appliances.

Should have capability to import configuration and software files for rapid provisioning and deployment using Trivial File Transfer Protocol (TFTP), HTTP, HTTPS.

The solution should have option for firewall configuration audit & compliance check to be done in automated or manual process.

Should capable to provide a convenient method for alerting administrators when critical events are encountered, by sending e-mail alert messages to administrator defined e-mail addresses.

Solution must allow administrator to choose to login in read only or read-write mode.

5. Lightning Protection System

<table>
<thead>
<tr>
<th>Sl. No</th>
<th>Description of Requirement</th>
<th>Compliance (Yes/No)</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a)</td>
<td>The Lightening protection should have radius of protection of 79 meters in Zone-I at 5 mtr height.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(b)</td>
<td>The Lightening Arrestor Should have profiled, in alterable and good conductor structure to generate a forced air circulation at its tip and in prolonged (Venturi System) air intakes and peripheral ejectors.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(c)</td>
<td>The Lightening should have mechanical stimulation system, no battery or electronics is to be used.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(d)</td>
<td>Lightening Arrestor should be equally effective of both positive and negative lightning strikes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(e)</td>
<td>The necessary fixing bracing PCC/grouting above the building/installation with testing commissioning to entire satisfaction of Engineer-in-charge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(f)</td>
<td>The installation of the system shall be carried out under the supervision of certified trained engineer from OEM of complete all as specified and directed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(g)</td>
<td>The certified Engineer have to produce the Certificate of Certified Engineer from OEM and having knowledge of International Standards.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(h)</td>
<td>Supply and installation of gun metal elevation rod 2 mtrs long from OEM with necessary bracing clamps, drilling, 1 fixing and grouting arrangement etc complete all as specified and directed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(i)</td>
<td>Supply and laying underground LT cable PVC insulated, PVC sheathed copper conductor single core,70 sqmm with necessary connection, laying, clipping on insulated pads, saddles all as specified and directed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(j)</td>
<td>Should provide M&amp;L for Gel compound earthing with earth enhancing compound with 25kgs including copper earth strip of size 25x3 mm with necessary clipping on insulated pads/saddles with earth pit to minimum resistance value complete all as specified and directed</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 6. Network Traffic Manager

<table>
<thead>
<tr>
<th>S No</th>
<th>Description of requirement</th>
<th>Compliance (Yes/No)</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BANDWIDTH CONTROLLER</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>An additional device for bandwidth control should be provided along with the system. The features are as follows.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>General Features</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(i) The system should ensure reliable performance for network dependent applications.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(ii) The system should reduce the impact of non-strategic traffic, and diagnose and resolve network problems</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(iii) The system should identify and control bandwidth hogs so that network administrators can identify problem users, applications and websites and apply automated policies to limit or prevent bandwidth allocation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(iv) The system should have the feature to easily monitor recreational traffic like video streaming and P2P sharing.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Technical Features</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(i) <strong>Real-time Monitoring</strong>: The system should monitor the health of network in real time and give insight about how applications are performing, bandwidth consumed by users, applications across the network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(ii) <strong>Policy-Based Shaping</strong>: The system should have the feature to prioritize how and when users, applications and websites can consume bandwidth on network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(iii) <strong>Interactive Analytics</strong>: Intuitive dashboard feature should be there to visualize activities by all users.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(iv) <strong>Application Acceleration</strong>: The system should support acceleration and caching features.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(v) <strong>Predictive Recommendations</strong>: The system should have the feature to study the patterns and trends in the network and automatically make suggestions to repair and improve network performance.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(vi) <strong>QX Boost for Skype application</strong>: Improve the quality of experience For voice, video and application sharing, QX Boost for Skype for Business correlates Skype® call data with network information to provide a complete end-to-end view of your call traffic, down to the Device level.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Hardware Features</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(i) <strong>Traffic shaping and Acceleration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(a) <strong>Shaping Throughput</strong>: 1 Gbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(b) <strong>Concurrent Flows</strong>: 220,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(c) <strong>Packets per second</strong>: 200,000/s</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(d) <strong>New Connection Rates</strong>: 10,000/s</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(e) <strong>Acceleration Throughout</strong>: 30 Mbps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
(f) Edge Cache Throughput: - 50 Mbps  
(g) Optimized Connections: - 6,000  
(h) APS Objects 250  
(i) SLA Objects 250  
(j) PDF Reports 60  
(k) Traffic Policies 1024  

