

GOVERNMENT OF INDIA
(Ministry of Home Affairs)
DIRECTORATE GENERAL
CENTRAL RESERVE POLICE FORCE
EAST BLOCK-7, SEC-1, R.K. PURAM, NEW DELHI-110066
(Email:- comncell@crpf.gov.in Tele/Fax:011-26107493)

No. B.V-7/2021-22-C (CSOC)

Dated, the 11th November'2021

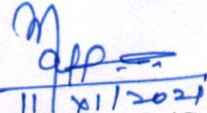
To

- | | |
|---|--|
| 1. DIG (Comn), ITBP
Block No. 2, CGO Complex
Lodhi Road, New Delhi-03 | 2. DIG (Comn), NSG
Meharam Nagar
Palam, New Delhi-37 |
| 3. DIG (Comn), SSB
East Block-V, R.K Puram
New- Delhi-66 | 4. AIG (Comn), CISF
Block No. 13, CGO, Complex
Lodhi Road, New Delhi-03 |
| 5. DIG (Prov), BSF
Block No. 10, CGO Complex
Lodhi Road, New Delhi-03 | 6. Liaison Office, Assam Rifle
Room No-171, North Block, MHA
New Delhi -01 |

Subject: Regarding revision of QRs/TDs of "Cyber Security Operating Centre".

Please find enclosed QRs/TDs of "Cyber Security Operating Centre" as Annexure-"A" duly approved by the competent authority is forwarded herewith for further necessary action.

Encl: (QRs & TDs of "Cyber Security Operating Centre")


11/11/2021
{P.R.Jha, DC (Comn)}
For DIG (Equipment)
Directorate General, CRPF

QRs OF CYBER SECURITY OPERATING CENTRE

A) SECURITY INFORMATION & EVEN MANAGEMENT (SIEM)

1. SECURITY INFORMATION AND EVENT MANAGEMENT

S.N	Description of Requirements
General	
1	<p>Collection Methodology: The proposed solution must provide agent and agent-less solution that can automatically scan the list of server and other device to be monitored and will automatically accept events and start to monitor device without any administrator intervention. In case for any specific device/ application agent are required, it must have provision for same as well.</p>
2	<p>Architecture: The capability in general of the components are given below:-</p> <p>(a) Collectors: Logs collectors will be deployed to collect logs from various device and application at a particular location. The main function (but not limited to) are:-</p> <ul style="list-style-type: none">(i) Collection(ii) Compression(iii) Encryption(iv) Caching, where the solution must provide for storing of logs in case of no communication with consolidator / correlate for minimum period of 7 days. <p>(b) Consolidator. The main function (but not limited to) are:-</p> <ul style="list-style-type: none">(i) Indexing and Searching.(ii) Reporting.(iii) Storage and Forensics. <p>(c) Correlators. Correlators will be deployed to process the event sent by various collectors/ consolidator. All logs collected should be analyzed and correlated. The main functions (but not limited to) are:-</p> <ul style="list-style-type: none">(i) Real-Time Incident Monitoring.(ii) Threat Notification and Alerting(iii) Incident Case Workflow.(iv) User and Entry Behavior Analytics. d) <p>Centralized Management Server.</p> <p>(i) The solution must provide central Management of entire SOC from a particular site and provide access to SOC administrators from other location for managing the device in their respective areas.</p>

Handwritten signature and initials

Handwritten signature and initials

S.N	Description of Requirements
	(ii) The proposed solution should provide all system-level administration through a single web User Interface. (e) All the software component of the SIEM solution must be from the same OEM .
3	Total aggregated EPS across the deployment should be 10,000 or more sustained EPS and 25,000 Peak EPS from day 1 without rated license limit of integrated devices, no of assets, no of console users, security analysts. Hardware, Virtual Machines, Operation System and all related software for all the component at all location will be supplied by the Bidder as part of turnkey solution to meet the required functionalities. The system may be delivered as appliances or as server bundled with integrated bundle of OS, software and database. Collectors will separate device with all requisite OS and applications. Consolidator and Corralator can be either same device or a separate device offering their respective functionalities with all requisite OS and applications. High Availability of device must be ensured at all location. If a correlator at any location fails, all its logs should be diverted to be handled by the alternate correlator.
4	Workflow Automation: The proposed solution must provide a SOC orchestration layer solution that can must facilitate incident Investigation and response workflow that must open tickets, assign the tickets to the appropriate team member while maintaining a complete audit trail for the incident handling process.
5	Deploying Methodology: Solution must support Hybrid deployment including Hardware, Software, Physical and virtual environment.
6	It should support any number of logs sources and devices without any licensing limitation. Solution must be designed for no log drops at any stage of the solution.
Event Collection & Normalization	
7	Device Support: The Proposed solution must provide a comprehensive coverage as cross all types of event sources (but not limited to) like Databases (SQL server 2005, 2008,2012, Oracle), ALX Server, Unix/Linux Server, Windows Server, Routers, Switches, Gateways, hubs, Windows OS 8.8.1,10, firewalls, for all types of OEM products
8	Application Logs: The solution should be able to collect security logs generated by software products like databases, web and applications like ERP etc and custom built applications.
9	Distributed Event Processing: The proposed solution must collect logs in a distributed manner, offloading the processing requirement of the logs management system for tasks such as filtering, aggregation, compression and encryption

AS CMN

Done R. A. [Signature]

S.N	Description of Requirements
10	<p><u>Custom Collection API:</u> The proposed solution must have a software tools to allow customers to create integration with unsupported legacy or internally developed event sources. The software tool must allow customer to integrate with Syslog, log files and Databases.</p>
11	<p><u>Normalized Event Data:</u> The Proposed Solution must normalized all collected event data into a consistent format.</p>
12	<p><u>Categorized Event Data:</u> The Proposed solution must categorized log data into an easy-to-understand humanly- readable format that does not require knowledge of OEM-specific event IDs to conduct investigation, defines new correlation rules, and/or create new reports/dashboards.</p>
13	<p><u>Secure Transport:</u> The proposed solution must provide encrypted transmission of log data between all the collected/consolidators and correlators.</p>
14	<p><u>Reliable Transport:</u> Logs Transmission should use reliable TCP protocol that will ensure retransmission in the event of protocol failure to ensure that no log data is lost in transit.</p>
15	<p><u>Collection Health Monitoring:</u> Any failures of the event collection infrastructure must be detected immediately and operations personnel must be notified. Health monitoring must include the ability to validate that original event sources are still sending event.</p>
16	<p><u>Event filtering:</u> The Proposed solution must provide inline (user definable) options to reduce event data by filtering out unnecessary event data before it is tored or correlated.</p>
17	<p><u>Event Aggregation:</u> Aggression must be flexible in which normalized fields can be aggregated and provide the ability to aggregate in batches or time windows. An examole of aggregated would be every 1000 identical event be aggregated into one record with the necessary start and end timestamp and the aggregate count of 1000.</p>
18	<p><u>Compression:</u> The proposed solution must provide at least 70% compression.</p>
19	<p><u>Raw Event data:</u> Proposed Solution must support the option of colleting raw event data using Syslog, FTO, SCP, SNMP, and any other protocol required for collection of logs etc. This ensures original audit data is available for forensics.</p>

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements
20	<p><u>Windows and Event Logs:</u> The proposed solution must be integrated with a Windows Domain in an agent- less fashion and collect the vent logs from multiple systems without requiring any agent to be installed on the end device.</p>
21	<p><u>Time Synchronization:</u> The SIEM solution components along with the log source should be synchronized to single time.</p>
22	<p><u>Centralized Management:</u> The proposed Solution must be managed centrally allowing users to configure all features; backup configuration and push software update etc. Using one centralized creation.</p>
23	<p><u>Event replay:</u> The Proposed solution must provide a software based tool or facility which allows production event data to be exported and replayed into the system for testing and content creation.</p>
<u>Log Management- General</u>	
24	<p><u>Scalability:</u> The proposed Solution must be scale to large environment (upto 1,00,000 EPS) with additional EPS licenses and additional hardware. This should be software based solution.</p>
25	<p><u>Storage integrity:</u> The proposed solution must utilize storage RAID levels for Local data redundancy with the ability to reinitialize a failed disk from data stored in the RAID cluster.</p>
26	<p><u>Storage Flexibility:</u> The proposed solution must be able to store log data both locally and with SAN/NAS/Tape Drive Integration.</p>
27	<p><u>Retention Policies:</u> The Proposed Solution must provide the Ability to create multiple policies for the automated retention and disposal of log data.</p>
28	<p><u>Log Data Integrity:</u> The proposed solution must provide audit quality integrity mechanisms.</p>
29	<p><u>Search interface:</u> The proposed solution must provide a simple intuitive search interface usable by different users with varying skill sets.</p>
30	<p><u>Search Drilldown:</u> The Proposed solution search interface must provide the ability to drill down on output data and alter the search filter by simply click on fields within an event.</p>
31	<p><u>Search Patterns:</u> The proposed search interface must provide support for simple Boolean-Style search patterns as well as complex regular expressions.</p>

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements
32	<p>Search Operators: The Proposed solution must provide a comprehensive list of search operators with expandable Syntax, and allow users to "grow" into complex patterns, as and when required.</p>
33	<p>Flow-based Searches: The proposed solution must allow easy and intuitive query structures which allow to compound search Expression into Complex patterns, Similar to what would otherwise required "piping" Multiple commands into Scripts using traditional tools, without requiring any knowledge of scripting languages.</p>
34	<p>Search- Structured and unstructured Data: The proposed Solution Search Performance must be capable of searching through structured (index) events as well as unstructured (natural Language) log messages.</p>
35	<p>Search Method Combination: The proposed solution search interface must provide the option to allow combined search queries using a combination of Methods such as index and in-indexed event data and regular expression and full unstructured text search simultaneously without impacting search performance.</p>
36	<p>Search Time Range: The proposed solution search interface must provide the option to search interface using either a custom time (data/ time start, end) or dynamic time (last 2 hours).</p>
37	<p>Search Result View: The proposed solution search interface must provide option to customize the output columns of the queries result. The option may include constraining the view to only normalized data or filtering the view to only see raw data.</p>
38	<p>Search Export: The log manager System must provide the ability to export the search result to the user's local system, a mounted files system or locally on the log management system for other users to view. The Export should be saved in either a csv or pdf format.</p>
39	<p>Save search Filters: The proposed solution must provide a simple, intuitive ways of allowing users to save search filters for later use and to be shared with other authorized users.</p>
40	<p>Historical Analysis: The proposed Solution must be capable of processing and storing large volume of historical log data that can be restored and analyzed for forensic investigation purpose.</p>

Handwritten signature and initials.

Handwritten signature and initials.

S.N	Description of Requirements
Log Management-Archiving	
41	Schedule Archive: The proposed solution must provide a simple interface to schedule the compression and archiving of log data.
42	Manual Archive: The proposed solution must provide a simple interface to manually archiving log data.
43	Retention: Solution will be capable of retaining online logs for 3 months with consolidator and correlate.
Log Management -Alerting	
44	Real-Time Alerts: The proposed Solution must be capable of generating alerts based on filter pattern matches for operation health monitoring.
45	Threshold Alerts: In addition to real-time alerts, the system must provide historical, threshold alerts, configuration from saved search queries.
46	Alert Filters: The proposed solution must provide per-defined alert and provide the ability to re-use pry-defined filters and own created filters as alert criteria.
47	Alert Delivery: The proposed Solution must provide options of how alerts are delivered to operations or security personnel or reporting to the web consol, send an email or generate an SNMP trap to an external management system. The solution must be capable of doing all three concurrently for each alert.
Log Management - Reporting	
48	Per-Defined Report: The proposed solution must provide per-defined reports for Operations, Security and Compliance that can easily be modified.
49	Compliance Report: Solution should provide compliance auditing, alerting and reporting.
50	Customized Reports: The proposed solution must provide the ability for customers to create their own reports with reports template, reporting wizards as well as an advance interface for power users to create their own custom report queries.

AS
2

AS
AS
AS
AS

S.N	Description of Requirements
51	<p><u>Report Export:</u> The proposed solution reporting function must be capable of exporting reports in various formats. At a minimum, the report formats should be Excel Spreadsheet (.Xls), Adobe Acrobat (.pdf), Word Document (.doc), web Page (.Html), and Comma-Separate Values (.csv). The reporting functions should also allow the report to be run and viewed ad-hoc by user as well.</p>
52	<p><u>Report Scheduling:</u> The proposed solution must provide the ability for customer to schedule and email reports to run hourly, daily, weekly or monthly as either an attachment or a URL path for users who have system access.</p>
53	<p><u>Drilldown report:</u> The proposed solution reporting engine must provide tenability to generate linked report with a master report that allows users to drill down into the data within the report dynamically.</p>
54	<p><u>Run-Time Report Options:</u> The proposed solution reporting engine must provide the ability to filter, highlight, and modify various report functions at runtime. This should include the ability to selectively define device group or storage portion to report upon.</p>
<p><u>Log Management-Dashboards</u></p>	
55	<p><u>Customizable dashboards:</u> The Proposed solution should provide dashboards specific to each user and should be user configurable. The dashboard must be capable of displaying multiple daily reports specific top each user job function.</p>
<p><u>Log Management Integration</u></p>	
56	<p><u>Syslog Forwarding:</u> The proposed solution must be able to receive raw (i.e. unprocessed) event data in the form of syslog message or text log files, in addition to receive the raw original event data from collectors.</p>
57	<p><u>Correlation- Analysis and Workflow</u></p>
58	<p><u>Correlation Rules:</u> The proposed solution must provide many correlation rules to automate the incident detection and workflow process</p>
59	<p><u>Cross-Device Correlation:</u> The proposed solution must be capable of correlating activity across multiple devices to detect authentication failures, perimeter security, worm outbreak and operational event in real-time without the need to specify particular device type.</p>
60	<p><u>Statistical Correlation:</u> the proposed solution must be capable of keeping a statistical baseline of "normal" monitored activity. This includes attacker, Target, Ports, Protocols and session data.</p>

Handwritten initials/signature

Handwritten signature

S.N	Description of Requirements
61	<p><u>Correlation Flexibility:</u> Solution must be capable of running cross device correlation, advance correlation real time correlation and historical correlation at the same time.</p>
62	<p><u>Historical Correlation:</u> The proposed solution must be capable of monitoring attack history against critical assets or by particular users.</p>
63	<p><u>Session Correlation:</u> The proposed Solution must provide the ability to correlate DHCP,VPN and active Directory event to provide session tracking for every user in the enterprise. This is essential for pinpointing who was using a particular workstation historically during an incident investigation.</p>
64	<p><u>Identity Correlation:</u> The proposed solution must natively integrate with existing authentication directories to import context related to users and role which will then correlate and attribute every event to an actual user, regardless of the event source.</p>
65	<p><u>Role Correlation:</u> The proposed solution must provide the ability to use real-time context from authentication directories in order to determine whether a user's activities are aligned with their role. This function must automatically alter the monitoring process when a user changes roles within the organization.</p>
66	<p><u>Geo-Spatial Location Correlation:</u> The proposed Solution must provide the ability to monitor activity between multiple geographical locations.</p>
67	<p><u>Dynamic/Static Lists:</u> The proposed solution must allow users to define either white list or blacklist that can be used as inclusion or exemption during the correlation process. Additionally, the correlation engine should utilize dynamic lists to provide important information such as shared user monitoring, secession tracking, attack history and privileged system access. Products must support import capability to create/ update monitoring list which can be dynamically add/removed values without manual intervention.</p>
68	<p><u>Correlation Tracking :</u> The proposed Solution must be able to correlate event data against static lists of items that the user either allows or doesn't allow on the network (i.e. list of insecure protocols). Additionally, lists should be automatically populated by the system for Tracking things such as attacks, user's session and other policy violation.</p>

Mr

Qml A. F dz

S.N	Description of Requirements
69	<p><u>Pattern Detection:</u> The system must be capable of discovering patterns of subverted activities that would otherwise go unnoticed (i.e. slow and low attacks).</p>
70	<p><u>Correlation Performance:</u> The proposed solution must be capable of efficiently presenting categorized data to the correlation engine to allow real-time detection and response.</p>
71	<p><u>Rule Chains:</u> The system must provide the ability to allow rules to be triggered in a series, matching various correlation activity before an alert is generated.</p>
72	<p><u>Vulnerability Based Correlation:</u> The proposed solution must be capable of assessing attack vector and the targeted system to determine the susceptibility of a threat and lower the priority if the target is not susceptibility and raise the severity if the target is susceptibility or the user is not Vulnerability data of each asset monitored should be imported/generated into the system which can then be used by the SIEM to manage false positive reduction or generated remediation activity to secure the system.</p>
73	<p><u>Asset Intelligence:</u> The proposed solution must provide the ability to generate/record context and keep an inventory of all data as it relates to assets. This includes hostname, IP Address, MAC, location Purpose, Owner, patch, Vulnerability data, exemption, compliance critically and other related data. The asset profile should be created for all monitored system which can be searched and correlated on.</p>
74	<p><u>Role Based Intelligence:</u> The proposed solution must provide a mechanism to logically segregate data by role, department, domain or customer.</p>
75	<p><u>Conditional Analysis:</u> The Proposed solution must allow the ability to define conditional or variable statement to derive additional information from "hard" event data to provide dynamic context during correlation and reporting. This conditional analysis must be globally available throughout the system.</p>
76	<p><u>Alert Thresholds:</u> The Proposed solution must provide the ability to aggregate and suppress alerting with granular option and use conditional logic to determine if any alert should be generated.</p>
77	<p><u>Re-usable Content:</u> The solution must allow users to create objective such as filters or search queries that are reusable throughout the system.</p>

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements
78	<p><u>Content Editor:</u> The proposed solution must provide a common interface to create or modify resources within the system. All Aspects of this editor must apply to the development of rules, reports, dashboards and other resource that will be created in the system.</p>
79	<p><u>SOC Orchestration:</u> There should not be separate rated license for orchestration engine (SOAR)</p>
80	<p><u>Case Management:</u> The proposed solution must provide complete process framework for integrating security monitoring and investigation with existing workflow procedures. Workflow should involve escalating and incident to other users within the same team or within other teams etc.</p>
81	<p><u>Workflow:</u> The process solution must provide a complete lifecycle management, audit trail and accountability (SLA management) during the incident handling or forensic category. The workflow should be customizable using tools provided in the system.</p>
<u>Colleration - Reporting and Visualization</u>	
85	<p>The system should allow configuring the parser to support any new system introduced in the future.</p>
86	<p><u>Ad Hoc Report Performance:</u> The proposed solution must have a mechanism to collect meta-data used by reports that track information over long periods of the time so that running these reports ad hoc does not take considerably longer than any other reports.</p>
87	<p><u>Dash board Drill-Down:</u> The proposed solution must provide the ability to allow analysts to drill-down from graphical dashboards to the underlying event data.</p>
88	<p><u>Attack Visualization:</u> The proposed solution must provide the ability visually represent event data into a dynamically updated graph. This will assist analysts in determining the expanse of attack and pin point the original attacker during incident response and remediation for example, -Event Graph. -Last State.</p>
89	<p><u>Content Management:</u> The proposed solution must provide the ability to synchronize its resource contents (i.e. rules dashboard, reports, filters, etc) automatically across multiple instances of the product, to support multi-instance/ high -event rate deployments.</p>

AS MR

Qml A. K. d

S.N	Description of Requirements
Correlation -Advance use Cases.	
90	<p><u>Compliance Automation:</u> The proposed solution must provide value in assisting in adhering to audit requirements, alerting of non- compliance and providing necessary reports that can be used during an audit.</p>
91	<p><u>Physical/ Logically Convergence:</u> The proposed solution must be capable of collecting log data from physically access devices such as card readers, biometrical and security cameras and correlate this information with logical network and security devices to detect such patterns as building access after office hours by contractors or users logged in through VPN and physically accessing the building within the same period.</p>
92	<p><u>Insider Threat Detection:</u> The proposed solution must be able to detect suspicious activity, such as printing large numbers of files outside working hours emailing large attachments to personal email accounts employee communication with competitors or the clearing of system audit logs to cover up malicious activity.</p>
93	<p><u>Forensic Investigators:</u> The proposed solution must be capable of allowing investigators to analyze 90 days worth of historical logs files and then perform complex pattern searches and reporting.</p>
94	<p><u>Real-Time Responses:</u> The proposed solution must be capable of triggering scripts or execute integration commands with third party solutions such as IPS or next generation intrusion prevention systems in order to quarantine or block nefarious activity in real-time.</p>
95	<p><u>Investigation & Remediation</u></p>
96	<p>Solution should have grouping common events for analysis.</p>
97	<p>Solutions should be capable of gathering information about the full context of the attack such as :-</p> <ul style="list-style-type: none"> (i) Who conducted the attack? (ii) What did they try to accomplish? (iii) When did they make the attempt? (iv) Where they attack?
98	<p>Solution should provide the information necessary to make a decision about how to remediate the threat .The solution should be able to provide incident response that consist of phases and tasks that guides the user on how to adequately responses to the incident ;integrating people processes and technology.</p>

Handwritten signature/initials

Handwritten signature/initials

Handwritten mark

S.N	Description of Requirements
	<u>Analytics -User Behavior.</u>
99	<u>User Activity Baseline:</u> The proposed solution must provide the ability to monitor user network and application activity to create baseline and then use these baseline to identify anomalous user behavior. User Behavior analysis: the solution should be able to detect anomalous behavior based on rules and behavioral anomalies.
100	<u>State or Terminated User Activity:</u> The proposed solution must be capable of automatically identifying when user accounts are terminated or state and then monitor for any activity from these accounts.
101	<u>Unaccountable User Activity:</u> The proposed solution must able to alert or report on any activity for identities that are not automatically synchronized with the authentication directories. This will help to detect rogue user accounts on critical systems.
102	<u>User Role Monitoring:</u> The proposed solution must provide the ability to synchronized with the authentication directories to collect information regarding user roles and responsibilities and correlate this data with all user activity .Users that violate their roles within the organization should be recorded for alerting and reporting purposes.
103	<u>User Activity Monitoring:</u> The proposed solutions must be able to track user activity and ultimately bind an individual to an action Analysts must be able to generate ad-hoc reports that will detail what a particular user or group of users has accessed in the enterprise for defined period of time.
104	<u>Generic Account Monitoring:</u> The proposed solution must provide the ability to correlate information regarding users that are logged into the domain where ever exists) and their accounts usage within the enterprise. The proposed solution must provide a mechanism whereby in the event of generic account violations the solution can contain the threat in real -time using quarantine methods such as disabling the user's switch ports adding filters to firewalls disabling user accounts etc.
105	<u>Miscellaneous.</u> Correlate identity attributes to a single user profile from IAM systems flat files, AD/LDAP, and HR repositories.
106	Correlate activity data to users through a common identifier (account, IP address MAC etc.).
107	<u>Account Management :</u> Uncorrelated vs correlated account identification & account tagging.
108	User based views (identify activity access policy violations risk scoreboard)

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements
109	Resource based views [correlated and uncorrelated accounts asset meta data (owner/hours/IP address) resource activity risk scorecard data management of historical transactions].
110	Lookup Data: Static data sets from flat files that the customers want to use in the policy engine (critical accounts resources assets list of domain admin).
111	Network Map: Import network information (IP address metadata) to be unused in the policy violation and behavior violation engine.
112	Organization Hierarchy & Management: Ability to create and view activities by organizations. User will belong to one organization and many peer groups.
113	Peer groups creation & management.
114	Master- Child node architecture.
115	Data Masking: Encryption in web interface controlled by privacy manager.
116	Role Based Access Control Support: Only user with specific permission can access menus, dashboards and reports control the functional control.
117	Case management Manage, White list resolve and act on user related incidents.
118	User Watch List: User accounts IP address and systems for targeted monitoring.
119	Policy Violation Engine: Flexibility to create rule based violations spanning data identity Access Peer Organization activity network classification time watch list lookup.
120	Rule based content for all devices and applications like (but not limited to) Windows, Proxy, Cisco, VPN, Citrix, Iron port, Juniper VPN, Oracle, Proxy SG, Squid Web Proxy Websense.
121	User Behavior content based content for all devices and applications like (but not limited to) Windows, Proxy, Cisco, VPN, Citrix, Iron Port, Juniper VPN, oracle, proxy SG, Squid web Proxy, Websense.