(ii) **Interface Capability**  
(a) The system should have 1 x RJ45 based dedicated console port for management purpose.  
(b) The system should have at least 3 x 1G (Copper) bypass bridge pair and 2x 1G (Fiber) bypass bridge pair. Also, the system should have one additional NIC slot for future expansion.  

(iii) **Physical Parameters**  
(a) Form Factor: - 1U rack mountable  
(b) Power Rating: - 17W @ 0.13A, 22W @ 0.16A (Max)  
(c) Environment: - 0 deg cel to 40 deg cel, 5% to 90% operating humidity.

Two units of undermentioned device should provide with the system.

<table>
<thead>
<tr>
<th>A</th>
<th>SYSTEM PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Speech band</strong></td>
<td>300 to 3400 Hz</td>
</tr>
<tr>
<td><strong>Modulation</strong></td>
<td>Pulse Code Modulation</td>
</tr>
<tr>
<td><strong>No. of channels per system</strong></td>
<td>32 (30 speech channels, 1 terminal Signaling and 1 Sync. Channel )</td>
</tr>
<tr>
<td><strong>Sampling frequency</strong></td>
<td>8000 Hz</td>
</tr>
<tr>
<td><strong>No of sample bits</strong></td>
<td>8 per channel</td>
</tr>
<tr>
<td><strong>Total bits per frame</strong></td>
<td>256</td>
</tr>
<tr>
<td><strong>Bit rate</strong></td>
<td>2048 Kbps ± 50 ppm</td>
</tr>
<tr>
<td><strong>Construction and Architecture</strong></td>
<td>Chassis based modular multiplexer shelf capable of supporting minimum 12 slots for integration of data, voice, fax and LAN traffic</td>
</tr>
<tr>
<td><strong>Universal Slots</strong></td>
<td>All slots (other than for power and control) should be universal i.e. capable of accepting any type of voice/data/fax card manufactured by the same OEM.</td>
</tr>
</tbody>
</table>
| **Add-Drop or Drop - Insert Function** | a) Should be able to add-drop/drop-insert voice and data at channel (64 kbps) multiple channel (nx64 Kbps) and at E1.  
b) Add-drop should be software configurable by user in the field |
| Digital Cross Connect function | a) It should have an inbuilt cross connect facility on the same equipment  
b) Cross Connect : It should be able to map the following voice interfaces:  
i) E1 to E1  
ii) E&M (two wire or four wire) to e1 and vice versa  
iii) FXO/FXS to E1 and vice versa  
c) Add-drop should be achievable by software by user in the field |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundancy</td>
<td>Dual controller, dual power with load sharing</td>
</tr>
</tbody>
</table>
| Protection                    | 1 for 1 protection , E1, T1, FOM  
|                               | PDH ring protection, QE1, QT1, FOM, Mini QE1, 3E1 for DS0 SNCP protection                                                |
| Management                    | Console, Telnet, SNMP, and In band management support  
|                               | Craft interface port for connection to external LCD display  
|                               | Compatible to a SNMP based GUI network management system                                                               |
| No. of Slots                  | Should have 16 or more hot plug-in slots with capability to support following cards.                                  |
|                               | Single E1/Quad E1 (G.703)/ Mini-Quad E1/3'E1 card-DS0 SNCP protection  
|                               | X.21/V.35/RS232/EIA530  
|                               | 2W/4W E&M  
|                               | QFXO/QFXS/12FXo/12FXS/24FXO/2 4FXS  
|                               | 10/100 Base-T Router Card  
|                               | 2/4 channel G.SHDSL card  
|                               | 8-channel Dry Contact I/O  
|                               | Magneto Interface Card  
|                               | TDMoE (TDM over Ethernet) with 2 Combo GigaBit (GbE) interface for IP uplink                                           |
| B Interface Support: - The system shall support below mentioned interfaces/Cards.                                       |
|                               | **Network Line Interface-E1** should comply with the following specifications:-  
|                               | Number of ports | 1E1 / 4E1 / 3E1 |
|                               | Line Rate | 2.048 Mbps ± 50 ppm |
|                               | Line Code | AMI or HDB3 |
|                               | Input Signal | ITU G.703 |
|                               | Output Signal | ITU G.703 |
|                               | Framing | ITU G.704 |
|                               | Connector | BNC/RJ48C , DB25S for Mini Quad E1 |
|                               | Electrical | 120 ohm twisted pair |
|                               | Jitter | ITU G.823 |
### 2* 10/100 Ethernet Router Card with capability to handle 64 WANs should comply with the following specifications