Handwritten initials/signature.

Handwritten signature and initials.

2.LOG COLLECTOR (SIEM)

S.No	Description of Requirements	
1	Chassis	4U Tower Server
2	CPU	1 x Intel Xeon E-2226G (3.4GHz/6-core) Processor or Higher
3	Memory	8 GB DDR-4 RAM - 2666 MTs
4	Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance
5	HDD Bays	Up to 4 HDD Bays. The drive carrier should have intuitive icon based display along with "DO NOT REMOVE" caution indicator that gets activated automatically in order to avoid data loss/downtime due to wrong drive removal.
6	Hard disk drive	1 TB SATA HDD
7	Interfaces	VGA Port: 1 standard (rear) Serial Port: 1 optional (rear) Network Port (RJ-45): 2 x 1 GB ports as standard (rear, 1 shared for HPE iLO) Dedicated iLO Management Port (RJ-45): 1 optional (rear) USB 3.0 Port: 6 (1 front, 4 rear, 1 internal) USB 2.0 Port: 1 (1 front)
8	Power Supply	Should support hot plug redundant low halogen power supplies minimum 2 x 500 Watt
9	Fans	Redundant hot-plug system fans
10	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support Energy Star ASHRAE A3/A4 UEFI 2.6 SMBIOS Redfish API SNMP v3 TLS 1.2 DMTF Systems Management Architecture
11	Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable 2. Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware

Handwritten signature/initials

Handwritten signature/initials

3. LOG CONSOLIDATOR (SIEM)

S.No	Description of Requirements	
1	Chassis	1U Rack Mountable
2	CPU	2 x Intel Silver Processor 4124R
3	Memory	16 DIMM slots. 4 x 32 GB
4	Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance
5	HDD Bays	Up to 8 HDD Bays The drive carrier should have intuitive icon based display along with "DO NOT REMOVE" caution indicator that gets activated automatically in order to avoid data loss/downtime due to wrong drive removal.
6	Hard disk drive	6 x 2.4 TB SAS 10K RPM
7	Controller	Hard Controller Should SUPPORT RAID 0.1 5.
8	Networking features	Server should support below networking cards: (i) 1Gb 4-port network adaptors (ii) 10Gb 2-port Ethernet adaptor (iii) 10GBaseT 4-port Ethernet adaptor (iv) 4x25Gb Ethernet adaptor (v) 10/25Gb 2-port Ethernet adaptor (vi) 100Gb Ethernet Infinib and Options: 40Gb dual port or 100Gb Single or Dual port Adapter 100Gb Single port Omni path adaptor Also 1G x dual Port Should be Provided from Day 1
9	Interfaces	Serial - 1 Micro SD slot - 1 USB 3.0 support With Up to 4 total: 1 front, 1 internal, 2 rear
10	Bus Slots	Two PCI-Express 3.0 slots, at least one x16 PCIe slots
11	Power Supply	Should support hot plug redundant low halogen power supplies minimum 2 x 500 Watt
12	Fans	Redundant hot-plug system fans
13	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support Energy Star ASHRAE A3/A4 UEFI 2.6 SMBIOS Redfish API SNMP v3 TLS 1.2 DMTF Systems Management Architecture

Handwritten signature/initials

Handwritten signature/initials

S.No	Description of Requirements	
14	System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Support for Commercial National Security Algorithms (CNSA) Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 TPM (Trusted Platform Module) 2.0 Smart card (PIV/CAC) and Kerberos based 2-factor Authentication Configurable for PCI DSS compliance Chassis Intrusion detection
15	System tuning for performance	(i) System should support feature for improved workload throughput for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode "ON" without the frequency fluctuations associated with running in turbo mode. (ii) System should support workload Profiles for simple performance optimization
16	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.
17	Firmware security	(i) For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable. (ii) Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware

Handwritten signature/initials

Handwritten signature/initials

S.No	Description of Requirements	
4.	LOG CORRELATOR (SIEM)	
1	Chassis	1U Rack Mountable
2	CPU	2 x Intel Silver Processor 4124R
3	Memory	16 DIMM slots. 6x 32 GB
4	Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance
5	HDD Bays	Up to 8 HDD Bays. The drive carrier should have intuitive icon based display along with "DO NOT REMOVE" caution indicator that gets activated automatically in order to avoid data loss/downtime due to wrong drive removal.
6	Hard disk drive	2 x1.2 TB SAS 10K RPM
7	Controller	Hard Controller Should SUPPORT RAID 0.1 5.
8	Networking features	Server should support below networking cards: (a) 1Gb 4-port network adaptors (b) 10Gb 2-port Ethernet adaptor (c) 10GBaseT 4-port Ethernet adaptor (d) 4x25Gb Ethernet adaptor (e) 10/25Gb 2-port Ethernet adaptor (f) 100Gb Ethernet Options: Infiniband Options: 40Gb dual port or 100Gb Single or Dual port Adapter 100Gb Single port Omni path adaptor Also 1G x dual Port Should be Provided from Day 1
9	Interfaces	Serial - 1 Micro SD slot - 1 USB 3.0 support With Up to 4 total: 1 front, 1 internal, 2 rear
10	Bus Slots	Two PCI-Express 3.0 slots, at least one x16 PCIe slots
11	Power Supply	Should support hot plug redundant low halogen power supplies minimum 2 x 500 Watt
12	Fans	Redundant hot-plug system fans
13	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support Energy Star ASHRAE A3/A4 UEFI 2.6 SMBIOS Redfish API SNMP v3 TLS 1.2 DMTF Systems Management Architecture

A. M/s

B. Pml. H. it. D

S.N	Description of Requirements	
14	System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Support for Commercial National Security Algorithms (CNSA) Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 TPM (Trusted Platform Module) 2.0 Smart card (PIV/CAC) and Kerberos based 2-factor Authentication Configurable for PCI DSS compliance Chassis Intrusion detection
15	System tuning for performance	(a) System should support feature for improved workload throughput for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode "ON" without the frequency fluctuations associated with running in turbo mode. (b) System should support workload Profiles for simple performance optimization.
16	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.
17	Firmware security	(a) For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable. (b) Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware.

5. HYPER CONVERGENT INFRASTRUCTURE WITH VIRTUALIZATION LICENSE

S.No	Description of Requirements	
1	Make/Brand	HCI appliance OEM shall be in the Leaders category consecutively in last two published Gartner's Magic Quadrant (or equivalent) reports on "Hyper converged Infrastructure".
2	Hyper Converged Appliance	Hyper converged appliance, which comes Factory Installed with various software including Software Defined Storage and hypervisor. SDS should NOT be top-up or add-on software license bundled on generic x 86 servers. It should be an integral part of appliance.
3		Proposed HCI Appliance should be in all flash drive configurations using not more than 2TB capacity drives. Usable capacity per-node should be after all overheads in respect of core/memory/storage being used for deduplication, compression and optimization.
4		Solution must be able to integrate 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.
5		Nodes should offer Storage Features such as De-duplication and Compression. Replication / backup license(s) should be provided for the full capacity of the system. Storage performance monitoring software should be included. Future capacity growth shall not warrant any additional software license on the storage landscape.
6		Proposed hardware must be capable to de-duplicate, compress & optimize all data inline, in real-time with fine data granularity of minimum 8KB data blocks.
7		Solution should ensure minimum impact to production workloads and guaranteed CPU and RAM available to user applications while doing global deduce, compression and optimization.
8		The Hypervisors are to be installed in the nodes along with Cloud / Virtualization Management. The management node requirements, if any should be included by default and management node to be considered outside of the HCI nodes. All offered licenses for virtualization manager are to be of non-embedded type and should have no limitation of functionality.

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements	
9		HCI Solution should have minimum 2 types of data copies across Cluster available in the offered solution.
10		HCI appliance hardware OEM shall provide a single TAC support for underlying virtualization and virtualization manager.
11	Processor	Latest Generation Intel® Xeon Processors product family, >=2.00 GHz per Core. Populated with minimum 2 sockets per node.
12	Total Physical Cores	48 Cores (Per-Node)
13	Processor Cache	Min. 35 MB L3 Cache
14	Total Physical RAM	Min. 500GB DDR4. Scalability to double or more of provisioned RAM
15	Total Usable Storage	Min. 20 TB usable capacity post Reduplication and compression per node. The proposed solution must be able to sustain one node failure and it should in no way affect/degrade the production services & usable resources, to the end user application.
16	Network	Minimum 4 x 10/25/40Gb SFP28 (10G SR optics populated) Ethernet ports (each Node) and 2 x 1Gb RJ45 Ethernet ports (Additional ports to be configured by bidders as per their solution requirement). Additionally, Minimum 1' no 1Gb RJ45 Ethernet OOB dedicated management port.
17	Data Protection Features	Backup functionality as an integrated feature or separate server / software license to be offered.
18		Backup must be an independent copy of source Virtual Server and must allow restore of deleted or corrupted source Virtual Server.
19		Support for Replication across separate data centre with the ability to carry simultaneous out bi-directional replication between two data centres and with the ability to replicate Any-to-Any in a Mesh Data Centre deployment of more than 3 DC's.
20		The ability to define backup policy per data store, a group of VMs or specific VM.
21		Data Protection should have RPO of 10 minutes for local backups

Handwritten signature

Handwritten signature

S.No	Description of Requirements	
22		The ability to execute backup tasks during office hours without impacting to production workloads.
23		Data loss protection against single node failure in cluster.
24		The proposed solution must be able to provide backup reports for audit purpose.
25	Private Cloud License	Virtualisation license for the complete solution needs to be proposed with the HCI Appliance for this requirement.
26		Proposed solution must be able to support the following VM-Centricity and Mobility feature:-
27		i) Backups for specific VMs and Clone specific VMs.
28		ii) Ability to move specific VMs between data centres.
29		iii) VM-level backup instead of forcing protection at the data store or protection domain level.
30	Data Recovery Features	Data recovery should be independent of source Virtual Server.
31		Solution should provide a backup catalogue to allow any Virtual Server to be recovered to any specific point-in-time.
32		Data recovery process should be simple with an RTO in minutes.
33	Storage Controller in Nodes	SAS RAID controller with minimum 4GB cache for RAID 0, 1 and 5
34	Rack Unit	Minimum 2U or higher rack unit (RU) configuration Appliance with Sliding Rails
35	Redundancy & Business Continuity	Dedicated non-shared Redundant platinum rated AC power supplies on each of the proposed HCI appliance nodes and should be able to sustain single power supply failure per-node.
36		Solution should be able to sustain one node failure per cluster.
37		Solution should be able to sustain 1 NIC port failure per node.
38		During a single component failure of any type in any node, production services should not be affected or degraded in anyway.
39		Solution should be able to sustain multiple points of failure with no loss of functionalities or data.
40		Availability of Data Store with zero RPO for all VMs is to be ensured in the event up to 2 Node failures for the stretch clusters at D3 domain.

Handwritten signature/initials.

Handwritten signature/initials.

S.No	Description of Requirements	
41		In the event of a Hard drive failure, appliance should not be affected and virtual machines should continue to run on the appliance. Drive replacement should be seamless to virtual machines hosted on the appliance.
42		Solution should be able to sustain 2 SSD Disk failures per physical node, and 1 HDD failure simultaneously in each node of cluster across all nodes in cluster.
43	Disaster Recovery Features	The solution must provide a simple failover operation.
44		The solution must allow changing of IP address of recovered Virtual Servers to match target data centre.
45		The solution should allow changing Virtual Server settings (example vCPU, vRAM, vSwitch) if required.
46		The solution must allow the option to test DR failover to separate network with no impact to production workloads.
47		The solution should have feature to assist in failback process to Primary data centre.
48		Hyper converged solution should have a guaranteed local cluster backup time of 1 minute.
49		Data Protection should have a minimum RPO of 10 minutes for local backups.
50		Data recovery process should be simple with an RTO in minutes.
51		Manageability
52	Globally manage Backup Policies per Data store or per VM.	
53	VM-centric management through a single pane of glass via the virtualization manager or server OEM browser based software.	
54	Programmatic/API interface to enable automated tasks like failover/failback.	
55	System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder.	
56	Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.	
57	System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support	

Handwritten signature/initials

Handwritten signature/initials

S.No	Description of Requirements	
58	Scalability	Minimum scalability of 16 nodes in the same cluster.
59		Hyper-converged solution must be able to allow in-box upgrade of CPU, RAM and storage capacity as well as scale-out expansion
60		Hyper-converged solution should support addition of compute/access nodes to provide additional compute resources
61	Server Security	Should maintain repository for firmware and drivers recipes in the flash drive associated to management port. This is to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware
62		For firmware security, Hyper converged system should support remote management chip creating a fingerprint in the silicon, preventing system from booting up unless the firmware matches the fingerprint. This feature should be immutable
63		Directory services (AD/LDAP) compliance, CNSA compliance, HTML5 remote console, Workload Performance Advisor, Support for external key managers, Security Dashboard for assessment of important security features, the Overall Security Status for the system, and the current configuration for the Security State including Server Configuration Lock features
64	OS Support	Windows 2012, 2016 and latest Standard/Data Centre, SUSE Enterprise Linux, RHEL 6.x, (All latest flavours of Linux and Windows) in Virtual Machines
65	Serviceability	Proposed Nodes shall provide insights, forecasting and recommendations for quicker problem resolutions including automating case creation or alternate onsite solution on proactive support services with proactive parts dispatch directly from OEM.
66	Warranty	On-site Comprehensive Warranty and Service including all spares, and service offering with NBD on-site for parts as well as telephone support 24 hours.

→ M₁₂

⊕ On-site W₂₄

S.N	Description of Requirements
Following devices should provide with the system (Number will be decided by the user organization)	
1	Architecture (a) Shall be 19" Rack Mountable (b) The switch should have dual hot-swappable power supplies (c) Switch shall have minimum 24 x 1/10G SFP+ ports, populated with 8x10G SR, 8x1G SX and 8x1G BaseT transceiver.
	(d) 1 RJ-45 serial console port (e) 1 RJ-45 out-of-band management port (f) Should have minimum 2GB SDRAM and 512 MB flash and 32 MB or higher packet buffer size (g) Shall have switching capacity of minimum 480 Gbps (h) Shall have up to 350 million pps switching throughput (j) The Switch should support minimum 64000 MAC address.
2	Software Defined Networking (SDN) Capability (a) Open Flow protocol capability to enable software-defined networking
3	Features (a) The switch should support HTTP redirect function (b) 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
4	Quality of Service (QoS) (a) 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 (b) The switch should support Layer 4 prioritization to enable prioritization based on TCP/UDP port numbers (c) 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 (d) The switch should support Port-based rate limiting to provide per-port ingress-/egress-enforced increased bandwidth. (e) 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. (f) The switch should support Reduced bandwidth to provide per-port, per-queue egress-based reduced bandwidth.

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements
	<p>(g) 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.</p> <p>(h) The switch should support Remote monitoring (RMON), Extended RMON (XRMON), and Flow v5 to provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events.</p> <p>(j) The switch should support Traffic prioritization allows real-time traffic classification into eight priority levels that will mapped to eight queues.</p>
5	<p>Management</p> <p>(a) The switch should allow assignment of descriptive names to ports.</p> <p>(b) The switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP).</p> <p>(c) 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.</p> <p>(d) The switch should support Multiple configuration files to store easily to the flash image.</p> <p>(e) The switch should support Dual flash images to provide independent primary and secondary operating system files for backup while upgrading.</p> <p>(f) 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.</p> <p>(g) The switch should support Unidirectional Link Detection (UDLD).</p>
6	<p>Connectivity</p> <p>(a) The switch should support Jumbo frames on Gigabit Ethernet and 10-Gigabit Ethernet ports</p> <p>(i) The switch should support following IPv6 feature</p> <p>(a) IPv6 host: enables switch management in an IPv6 network.</p> <p>(b) Dual stack (IPv4 and IPv6): transition IPv4 to IPv6, supporting connectivity for both protocols.</p> <p>(c) MLD snooping: forward IPv6 multicast traffic to the appropriate interface.</p> <p>(d) IPv6 ACL/QoS: support ACL and QoS for IPv6 traffic.</p> <p>(e) IPv6 routing: support static, RIPng, OSPFv3 routing protocols.</p> <p>(f) 6in4 tunneling: support encapsulation of IPv6 traffic in IPv4 packets.</p> <p>(g) Security: provide RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping.</p>

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements
7	<u>Performance</u>
	<p>(a) 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</p> <p>(b) The switch should support Energy-efficient Ethernet (EEE) support: reduces power consumption in accordance with IEEE 802.3az</p>
8	<u>Resiliency and high Availability</u>
	(a) The Switch should support 9 Switch or ore stacking and support up to 336 Gb/s of stacking throughput. The Switch support Ring, chain, and mesh stacking topologies. Stacking required from day-1.
	(b) The Switch should support Virtualized switching to provide simplified management as the switches appear as a single chassis when stacked.
	(c) The switch should support Virtual Router Redundancy Protocol (VRRP).
	(d) The switch should support Nonstop switching and routing.
	(e) 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.
	(f) The switch should support IEEE 802.1s Multiple Spanning Tree.
	(g) 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.
(h) The switch should provide easy-to-configure link redundancy of active and standby links.	
9	<u>Layer 2 switching</u>
	(a) The switch should support IEEE 802.1ad QinQ
	(b) The switch should support VLAN and tagging and support the IEEE 802.1Q standard and 4096 VLANs simultaneously.
	(c) The switch should support IEEE 802.1v protocol VLANs.
	(d) The switch should support MAC-based VLAN.
	(e) The switch should support Rapid Per-VLAN Spanning Tree (RPVST+)
	(f) The Switch should dynamically load balances across multiple active redundant links to increase available aggregate bandwidth and allow concurrent Layer 3 routing
(g) The switch should support GVRP and MVRP	

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements
10	<p>Layer 3 Services</p> <p>(a) The switch should support Loopback interface address.</p> <p>(b) The switch should support Route maps.</p> <p>(c) The switch should support User datagram protocol (UDP) helper function.</p> <p>(d) The switch should support DHCP server.</p> <p>(e) The switch should support Bidirectional Forwarding Detection (BFD) to enable link connectivity monitoring and reduces network convergence time for static routing, OSPFv2, and VRRP.</p>
11	<p>Layer 3 routing - Should support from Day-1</p> <p>(a) The switch should support Static IP routing for both IPv4 and IPv6 networks</p> <p>(b) The switch should support OSPFv2 for IPv4 routing and OSPFv3 for IPv6 routing</p> <p>(c) The switch should support Policy-based routing</p> <p>(d) The switch should support Border Gateway Protocol (BGP)</p> <p>(e) The switch should support RIPv1, RIPv2, and RIPv3 routing</p>
12	<p>Security</p> <p>(a) The switch should support Source-port filtering.</p> <p>(b) The switch should support RADIUS/TACACS+</p> <p>(c) The switch should support Secure shell.</p> <p>(d) The switch should support Secure Sockets Layer (SSL).</p> <p>(e) The switch should support Port security.</p> <p>(f) The switch should support MAC address lockout.</p> <p>(g) The switch should support Detection of malicious attacks.</p> <p>(h) The switch should support Secure FTP.</p> <p>(j) The switch should support Switch management logon security.</p> <p>(k) 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</p> <p>(l) The switch should support ICMP throttling.</p> <p>(m) The switch should support Identity-driven ACL.</p> <p>(n) The switch should support STP BPDU port protection.</p> <p>(o) The switch should support Dynamic IP lockdown.</p> <p>(p) The switch should support DHCP protection.</p> <p>(q) The switch should support Dynamic ARP protection.</p> <p>r) The switch should support STP root guard.</p> <p>(s) The Switch should secure management interfaces such as SNMP, Telnet, SSH, SSL, Web, and USB at the desired level.</p> <p>(t) The Switch should display a customized security policy when users log in to the switch.</p> <p>(u) The switch should support CPU protection.</p>

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements	
	(v) 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. (w) The switch should support IEEE 802.1X (x) The switch should support Web-based authentication. (y) The switch should support MAC-based authentication. (z) Authenticates client with the RADIUS server based on client's MAC address. (aa) The switch should support Concurrent authentication modes to enables a switch port to accept up to 32 sessions of 802.1X, Web and MAC authentication. (ab) The switch should support Private VLAN.	
13	Convergence (a) The switch should support IP multicast snooping (data-driven IGMP). (b) The switch should support LLDP-MED (Media Endpoint Discovery). (c) The switch should support IP multicast routing including PIM sparse and dense modes to route IP multicast traffic. (d) The switch should support Auto VLAN configuration for voice. (e) The switch should support RADIUS VLAN. (f) 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 (a) Shall support IEEE 802.3az Energy-efficient Ethernet (EEE) to reduce power consumption. (b) Operating temperature of 0°C to 45°C (c) Safety and Emission standards including EN 60950; IEC 60950; VCCI Class A; FCC Class A	
15	Warranty and Support (a) The below Warranty shall be offered directly from the switch OEM. (b) Software upgrades/updates shall be included as part of the warranty. Following devices should provide with the system (Number will be decided by the user organization)	
1	Chassis	1U Rack Mountable
2	CPU	2 x Intel Bronze Processor 3204
3	Memory	16 DIMM slots. 2x 32 GB
4	Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance

Handwritten signature/initials: *Mm*

Handwritten signature/initials: *Amal*

S.N	Description of Requirements	
5	HDD Bays	Up to 8 HDD Bays The drive carrier should have intuitive icon based display along with "DO NOT REMOVE" caution indicator that gets activated automatically in order to avoid data loss/downtime due to wrong drive removal.
6	Hard disk drive	2 x1.2 TB SAS 10K RPM
7	Controller	Hard Controller Should SUPPORT RAID 0.1 5.
8	Networking features	Server should support below networking cards: 1. 1Gb 4-port network adaptors 2. 10Gb 2-port Ethernet adaptor 3. 10GBaseT 4-port Ethernet adaptor 4. 4x25Gb Ethernet adaptor 5. 10/25Gb 2-port Ethernt adaptor 6. 100Gb Ethernet Infiniband Options: 40Gb dual port or 100Gb Single or Dual port Adapter 100Gb Single port Omni path adaptor Also 1G x dual Port Should be Provided from Day 1
9	Interfaces	Serial – 1, Micro SD slot – 1, USB 3.0 support With Up to 4 total: 1 front, 1 internal, 2 rear
10	Bus Slots	Two PCI-Express 3.0 slots, at least one x16 PCIe slots
11	Power Supply	Should support hot plug redundant low halogen power supplies minimum 2 x 500 Watt
12	Fans	Redundant hot-plug system fans
13	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support Energy Star ASHRAE A3/A4 UEFI 2.6 SMBIOS Redfish API SNMP v3 TLS 1.2 DMTF Systems Management Architecture
14	System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Support for Commercial National Security Algorithms (CNSA) Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Tamper free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 TPM (Trusted Platform Module) 2.0 Smart card (PIV/CAC) and Kerberos based 2-factor Authentication Configurable for PCI DSS compliance Chassis Intrusion detection.