<table>
<thead>
<tr>
<th>Number of ports</th>
<th>2 LAN ports, Max. 64 WAN ports, Each WAN port has data rate n x 64K bps, 1 ≤ n ≤ 32 (≤ 4Mbps for total of all 64 WAN ports)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td>10/100 BaseT x 2</td>
</tr>
<tr>
<td>Connector</td>
<td>RJ45</td>
</tr>
<tr>
<td>Routing protocol</td>
<td>RIP-I, RIP-II, OSPF, Static</td>
</tr>
<tr>
<td>Supporting Protocols</td>
<td>PPP (IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT, DHCP</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>Ping, Trace route</td>
</tr>
<tr>
<td>QoS</td>
<td>Rate limit</td>
</tr>
</tbody>
</table>

### 8* 10/100 Ethernet Router Card with capability to handle 64 WANs

<table>
<thead>
<tr>
<th>Number of ports</th>
<th>8 LAN ports, Max. 64 WAN ports. Each WAN port has data rate n x 64K bps.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td>10/100 BaseT x 8</td>
</tr>
<tr>
<td>Connector</td>
<td>RJ45</td>
</tr>
<tr>
<td>Routing protocol</td>
<td>RIP-I, RIP-II, OSPF, Static</td>
</tr>
<tr>
<td>Supporting Protocols</td>
<td>PPP (IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT, DHCP</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>Ping, Trace route</td>
</tr>
<tr>
<td>QoS</td>
<td>Rate limit</td>
</tr>
</tbody>
</table>

### Voice Card (8EM) port (interfaces) should comply with the following specifications:-

1. **Connector:** RJ45 connector
2. **Alarm conditioning:** CGA busy after 2.5 seconds of LOS, LOF
3. **Encoding:** a low or u low user selectable together for all.
4. **Impedance:** balanced 600 or 900 ohms.
5. **Longitudinal rejection:** 55 dB
6. **Loss adjustment:** -21 to +10 dB/0.1dB step transmit and receive
7. **Single distortion:** >46 dB with 1004 Hz, 0 dBm input
8. **Frequency response:** -0.25 to -1 dB from 300 to 3400Hz
9. **Signaling:** Type 1, Type 2, Type 3, Type 4, Type 5 transmit only
**Voice card (12 FXS/12 FXO/24 FXS/24 FXO) port (interfaces) should comply with the following specifications:**

(a) 12 FXS/FXO Connector: Twelve RJ11  
(b) 24 FXS/FXO Connector: One RJ21X  
(c) Alarm conditioning: CGA busy after 2.5 seconds of LOS, LOF  
(d) Encoding: A-law or μ-law, user selectable together for all  
(e) AC Impedance: balanced 600 or 900 ohms  
(f) Longitudinal Conversion Loss: > 46dB  
(g) Cross talk measure: Max -70dBm0  
(h) Gain Adjustment: -21 to +10 dB / 0.1 dB step transmit & receive  
(i) Signal/ Distortion: > 25dB with 1004 Hz, 0dBm input  
(j) Frequency Response: - 0.25 to -1 dB from 300 to 3400 Hz, coincide with ITU-T G.712  
(k) Loss adjustment: -21 to +10 dB/ 0.1 dB step transmit and receive  
(l) Signal / Distortion: 46 dB with 1004 Hz, 0dBm input  
(m) Frequency response: - 0.25 to -1 dB from 300 to 3400 Hz, coincide with ITU-T.  
(n) Ideal channel noise: Max -65 dB Mop  
(o) Inter modulation: coincide with ITU-T B.712  
(p) 2Wire return loss: > 2 dB echo, > 20 dB signing  
(q) FXS loop feed: Nominal -48 V dc with 20 mA current limit  
(r) Signaling: Loop Start, DTMF, pulse, PLAR, Battery Reverse  