Handwritten signature

95 *Handwritten signature* 29

S.N	Description of Requirements	
15	System tuning for performance	<p>1. System should support feature for improved workload throughput for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode "ON" without the frequency fluctuations associated with running in turbo mode.</p> <p>2. System should support workload Profiles for simple performance optimization</p>
16	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.
17	Firmware security	<p>1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable.</p> <p>2. Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware</p>

6. NETWORK TRAFFIC MANAGER

BANDWIDTH CONTROLLER		
An additional device for bandwidth control should be provided along with the system. The features are as follows.		
1	General Features	(i) The system should ensure reliable performance for network dependent applications.
		(ii) The system should reduce the impact of non-strategic traffic, and diagnose and resolve network problems
		(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.
		(iv) The system should have the feature to easily monitor recreational traffic like video streaming and P2P sharing.
	Technical Features	<p>(i) Real-time Monitoring: 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</p>

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements
	<p>(ii) Policy-Based Shaping: The system should have the feature to prioritize how and when users, applications and websites can consume bandwidth on network.</p> <p>(iii) Interactive Analytics: Intuitive dashboard feature should be there to visualize activities by all users.</p> <p>(iv) Application Acceleration: The system should support acceleration and caching features.</p> <p>(v) Predictive Recommendations: 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.</p> <p>(vi) QX Boost for Skype Application: 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.</p>
<p>Hardware Features</p>	<p>(i) Traffic shaping and Acceleration</p> <p>(a) Shaping Throughput: - 1 Gbps</p> <p>(b) Concurrent Flows: - 220,000</p> <p>(c) Packets per second: - 200,000/s</p> <p>(d) New Connection Rates: - 10,000/s</p> <p>(e) Acceleration Throughput: - 30 Mbps</p> <p>(f) Edge Cache Throughput: - 50 Mbps</p> <p>(g) Optimized Connections: - 6,000</p> <p>(h) APS Objects 250</p> <p>(i) SLA Objects 250</p> <p>(j) PDF Reports 60</p> <p>(k) Traffic Policies 1024</p> <p>(ii) Interface Capability</p> <p>(a) The system should have 1 x RJ45 based dedicated console port for management purpose.</p> <p>(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.</p> <p>(iii) Physical Parameters</p> <p>(a) Form Factor: -1U rack mountable</p> <p>(b) Power Rating: - 17W @ 0.13A, 22W @ 0.16A (Max)</p> <p>(c) Environment: - 0 deg cel to 40 deg cel, 5% to 90% operating humidity.</p>



S.N	Description of Requirements	
Following devices should provide with the system (Number will be decided by the user organization)		
	Speech band	300 to 3400 Hz
	Modulation	Pulse Code Modulation
	No. of channels per system	32 (30 speech channels, 1 terminal Signaling and 1 Sync. Channel)
	Sampling frequency	8000 Hz
	No of sample bits	8 per channel
	Total bits per	256
	Bit rate	2048 Kbps \pm 50 ppm
	Construction and Architecture	Chassis based modular multiplexer shelf capable of supporting minimum 12 slots for integration of data, voice, fax and LAN traffic.
	Universal Slots	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.
	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
	Redundancy	Dual controller, dual power with load sharing
	Protection	1 for 1 protection , E1, T1, FOM PDH ring protection, QE1, QT1, FOM, Mini QE1, 3E1 for DS0 SNCP protection

Mr

of one to

2

S.N	Description of Requirements	
	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/24FXS
		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	

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements	
	2* 10/100 Ethernet Router Card with capability to handle 64 WANs should comply with the following specifications	
Number of ports	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)	
Physical Interface	10/100 BaseT x 2	
Connector	RJ45	
Routing protocol	RIP-I, RIP-II, OSPF, Static	
Supporting Protocols	PPP (IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT, DHCP	
Diagnostic	Ping, Trace route	
QoS	Rate limit	
	8* 10/100 Ethernet Router Card with capability to handle 64 WANs	
Number of ports	8 LAN ports, Max. 64 WAN ports. Each WAN port has data rate n x 64K bps.	
Physical Interface	10/100 BaseT x 8	
Connector	RJ45	
Routing protocol	RIP-I, RIP-II, OSPF, Static	
Supporting Protocols	PPP (IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT, DHCP	
Diagnostic	Ping, Trace route	
QoS	Rate limit	
	Voice Card (8EM) port (interfaces) should comply with the following specifications:-	
	<ul style="list-style-type: none"> a) Connector: RJ45 connector (b) Alarm conditioning: CGA busy after 2.5 seconds of LOS ,LOF (c) Encoding: a low or u low user selectable together for all. (d) Impedance: balanced 600 or 900 ohms. (e) Longitudinal rejection : 55 dB (f) Loss adjustment : -21 to +10 dB/0.1dB step transmit and receive (g) Single/ distortion: >46 dB with 1004 Hz, 0 dBm input (h) Frequency response: -0.25 to-1 dB from 300 to 3400Hz (j) Signaling : Type 1,Type 2,Type 3,Type 4,Type 5 transmit only 	

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements	
	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 / 0.1dB step transmit & receive (j) Signal/ Distortion : > 25dB with 1004 Hz, 0dBm input (k) Frequency Response : - 0.25 to -1 dB from 300 to 3400 Hz, coincide with ITU-T G.712 (l) Loss adjustment: -21 to +10 dB/ 0.1 dB step transmit and receive (m) Signal / Distortion:.. 46 dB with 1004 Hz , 0dBm input (n) Frequency response: - 0 .25 to -1 dB from 300 to 3400 Hz , coincide with ITU-T. o) Ideal channel noise : Max -65 dB Mop (p) Inter- modulation : coincide with ITU-T B.712 (q) 2Wire return loss : > 2 dB echo , > 20 dB signing (r) FXS loop feed : Nominal -48 V dc with 20 mA current limit (s) Signaling : Loop Start, DTMF, pulse, PLAR, Battery Reverse	
	G.SHDSL Line port (interfaces) should comply with the following specifications:-	
	Number of ports	2 or 4
	Line Rate for 4-channel G.shdsl	n x 64Kbps (n= 3 to 31)
	Line Rate for 2-channel G.shdsl	n x 64Kbps (n= 3 to 15)
	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

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements	
TDM over Ethernet Card		
Combo Gigabit Ethernet (GbE) Interface	-> Number of Ports 2 -> Speed 10/100/1000M bps -> Connector RJ45 for twisted pair GbE, LC for optical GbE, auto detection	
Gigabit Ethernet (GbE) Interface	-> Number of Port 2 -> Speed 10/100/1000 BaseT -> Connector RJ45	
Ethernet Function	MDI/MDIX for 10/100/1000M BaseT auto-sensing Ping function contained ARP Per port, programmable MAC hardware address learn limiting (max. MAC table 8192 (8k) entry)	
Basic Features:		
Packet Transparency	Packet transparency support for all types of packet types including IEEE 802.1q VLAN and 802.1ad (Q-in-Q)	
QoS	User configurable 802.1p CoS, ToS in outgoing IP frame.	
Traffic Control	(a) Ingress packet Rate limiting buckets per port for Ethernet port (b) Supporting Rate-based and Priority-based rate limiting for LAN port. (c) Pause frame issued when the traffic exceeding the limited rate before packet dropped following IEEE802.3X	
Link Aggregation	WAN support link aggregation	
Jitter & Wander	PPM: per G.823 Traffic PPB: per G.823 Synchronous*	
Standard Compliance		
IETF	TDMoIP (RFC5087), SAToP (RFC4553), CESoPSN (RFC5086)	
IEEE	802.1q, 802.1p, 802.1d, 802.3, 802.3u, 802.3x, 802.3z, 802.1s, 802.1w, 802.1AX	
Co-directional port (interfaces) should comply with the following specifications :-		
Interface	ITU G.703 64 Kbps co-directional interface	
Connector	120ohm, RJ48	
Line Distance	Up to 500 meters	
Loopback	DTE Payload Loopback, Local Loopback	

Handwritten signature/initials

Handwritten signature/initials

S. N	Description of Requirements	
Voice Card 12 MAG (Magneto)		
	(a) Connector : Twelve RJ11 (b) Alarm Conditioning CGA busy after 2.5 seconds of LOS, LOF. (a) Encoding A-law or μ -law, user selectable together for all. (b) Impedance Balanced 600 or magneto telephone impedance match. (c) Longitudinal Conversion Loss > 46dB. (d) Gain Adjustment -21 to +10 dB / 0.1dB step transmit & receive. (e) Signal/ Distortion > 25dB with 1004 Hz, 0dBm input. (f) Frequency Response - 0.25 to -1 dB from 300 to 3400 Hz, coincide with ITU-T G.712. (g) Idle Channel Noise Max. -65 dBm0p. (h) Min Detectable Ringing Voltage 16 Vrms. (i) Ringing Detectable Across L1 and L2 (Tip and Ring), L1 and GND (Tip and GND) (j) Single Ring Type: ring for 2 sec. and stop, or ring for 4 sec. and stop. (k) Continuous Ring Type: 1 sec on 2 sec off, or 2 sec on 4 sec off (l) Ringing Send across L1 and L2 (Tip and Ring), L1 and GND (Tip and GND). (m) Signaling Magneto MRD (Ringing across Tip and Ring or Tip and Ground). (n) Signaling Bit A, B, C, D Programmable. (o) Signaling is carried transparently by the digitizing process.	
C	Clock Source	Internal, E1/T1 Line, External
D	Alarm Relay	Alarm Relay: max. Voltage 3 Vdc/ max. current: 1A Fuse alarm, and performance alarm
E	System Configuration Parameters	Active Configuration, Stored Configuration, and Default Configuration
F	Supervisor	
	RS232 Console Port (VT100)	10 Base-T, Ethernet, SNMP In-band 64Kbps supports HDLC/PPP, SSH
G	Performance Monitor	
	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 & time

S.N	Description of Requirements	
	Threshold	Bursty Seconds, Severely Errored Second, Degraded Minutes
H	Diagnostics	
	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
J	Front Panel	
	LED	1 per V.35-interface, ACO, Power, SYNC/TEST, LOF, BPV, RAI/AIS
K	Physical /Electrical	
	Dimensions	432.4 x 220 x 223.5 mm (W×H×D)
	Power	Single/ Dual -48 Vdc: -36 to -75 Vdc, 100 Watts max.
		Single/ Dual -48 Vdc: -36 to -75 Vdc, 150 Watts max.
		Single/ Dual -24 Vdc: -18 to -36 Vdc, 150 Watts max
	Temperature	0°C -55°C
	Humidity	0-95%RH (non-condensing)
	Mounting	Desk-top stackable, 19" /23" rack mountable
	Line Power supply	Available only with DC power for G.SHDSL card only
	Power Consumption	Max 110 Watts
	The OEM should have authorized R & D & Repair/Replacement center in India with presence in India of about 10 Years	
L	Certification	EN55022 Class A, EN50024, FCC Part 15 ,Class A, FCC Part 68, CS-03, IEC60950, UL60950, IEC 61850-3, IEEE 1613
M	Compliance	ITU G.703, G.704, G.706, G.732, G.736, G.823, G.826, G.711, G.712, G.775, O.151, V.11, V.28, V.54
N	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
O	DC Power Source (-48V)	(a) Input 230 VAC (Range 170-264 VAC, single phase, 50 Hz).
		(b) Output Current :- 8 Amp
		(c) Size: - 485(W) x385(D) x165(H) mm with screw terminals at front
		(d) Should have short circuit protection.

Handwritten signature/initials: *Aw Mr*

Handwritten signature/initials: *One A. J. J.*

7. 24" MONITOR

S.No	Description of Requirements
1.	Screen Size: 24 inch Full HD (1920 X 1080) IPS Panel
2.	Connectivity Port: 1 VGA Port, 1 HDMI Port
3.	Aspect Ratio: 16:9, Brightness (Typical): 250 cd/m ²
4.	Number of Colour: 16.7 m Colours
5.	Refresh Rate: 60 Hz (Analog),
6.	Response Time: 4 ms
7.	Viewing Angle: 178-degree horizontal 178-degree vertical

8. KEYBOARD & MOUSE

S.No	Description of Requirements
1.	104 Keys USB keyboard
2.	2 Button USB Optical Scroll Mouse
3.	The Keyboard and Mouse should be from the same OEM.

INTRUSION & FIREWALL

1. UNIFIED THREAD MANAGEMENT

S.No	Description of Requirements
General Requirements	
1	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.
2	The proposed vendor must have successfully completed NSS Labs' NGFW Methodology v8.0 testing with a minimum exploit blocking rate of 99%
3	OEM should be in Leaders quadrant of Gartner's - in Enterprise Firewall Magic Quadrant (or equivalent) as per the latest report
4	Appliance shall be EAL4 and ICSA certified for Firewall
Hardware & Interface requirements	
1	The platform must be supplied with minimum 10 x GE RJ45 inbuilt interfaces & 4 x GE SFP interface slots from day one.
2	The Appliance should have USB & Console Ports.
Performance and Availability	
1	The Firewall should be on multiprocessor architecture with minimum 5Gbps (or more as per user requirement) of Firewall throughput & support of 1,500,000 concurrent sessions, and 130,000 new sessions per second from day one & latency should not be more than 3 μs

Handwritten signature/initials

Handwritten signature/initials

S.No	Description of Requirements
2	Minimum IPS throughput of 2000 Mbps for real world traffic or enterprise mix traffic
3	Minimum SSL Inspection Throughput of 500 Mbps
4	Minimum Threat Prevention Throughput (measured with Application Control and IPS and Anti-Malware enabled) of 1000 Mbps for real world traffic or enterprise mix traffic.
5	IPSec VPN throughput: minimum 5 Gbps
6	Simultaneous Client-to-Site IPSec VPN tunnels: 300
7	Proposed solution must support minimum 300 SSL VPN users from day one
8	Proposed solution must support minimum 10 virtual firewall from day one
	<u>Routing Protocols</u>
1	Static Routing
2	Policy Based Routing
3	The Firewall should support dynamic routing protocol like RIP, OSPF, BGP, ISIS
	<u>Firewall Features</u>
1	Firewall should provide application inspection for LDAP, SIP, H.323, SNMP, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, IMAP, NFS etc.
2	IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP
3	Allows secure deployment of next-generation IPv6 networks, as well as hybrid environments that require simultaneous, dual stack support of IPv4 and IPv6
4	The firewall should support transparent (Layer 2) firewall or routed (Layer 3) firewall Operation
5	The Firewall should support ISP link load balancing for outbound traffic & also should support SDWAN functionality for future scalability
6	Firewall should support link aggregation functionality to group multiple ports as single port.
7	Firewall should support minimum VLANS 2048
8	Firewall should support static NAT, policy based NAT and PAT
9	Firewall should support IPSec data encryption
10	It should support the IPSec VPN for both site-site and remote access VPN
11	Firewall should support IPSec NAT traversal.
12	control SNMP access through the use of SNMP and MD5 authentication.
13	Firewall system should support virtual tunnel interfaces to provision route-based IPSec VPN

Handwritten signature/initials

Handwritten signature/initials

S.No	Description of Requirements
14	The Firewall should have integrated solution for SSL VPN & both IPSec & SSL VPN functionality should be ICSA certified
15	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
16	The solution should have basic server load balancing functionality as an inbuilt feature
<u>Integrated IPS Features Set</u>	
1	IPS should have DDoS and DoS anomaly detection and protection mechanism with threshold configuration.
2	Support SYN detection and protection for both targets and IPS devices.
3	The device shall allow administrators to create Custom IPS signatures
4	Should have a built-in Signature and Anomaly based IPS engine on the same unit
5	Signature based detection using real time updated database & should have minimum 10000+ IPS signature database from day one
6	Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)
7	Signature updates do not require reboot of the unit.
8	Configurable IPS filters to selectively implement signatures based on severity, target (client/server) and operating systems
9	IPS Actions: Default, monitor, block, reset, or quarantine
10	Should support packet capture option
11	IP(s) exemption from specified IPS signatures
12	IPS should be ICSA Certified & should be recommended by NSS Labs
<u>Anti Virus & Anti Bot</u>	
1	Firewall should support antimalware capabilities , including antivirus, botnet traffic filter and antispysware
2	Solution should be able to detect and prevent unique communication patterns used by BOTs i.e. information about botnet family
3	Solution should be able to block traffic between infected host and remote operator and not to legitimate destination
4	Should have antivirus protection for protocols like HTTP, HTTPS, IMAPS, POP3S, SMTPS protocols etc.
5	Solution should have an option of packet capture for further analysis of the incident
6	Solution should uncover threats hidden in SSL links and communications

Handwritten signature

Handwritten signature

S.No	Description of Requirements
7	The AV should scan files that are passing on CIFS protocol
8	The proposed system shall provide ability to allow, block attachments or downloads according to file extensions and/or file types
9	The proposed system should provide cloud based sandboxing solution from day one to prevent from zero day threats
10	The gateway Anti-Virus functionality should be ICSA certified
	<u>Other support</u>
1	Should support features like Web-Filtering, Application-Control & Gateway level DLP from day one
2	The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should support over 2 billion WebPages in 72+ categories and 68+ languages without external solution, devices or hardware modules.
3	Should support detection over 4,000+ 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)
4	The solution should have the flexibility to write security policies based on IP Address & User Name & Endpoint Operating System
5	The product must supports Layer-7 based Firewall virtualization, and all Firewall features should be supported in each virtual firewall like Threat Prevention, IPS, Web filter, Application Control, content filtering etc.
6	QoS features like traffic prioritization, differentiated services,. Should support for QoS features for defining the QoS policies.
7	It should support the VOIP traffic filtering
8	Appliance should have identity awareness capabilities
9	The firewall must support Active-Active as well as Active-Passive redundancy.
10	Solution must support VRRP clustering protocol.
	<u>Management & Reporting functionality</u>
1	Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI.
2	Support accessible through variety of methods, including console port, Telnet, and SSHv2
3	Support for both SNMPv2 and SNMPv2c, providing in-depth visibility into the status of appliances.
4	Should have capability to import configuration and software files for rapid provisioning and deployment using Trivial File Transfer Protocol (TFTP), HTTP, HTTPS

Handwritten signature/initials

Handwritten signature/initials

S.No	Description of Requirements
5	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
6	The Firewall appliance should have minimum 450GB of internal storage for logging & reporting functionalities
7	Solution must allow administrator to choose to login in read only or read-write mode

2. FIREWALL LOG ANALYZER

S.N	Description of Requirements
1	The solution should have a separate appliance for storing logs & generating reports centrally for all connected Firewalls of the same OEM & should have minimum capacity of connecting 30 Firewalls
2	The proposed centralized logging & reporting solution should have a capacity of accepting minimum 200GB logs per day & a total storage capacity of 12TB.
3	The solution should have support for RAID 0/1/5/10
4	The reporting solution should have customizable interactive dashboard to rapidly pinpoint problems
5	It should support drill-down to follow the trail of an attacker, trace transactions and gain new insights
6	It should have minimum 25+ built-in templates with sample reports ready for use
7	The solution should support to run report on-demand or on a schedule with automated email notification and Calendar view
8	It should support customization with 300+ built-in charts ready for generating custom reports
9	The solution should provide flexible report formats like HTML/CSV/XML/PDF
10	It should support retrieving of archived logs to perform analytics against historic data
11	The solution should support forwarding of logs to a Syslog server or a CEF log server for long-term storage, forensics or regulatory compliance

Handwritten signature/initials

Handwritten signature/initials

3. FIREWALL POLICY MANAGER

S.N	Description of Requirements
1	The solution should have a centralized management appliance for managing minimum 30 Firewall appliances of the same OEM from a single console
2	The management solution can collectively configure the device settings, objects and policies across the network from a single user interface
3	The management solution can review, approve and audit policy changes from a central place
4	It should support automated process to facilitate policy compliance and policy lifecycle management
5	Should support enforcing workflow to reduce risk for policy changes
6	The centralized management solution should support for: Application Control and Intrusion Prevention updates, Vulnerability Management, Antivirus and Web Filtering updates to all the connected Firewall appliances from a single console
7	It should support for RESTful API which allows to create customized, branded web portals for policy and object administration
8	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
9	The solution should support ensuring common security baseline to be enforced and shared among multiple administrative domains (ADOMs).

C. CYBER FORENSIC

1. Data Analysis Tool

S.N	Description of Requirements
1.	Ability to automatically queue multiple acquisition and processing actions – to increase efficiencies and save time.
2.	End-to-end experience that brings together acquisition, processing and analysis, creating integration and a more navigable and manageable digital evidence database.
3.	Support for a broad array of artifact types, and support for the latest versions of those apps and artifact types.
4.	Access to file system, registry and artifacts data and trace artifact evidence to its source data efficiently for a better verification process.
5.	The ability to present findings in a customizable way that fits their report needs and parameters.

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements
6.	Acquire images from any iOS or Android device, hard drives, and removable media.
7.	Recovers evidence from 300+ types of Internet Artifacts from Windows and Mac computers.
8.	Recovers 165+ types of Smartphone Artifacts from iOS, Android, and Windows Phone powered smart phones and tablets.
9.	Get to relevant evidence faster using filters. Isolate evidence from a specific date or time range, or create filters to narrow results based on field values for any supported artifact type. Filter stacking allows you to layer on several dimensions of filter criteria to pinpoint specific items in a large dataset.
10.	Create and manage a number of different tags to help you narrow down the results quickly and begin to see patterns in an individual's activity. Using the comments function, identify and share your thoughts with other key stakeholders. You can also create profiles that are associated with an individual and then associate other identifiers (email addresses, phone numbers, etc) with the profile, so that you can filter evidence to show only the evidence associated with the individual.
11.	Create your own custom artifact definitions to find more artifact data or have Evidence Analyzer's Dynamic App Finder automatically identify new apps and create artifact definitions which can then be saved for future use.
12.	Recovers more artifacts from both allocated and unallocated space by extracting data from full files or carving for deleted data and traces of data elements/fragments left behind by apps and websites, presenting it in an organized and easy to read format.
13.	Add hash sets to either filter out non-relevant files to enhance search performance and reduce false positives or add hash sets that will specifically call out and identify known bad pictures and videos.
14.	Efficiently analyze large volumes of data
15.	Explore file systems and registry hives for greater insights
16.	Process and recover 500+ types of artifacts
17.	Automate all acquisition and processing tasks required to prepare evidence for analysis.
18.	Explore file systems and registry hives for greater insights
19.	Trace artifact evidence back to its source data in seconds
20.	Trace artifact evidence back to its source data in seconds.
21.	built on the analysis capabilities allowing you to recover hundreds of types of digital forensic artifacts
22.	Should be able able to extract data from cloud data source using Tokens from evidence
23.	Easy-to-use interface that moves you through your investigation.