### G.SHDSL Line port (interfaces) should comply with the following specifications:

<table>
<thead>
<tr>
<th>Number of ports</th>
<th>2 or 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line Rate for 2-channel G.shdsl</td>
<td>n x 64Kbps (n= 3 to 15)</td>
</tr>
<tr>
<td>Line Rate for 4-channel G.shdsl</td>
<td>n x 64Kbps (n= 3 to 31)</td>
</tr>
</tbody>
</table>

| Line Code | 16-TCPAM, full duplex with adaptive echo cancellation |
| Connector | RJ45 |
| Electrical | Unconditioned 19-26 AWG twisted pair |
| Sealing current | Max. 20 MA source current |
| Clock Source | From System, Line |
| Diagnostic Test | G.SHDSL Loopback: To-LINE, To-bus |

### TDM over Ethernet Card

<table>
<thead>
<tr>
<th>Combo Gigabit Ethernet (GbE) Interface</th>
<th>-&gt; Number of Ports 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-&gt; Speed 10/100/1000M bps</td>
</tr>
<tr>
<td></td>
<td>-&gt; Connector RJ45 for twisted pair GbE, LC for optical GbE, auto detection</td>
</tr>
<tr>
<td>Gigabit Ethernet (GbE) Interface</td>
<td>Number of Port 2</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>Speed 10/100/1000 BaseT</td>
</tr>
<tr>
<td></td>
<td>Connector RJ45</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ethernet Function</th>
<th>MDI/MDIX for 10/100/1000M BaseT auto-sensing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ping function contained ARP</td>
</tr>
<tr>
<td></td>
<td>Per port, programmable MAC hardware address learn limiting (max. MAC table 8192 (8k) entry)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Basic Features:</th>
<th>Packet transparency support for all types of packet types including IEEE 802.1q VLAN and 802.1ad (Q-in-Q)</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS</td>
<td>User configurable 802.1p CoS, ToS in outgoing IP frame</td>
</tr>
<tr>
<td>Traffic Control</td>
<td>Ingress packet Rate limiting buckets per port for Ethernet port</td>
</tr>
<tr>
<td></td>
<td>Supporting Rate-based and Priority-based rate limiting for LAN port.</td>
</tr>
<tr>
<td></td>
<td>Pause frame issued when the traffic exceeding the limited rate before packet dropped following IEEE802.3X</td>
</tr>
<tr>
<td>Link Aggregation</td>
<td>WAN support link aggregation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Jitter &amp; Wander</th>
<th>PPB: per G.823 Synchronous*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Compliance</td>
<td>TDMoIP (RFC5087), SAToP (RFC4553), CESoPSN (RFC5086)</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.1q, 802.1p, 802.1d, 802.3, 802.3u, 802.3x, 802.3z, 802.1s, 802.1w, 802.1AX</td>
</tr>
<tr>
<td>Co-directional port (interfaces) should comply with the following specifications:-</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>ITU G.703 64 Kbps co-directional interface</td>
</tr>
<tr>
<td>Connector</td>
<td>120ohm, RJ48</td>
</tr>
<tr>
<td>Line Distance</td>
<td>Up to 500 meters</td>
</tr>
<tr>
<td>Loopack</td>
<td>DTE Payload Loopback, Local Loopback</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Voice Card 12 MAG (Magneto)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) Connector : Twelve RJ11</td>