Handwritten signature/initials

Handwritten signature/initials

S.No	Description of Requirements
2	EVIDENCE SEIZURE KIT
1	Multipurpose, Portable Unit That Contains A Complete Array Of Hardware/ Software Solutions To Preview, Acquire Or Process Digital Evidence.
2	Kit Should Contain High End Forensic Laptop With The Following Minimum Configuration
	(a) Intel Core i7-6700K Skylake Quad Core Processor or higher or equivalent, 4.0 GHz, 8MB Intel Smart Cache or higher
	(b) 32 GB PC4-17000 DDR4 2133 Memory
	(c) 256 GB Solid State Internal SATA Drive or higher
	(d) Intel Z170 Express Chipset Or equivalent or higher
	(e) 15.6" Full HD (1920x1080) IPS Display with G-Sync Technology, Matte Finish
	(f) NVIDIA GeForce GTX 1060 with 6 GB GDDR5 VRAM
	(g) 1 RJ-45 LAN (10/100/1000Mbps)
	(h) Intel Dual Band Wireless-AC 8260 - 802.11ac, Dual Band, 2x2 Wi-Fi + Bluetooth 4.2
	(j) Card Reader 6-in-1 (MMC/RSMHC/SD/Mini-SD/SDHC/SDXC up to UHS-II)
	(k) 2.0 Megapixel FHD Video Camera
	(l) High Definition Audio
	(m) Microphone
	(n) Speakers (2)
	(o) 19mm Full-Size Keyboard with numeric keypad – Illuminated
	(p) Touch Pad pointing device(2 buttons)with multi-gesture and scrolling function
	(q) Finger Print Reader
	(r) 1 HDMI Port
	(s) 2 Mini Display Port 1.3 ports
	(t) 1 Thunderbolt 3 / USB 3.1 Gen 2 Combo Port (Type C)
	(u) 1 USB 3.1 Gen 2 Port (Type C)
	(v) 3 USB 3.0 ports
	(w) 1 USB 2.0 Port
	(x) 1 Headphone jack (2-in-1 Head phone/ S/PDIF Optical)
	(y) 1 Microphone jack
	(z) 1 Line-In jack
	(aa) 1 Line-out jack
	(ab) 8 Cell Smart Lithium -Ion, 82WH Battery Pack
	(ac) Kensington Lock Slot
	(ad) Universal AC Adapter (100~240V AC 50/60hz)
	(ae) Dimensions: 15.20 x 10.32 x 1.41 (inch)
	(af) Weight: 7.5 lbs (complete system + battery)
	(ag) Windows 10 Professional (64 bit)/ Other Operating Systems included: SUSE Professional Linux (64 bit)
	(ah) System Restore Media - Bootable Blu-ray disc containing restore environment and factory configured operating system images

Handwritten initials: *AV* and *MV*

Handwritten initials: *Q*, *Qul*, *A. J. d*, and page number **46**

S.No	Description of Requirements
3	<p>KIT SHOULD CONTAIN PORTABLE FORENSIC WRITE BLOCKER WITH THE FOLLOWING INTERFACE</p> <p>(a) USB 3.0 - IDE/SATA, SAS, USB 3.0, Firewire, USB 3.0 Forensic Card Reader and Writer has been designed specifically for forensic use and incorporates Super Speed USB3 (5Gb/s) technology.</p> <p>(b) Universal Power Supply and Power Adapter cables, Standard Cables and Adapters</p>
4	<p>KIT SHOULD CONTAIN LATEST FORENSIC DUPLICATOR WITH FOLLOWING CONFIGURATION</p> <p>(a) Should have a Forensic Duplicator with capabilities to support Greater than 2TB HARD DRIVES</p> <p>(i) Image a 2TB HDD (2000GB)</p> <p>(ii) Clone HDDs with no size limit</p> <p>(b) Forensically duplicates HDD's faster than ever - up to 15 GB/min with hashing</p> <p>(c) Standard features include Disk-to-Disk (clone) and Disk-to-File (image) duplication, Format, Wipe, Hash (MD5 or SHA-1), HPA / DCO detection and removal, and Blank Disk Check.</p> <p>(d) Make one (1:1), two (1:2), or three (1:3) copies of evidence drives.</p> <p>(e) Acquisitions of USB 3.0, SATA, and IDE/PATA devices can be directed to either USB 3.0 or SATA output devices.</p> <p>(f) Option to acquire SAS drives with additional modules</p> <p>(g) Outputs to raw DD, .e01 (compressed), .ex01 (compressed), or .dmg formats</p> <p>(h) USB 3.0 convenience and speed built in</p> <p>(j) Extensive log files is easy to view and save</p> <p>(k) Built-in, user-selectable MD5 and SHA256 verification</p> <p>(l) Hash re-verification on read from destination(s) - user-selectable</p> <p>(m) Colour LCD user interface</p>
5	<p>EXTERNAL DEVICES AND ENCLOSURES</p> <p>(a) USB3 Read Only/Read Write switchable External Hard Drive Chassis with Power Supply</p>
6	<p>EXTRAS</p> <p>(a) Hard Drive Adapter 2.5 Inch</p> <p>(b) Hard Drive Adapter 1.8 Inch</p> <p>(c) TDA5-ZIF ZIF HD Adapter w/case</p> <p>(d) TDA3-1 Micro SATA HD Adapter</p> <p>(e) SATA LIF Adapter</p> <p>(k) 2 TB SATA Hard Drive</p> <p>(l) Precision Electronic Tool Kit</p> <p>(m) Power Strip - 120v/240v Compatible</p> <p>(n) Universal Power Adapter</p>

Handwritten signature/initials

Handwritten signature/initials and number 47

S.No	Description of Requirements
7	PELICAN CASE
	(a) Hard-sided with Padded Laptop Insert
	(b) Watertight / Airtight
	(c) High Impact
	(d) Custom Foam Lined
	(e) Custom Lid Organizer for Cables and Adapters
	(f) 24" x 20" x 14" - 58lbs
8	SOFTWARE
	(a) Microsoft Windows 98SE Standalone DOS (Configured & Pre-Installed)
	(b) Microsoft Windows 8 Professional 64 bit (Configured & Pre-Installed)
	(c) Microsoft Office 2016
	(d) Suse Linux Professional (Pre-Configured)
	(e) Symantec GHOST
	(f) DVD/CD Authoring Software
	(g) High-End Forensic laptop should come pre-installed with Forensic analysis software with Live Boot virtualization, Shadow Copy, Meta extraction, Carving, Hash Sets, Index and Keyword search, flexible graphic user interface (GUI) with advanced sorting, filtering, keyword searching, previewing and scripting technology and Bookmarking capability. The software should allow the investigator to Boot forensic image files and view electronic evidence in a forensically sound virtual environment. Boot both Windows (all versions) and Macintosh computers.
	(h) Product Offered should be of International Repute & Brand and should not be assembled Machine.
	(j) In case of Distributor/ Reseller; OEM/ Manufacturer's Authorization for Supply and Service should be attached with the Tender.
	(k) Bidder should have OEM trained Manpower for Product Installation and support, Supporting document for the same to be attached.

3. INTELLIGENT INVESTIGATION MANAGEMENT SYSTEM

S.N	Description of Requirements
1	Tool should be collaborative end-to-end product that uses a clean, intuitive interface, allowing anyone get started with very little training. It should provide digital evidence and lab management, as well as archiving, which allows teams to understand how the evidence was handled and where to find it in the future.
2	Tool should works through common browsers on Windows, Mac, Linux, and mobile OSs and it builds statistics as you enter information. It should be able to incorporate case management stats into reporting tools.

Handwritten signature/initials

Handwritten signature/initials and number 48

S.N	Description of Requirements
3	Also have below features:
	(a) Global Collaboration on Any Case
	(b) Unlimited Client Base
	(c) Permanent Case Archives
	(d) Chain of Custody Preservation
	(e) Complete Exam Documentation
	(d) Curriculum Vitae Management
	(e) Asset Management
	(f) Local or Remote Browser Access
	(g) Consolidation of All Case Information
	(h) Automatic Statistics Generation
	(j) ICAC and Cyber tip Management for Law Enforcement
	(k) Financial Information Management
	(l) Lab Expenses Analysis
	(m) Grant Documentation Management
	(n) Project Expense Accountability
	(o) Invoice Generation
	(p) Process Review Facilitation
	(q) In- eld Evidence Triage
	(r) Scalability to Grow with Your Needs
	(s) Barcode Generation
	(t) Secure 256-bit Encryption
	(u) Standardized, repeatable process management

4. ARTIFICIAL INTELLIGENCE (Workstation)

S. No	Description of Requirements								
1	The system should have deep learning platform providing unprecedented performance with industry leading 1 GPUs, fast GPU interconnect, high bandwidth fabric and a configurable GPU topology to match your workloads.								
2	The system should have the ability to autonomously learn, predict, and adapt using massive data sets.								
3	<table border="1"> <tr> <td>Processor/ Cache</td> <td> <ul style="list-style-type: none"> 2 x Intel Xeon Scalable Processors with 3UPI links, 2.4GHz Processor base frequency 20 cores with Intel HT Technology </td> </tr> <tr> <td>CPU</td> <td> <ul style="list-style-type: none"> 4 NVIDIA TESLA V100 SXM2 GPUs </td> </tr> <tr> <td>Cores</td> <td> <ul style="list-style-type: none"> 300 GB/s GPU-to-GPU NVIDIA NVLINK </td> </tr> <tr> <td>GPU</td> <td></td> </tr> </table>	Processor/ Cache	<ul style="list-style-type: none"> 2 x Intel Xeon Scalable Processors with 3UPI links, 2.4GHz Processor base frequency 20 cores with Intel HT Technology 	CPU	<ul style="list-style-type: none"> 4 NVIDIA TESLA V100 SXM2 GPUs 	Cores	<ul style="list-style-type: none"> 300 GB/s GPU-to-GPU NVIDIA NVLINK 	GPU	
Processor/ Cache	<ul style="list-style-type: none"> 2 x Intel Xeon Scalable Processors with 3UPI links, 2.4GHz Processor base frequency 20 cores with Intel HT Technology 								
CPU	<ul style="list-style-type: none"> 4 NVIDIA TESLA V100 SXM2 GPUs 								
Cores	<ul style="list-style-type: none"> 300 GB/s GPU-to-GPU NVIDIA NVLINK 								
GPU									

Handwritten signature

Handwritten signature and date

S.N	Description of Requirements	
4	System Memory Memory Capacity Memory Type	<ul style="list-style-type: none"> • 12 DIMM slots • 384GB DDR4- 2666 ECC DIMM • 2666/2400/2133MHz ECC DDR4 SDRAM
5	SSD	<ul style="list-style-type: none"> • 4 x 1.92TB
6	On-Board Devices Chipset SATA Network Connectivity IPMI	<ul style="list-style-type: none"> • Intel C621 chipset or higher • SATA3 (6Gbps) with RAID 0, 1, 5, 10 • Intel X540 Dual Port 10GBase-T • Support for Intelligent Platform Management Interface v.2.0
7	Input/Output SATA LAN USB VGA	<ul style="list-style-type: none"> • 4 SATA3 (6Gbps) ports • 2 RJ45 10GBase-T ports and 1 RJ45 Dedicated IPMI LAN port • Minimum 2 USB 3.0 ports • 1 VGA port
8	Chassis Form Factor	<ul style="list-style-type: none"> • 4U Rack mount
9	Expansion Slots PCI-Express	<ul style="list-style-type: none"> • 4 PCI-E 3.0 x 16 slots
10	Drive Bays Hot-swap	<ul style="list-style-type: none"> • 2 Hot-swap 2.5" SAS/SATA drive bays
11	Power Supply	<ul style="list-style-type: none"> • 2000W Redundant Power Supplies Titanium Level

CYBER MANAGEMENT AND MONITORING

1. 55" DISPLAY FOR CONTROL CENTRE

S.No	Description of Requirements	
1.	Supply Screen Size	55" or above.
2.	Panel Technology	IPS.
3.	Back Light Type	Direct/Edge LED for Slim depth of display.
4.	Aspect Ratio	16.9.
5.	Native Resolution	1,920 X 1,080 (FHD) or High, display should support UHD resolution in Video wall application.
6.	Brightness	700nits or Higher to get clear visibility in highlight condition of room if required.
7.	Contrast Ratio Dynamic CR	450,000:1 or Better to ensure the contrast as per requirement of contents.
8.	Viewing Angle(HxV)	178 X 178 angle to cover Max viewing angle from any location of Room. Response Time
9.	Life time (Typ.) or High to ensure full performance of LED for Long period. Operation Hours:	24Hrs grade panel for ensure Heavy Duty cycle if required Portrait & Landscape suitable format to ensure zero gravity effect in case of customized installation for long period.