<td></td>
</tr>
<tr>
<td>(b) Alarm Conditioning CGA busy after 2.5 seconds of LOS, LOF.</td>
<td></td>
</tr>
<tr>
<td>(c) Encoding A-law or μ-law, user selectable together for all.</td>
<td></td>
</tr>
<tr>
<td>(d) Impedance Balanced 600 or magneto telephone impedance match.</td>
<td></td>
</tr>
<tr>
<td>(e) Longitudinal Conversion Loss &gt; 46dB.</td>
<td></td>
</tr>
<tr>
<td>(f) Gain Adjustment -21 to +10 dB / 0.1dB step transmit &amp; receive.</td>
<td></td>
</tr>
<tr>
<td>(g) Signal/ Distortion &gt; 25dB with 1004 Hz, 0dBm input.</td>
<td></td>
</tr>
<tr>
<td>(h) Frequency Response - 0.25 to -1 dB from 300 to 3400 Hz, coincide with ITU-T G.712.</td>
<td></td>
</tr>
<tr>
<td>(i) Idle Channel Noise Max. –65 dBm0p.</td>
<td></td>
</tr>
<tr>
<td>(j) Min Detectable Ringing Voltage 16 Vrms.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>C</strong> <strong>Clock Source</strong></td>
<td>Internal, E1/T1 Line, External</td>
</tr>
<tr>
<td><strong>D</strong> <strong>Alarm Relay</strong></td>
<td>Alarm Relay: max. Voltage 3 Vdc/ max. current: 1AFuse alarm, and performance alarm</td>
</tr>
<tr>
<td><strong>E</strong> <strong>System Configuration Parameters</strong></td>
<td>Active Configuration, Stored Configuration, and Default Configuration</td>
</tr>
<tr>
<td><strong>F</strong> <strong>Supervisor</strong></td>
<td>RS232 Console Port (VT100) 10 Base-T, Ethernet, SNMP In-band 64 Kbps supports HDLC/PPP, SSH</td>
</tr>
<tr>
<td><strong>G</strong> <strong>Performance Monitor</strong></td>
<td>Separate Registers Network, user, and remote site Performance Reports Reports include E1 Bursty Errored Second, Severe Errored Second, and Degraded Minutes. Also available in Statistics (%) Alarm Queue To record the latest alarm type, location, and date &amp; time Threshold Bursty Seconds, Severely Errored Second, Degraded Minutes</td>
</tr>
<tr>
<td><strong>H</strong> <strong>Diagnostics</strong></td>
<td>Loopback E1/T1 interface (Line Loopback, Payload Loopback, Local Loopback), DTE Loopback (DTE-to-DTE, DTE to Line) Test Pattern For Controller: 221-1, 215-1, 211-1, 29-1, and 4-byte user define pattern</td>
</tr>
<tr>
<td><strong>J</strong> <strong>Front Panel</strong></td>
<td>LED 1 per V.35-interface, ACO, Power, SYNC/TEST, LOF, BPV, RAI/AIS</td>
</tr>
</tbody>
</table>
The OEM should have authorized R & D & Repair/Replacement center in India with presence in India of about 10 Years.

<table>
<thead>
<tr>
<th>Certification</th>
<th>EN55022 Class A, EN50024, FCC Part 15, Class A, FCC Part 68, CS-03, IEC60950, UL60950, IEC 61850-3, IEEE 1613</th>
</tr>
</thead>
</table>

Card Configuration required as part of supply.

- Controller (CPU) card - 1 no
- 48 V Dc Power Supply Card - 1 No
- 3-Port E1 card – 1 No
- 2-port Router Card – 1 No

DC Power Source (-48V)

- Input 230 VAC (Range 170-264 VAC, single phase, 50 Hz).
- Output Current: 8 Amp
- Size: - 485(W) x 385(D) x 165(H) mm with screw terminals at front
- Should have short circuit protection.

7. Network Time Server

<table>
<thead>
<tr>
<th>SI</th>
<th>Particulars</th>
<th>Compliance (Yes/No)</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a)</td>
<td>Power Supply:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voltage</td>
<td>230 +/- 10% V AC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frequency</td>
<td>47-55 Hz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(b)</td>
<td>Functions / Features :</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Facility</td>
<td>Using Universal Time co-ordination(UTC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Propagation delay Compensation</td>
<td>Supported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accuracy</td>
<td># +/- 250 Nanosecond</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Accuracy</td>
<td>Better than 1 PPM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LCD Display</td>
<td>Front panel LCD display to show status, time and no. of satellites</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(c)</td>
<td>Inputs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPS Antenna input through BNC connector.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Supply</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(d)</td>
<td>Outputs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP output (2 nos. customizable) for NTP client access through RJ-45. Both Ports shall be independent</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RS232 serial port output (2 Nos)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pulse output: 1 PPS, ½PPM, 1PPM (Configurable).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support Client request per Second</td>
<td>10,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(e)</td>
<td>Antenna</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length of GPS</td>
<td>50 meters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gain</td>
<td>Over 30 DB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECEIVER,GLOBAL POSITIONING SYSTEM,DISPLAY TYPE:LCD,DISPLAY SIZE:2 X 3.5 INCH;DISPLAY</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 8. Smart Rack

<table>
<thead>
<tr>
<th>Ser No</th>
<th>Description</th>
<th>Parameter</th>
<th>Technical Requirement</th>
<th>Compliance (Yes/No)</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a)</td>
<td>System specifications</td>
<td>(WxDxH)</td>
<td>Maximum 800x1200x2150mm (42U)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Power supply input</td>
<td>Minimum Dual Feed AC 230V/1P/50Hz.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IT Load</td>
<td>3kW</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minimum Usable U space for IT Equipments</td>
<td>34 U</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Installation Site</td>
<td>Should be suitable for Elevated floor installation / general ground installation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Utility Entry</td>
<td>Should have provision for both Top/Bottom as Standard</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>System supported languages</td>
<td>Should support English as language for operation by default</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cabinet interior lighting</td>
<td>LED - with door limit switch</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Exterior colors</td>
<td>Black or as per OEM standard</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Front &amp; back door</td>
<td>Front toughened glass, rear plain dual door</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Local interface</td>
<td>Colour TouchScreen Display</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitoring</td>
<td>Power, Cooling, Smoke, WLD, temperature and humidity, UPS, door sensor to be integrated for monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sensor</td>
<td>Minimum 1 No. Spot sensor for water leak detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Minimum 1 No. Temperature and humidity sensors</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Minimum 1 No. Smoke sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Minimum 1 No. Proximity sensors for doors</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Minimum 1 No. Beacon- for local alarm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(b)</td>
<td>Power subsystem</td>
<td>UPS capacity</td>
<td>Minimum 6 kVA UPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UPS rated input</td>
<td>230VAC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Input Voltage Range</td>
<td>160 V - 285 V</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Input Frequency Range</td>
<td>40-70Hz</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Input Power Factor</td>
<td>0.98</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Input power consumption meter</td>
<td>Energy meter with digital display should be installed at input to monitor</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Output Max Power</td>
<td>6kVA/5.4kW</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Efficiency</strong></td>
<td>94% at 100 % Load in online &amp; 98% in Green Mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Backup Time</strong></td>
<td>15 Mins - 1 Battery Pack</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RPDU parameters</strong></td>
<td>Basic Rack PDU should be provided, Zero U, 32A, 230V, (20)C13 &amp; (4)C19</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>(c) Cooling subsystem</strong></td>
<td>Total air conditioning cooling Capacity 3.5kW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minimum Air flow 700CMH</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Air conditioning installation Should be Rack mount type, not more than 5U</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Outdoor ambient temperature -20°C ~ +45°C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refrigerant Environmental Friendly R410A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Emergency fan module Minimum 1 No. at front (Inlet) and top (Exhaust)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OEM for UPS, Racks, PDU, Sensors should be same including the monitoring software. OEM should be minimum ISO 9001, ISO 14001 and ISO 50001.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>