Handwritten signature

Handwritten signature 50

S.No	Description of Requirements	
10.	Orientation:	Portrait & Landscape suitable format to ensure zero gravity effect in case of customized installation for long period.
11.	Input ports:	HDMI 1.DP1. DVI D1.USB RJ45(LAN1) or high to cover all types of inputs as per site requirements & future requirements.
12.	Output ports.	Display port (DP) for daisy chain to run FHD contents without controller.
13.	External Control:	RJ45 (LAN 1) for daisy chain to take control of video wall from remote location.
14.	Bezel to Bezel (Gap):	1 mm or less to get seamless picture/video experience.
15.	Key Feature required ;	Temperature Sensor, Auto source selection, Energy Saving Calibration Mode, Failover, Wake on LAN, No signal Screen.
16.	Power supply:	100 240V. 50/60Hz
17.	Power Consumption	300 Watts or less.
18.	Operation Humidity	10% to 80%. -
19.	Certification's	UL for safety. FCC for Electro Magnetic Communication, Energy star rated for confirmation of power consumption & BIS.

2. DATA WALL CONTROLLER

S.No	Description of Requirements
1.	Supply of controller for video wall Display & Scaling,
2.	Display multiple sources anywhere on display up to any size,
3.	All input sources should be displayed on the video wall in freely resizable and movable windows inputs.
4.	Should have option to connect to 4 minimum sources through, HDMI.
5.	Each in Full HD Format(1920x1080) output to connect to minimum 4 Displays. Each in Full HD Format (1920x1080)

3. INCIDENT RESPONSE MANAGEMENT AND ALERT SYSTEM

S.No	Description of Requirements
1.	General Requirement of IT Service Management Solution:
	(a) Should able to support and handle large volume of incident
	(b) Should able to support and handle large volume of service requests
	(c) Should able to support and handle large volume of changes
	(d) Proposed Service desk/ HDMS must be ITIL certified

Handwritten signature/initials

Handwritten signature/initials

S.No	Description of Requirements
	(e) Native integration of processes i.e. Incident Management with Change Management and vice-versa
	(f) Native integration of processes with Knowledge base i.e. automatically creation of knowledge base post closure of tickets
	(g) The solution should have a Single Architecture and leverage a single application instance across ITIL processes, including unique data and workflows segregated by business unit.
	(h) Able to create and modify forms as per customer requirement
	(j) Able to define different SLAs for different services / domains
	(k) Solution should support multi-tenancy with complete data isolation as well as with ability for analysts based on access rights to view data for one, two or more organizational units
	(l) Able to define different workflows for different processes
	(m) Able to send automatic escalation mails as defined in workflow
	(n) Should be able to integrate CMDB from different federated data sources and build a single CMDB
	(o) Should provide email based interactions allowing ticket creation, update and approval of request.
	(p) Should able to integrate with Active Directory and populate user information automatically
	(q) The system should have graphical interface to define, visualize and update ITIL processes
	(r) The solution should provide to browse through CMDB which should offer powerful search capabilities and auto-completion for configuration items and services, enabling to quickly find Cis as well as their relationships to other Cis.
2.	<u>Incident and Problem Management</u>
	(a) Service Desk solution should allow detailed multiple levels/tiers of categorization on the type of incident being logged for IT services that shall span across multiple domains.
	(b) Service Desk solution should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.
	(c) The solution should provide embedded and actionable best practices workflows i.e., best-practices process & views based upon implementations
	(d) It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location.

Handwritten signature

Handwritten signature

S.No	Description of Requirements
	(e) Solution should support fast service restoration leveraging previous incident data.
	(f) It should have the ability to search multiple built-in knowledge bases like the incident, problem, and known-error database simultaneously without requiring the agent to search each knowledge base individually.
	(g) Should support automatic assignment of ticket to the right skilled resource based on business priority Ex - Database crash issue need not be assigned to an L3 DBA unless the business service is completely down.
	(h) It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
	(j) Should support text search capabilities
	(k) Should centralize all known error and problem workarounds into a single, searchable knowledge base
	(l) It should provide an interactive process flow bar that guides novice users through the ITIL process for incident management to ensure faster issue resolution.
	(m) The incident Management solution should be completely integrated to the CMDB to ensure that Cis can be associated with the ticket to provide better visibility
	(n) The incident management solution should have the ability to initiate the change request
	(o) The solution should have the ability to associate an incident with an existing change request, a problem or known error for tracking purposes
	(p) The service desk should have shift management capabilities for support staff wherein tickets are allocated based on shift availability.
	q) It should allow the CI to be associated with tickets.

Handwritten signature/initials

Handwritten signature/initials

4.

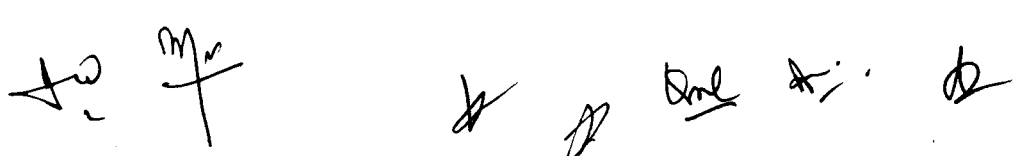
CENTRAL NETWORK ASSET MANAGER

S.No	Description of Requirements
1.	Should be a comprehensive management platform that delivers integrated, modular management capabilities across fault, configuration, accounting, performance, and security (FCAPS) needs
2.	Should support minimum 50 wired devices from day 1 and the solution should be scalable up to 1500 wired devices without any hardware or software up-gradation.
3.	Should allow automatic topology discovery and creation of network maps for layer 2 as well as layer 3 networks including all the available VLANs
4.	Should have network inventory polling capability for IP network nodes, available line cards, modules, ports, physical links, VLAN interfaces and all the other SNMP capable devices in the network.
5.	Should allow extensive fault management with real time event and alarm notifications including system logs
6.	Should allow centralized creation and management of VLAN and ACL policies
7.	Should have scheduled device configuration back-up and restore functionality
8.	Should have automatic detection of configuration changes for easy trouble shooting and isolation.
9.	Should allow monitoring and management of 3rd party devices and end points.
10.	Should have the functionality of scheduled configuration roll out
11.	Should have the functionality to perform scheduled or unscheduled network wide software or firmware upgrades
12.	Should have the ability to customize NMS dash board.
13.	Should allow grouping of devices for applying any particular change/task
15.	Should have 64-bit support
16.	Should support centralized as well as distributed deployment.
17.	Should support virtualization management; management and monitoring of both physical and virtual networks. It should provide insight into and management of virtual networks and reduce migration complexity by aligning and automatic network policies with virtual images.
18.	Should support role based access control
19.	Should be with software update and upgrade assurance during the warranty period
20.	Should have support for add-on modules on the same software platform for monitoring and management of routers, wireless controller, wireless access points and wireless client devices.

to Mr

Dr. Ar. 2 54

S.No	Description of Requirements
21.	Should facilitate enable centralized management of proposed network elements with a variety of automated tasks, including discovery, categorization, baseline configurations, software images, configuration comparison tools, version tracking, change alerts, and more
22.	Should support centralized VLAN Management to view current VLAN configuration, VLAN topology, bulk VLAN deployment etc.
23.	<p>(a) Should provide high-performance, scalable network log audit and analysis support with auditing online activities of internal users</p> <p>(b) Should support various log formats such as NAT, flow, NetStream including log formats that allows audit security-sensitive operations and digest data from HTTP, FTP, and SMTP packets</p> <p>(c) Should support policy driven log filtering</p> <p>(d) Should support log collection from devices that do not otherwise support the standard protocols such as Flow, NAT, NetStream, sFlow/Netflow etc.</p> <p>(e) Should support user activity auditing of at least 50 users from day 1 and this should be optionally extendable up to 1500 users.</p>
24.	Should offer following RADIUS/AAA features:
	<p>a) Shall support user identity authentication based on the access policies associated with infrastructure resources, such as routers, switches, license for 100 users from day 1.</p> <p>b) Shall provide a full-featured RADIUS server that supports centralized authentication, authorization, and accounting management.</p> <p>c) Network-agnostic device fingerprinting capabilities based on HTTP+MAC+DHCP device recognition for BYOD.</p> <p>d) Shall support authentication modes like 802.1X, VPN, portal, and wireless access identity modes like PAP, CHAP,EAP-MD5, EAP-TLS, and PEAP to fit into applications with different security requirements.</p> <p>e) Shall provide centralized policy creation to set the appropriate access rights for each type of user and device across the network.</p>
25.	Should be a ITILv3 compliant comprehensive management platform that delivers integrated, modular management capabilities across fault, configuration, accounting, performance, and security (FCAPS) needs.
26.	Offered software should have compatibility with Microsoft Windows or Linux operating systems
27.	Offered software should be scalable up to 1500 wired devices and 1500 users.




E. COMMON HARDWARE

1. TIME SERVER

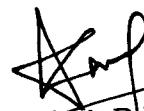
S.N	Description of Requirements	
Power Supply:		
1.	Voltage	230 +/- 10% V AC
2.	Frequency	47-55 Hz
Functions/ Features :		
3.	Time Facility	Using Universal Time co-ordination(UTC)
4.	Propagation delay Compensation	Supported
5.	Accuracy	+/- 250 Nanosecond
6.	Time Accuracy	Better than 1 PPM
7.	LCD Display	Front panel LCD display to show status, time and no. of satellites
8.	Inputs	GPS Antenna input through BNC connector.
9.		Power Supply
Outputs		
10.	NTP output (2 nos. customizable) for NTP client access through RJ-45 .Both Ports shall be independent	
11.	RS232 serial port output (2 Nos)	
12.	Pulse output: 1 PPS, 1/2PPM, 1PPM (Configurable).	
13.	Support Client request per Second	10,000 or higher
Antenna		
14.	Length of GPS	50 meters
15.	Gain	Over 30 DB


Handwritten signatures and initials:
 To: M.V. [Signature] [Initials] [Initials] [Initials] [Initials]

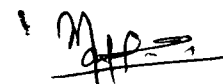
S.N	Description of Requirements
16.	Receiver, Global Positioning System, Display Type:Lcd; Display Size:2 X 3.5 Inch; Display Resolution:240x400 Pixels; Data Interface:Ethernet; Pc Interface:Ethernet;; Expansion Slot Type:USB; Way Points:2; Server Frequency:48-55 Hz; Operating Temperature:0-55 Deg.C; Electrical Rating:230 V AC; Additional Information:With Antenna And Surge Arrestor



(Avirat Pandey, AC)
ITBP

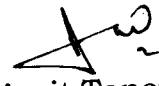

(Sandesh Kumar, AC)
SSB

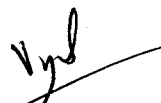

(Maj. A.P. Eldo)
NSG

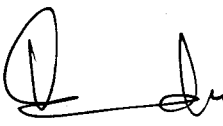

(Vivek), DC(IT)
CRPF



(P. R. Jha), DC(Comn)
CRPF


(Col. Omkar Singh)
Assam Rifles



(Amit Taneja), DIG(Eqpt)
CRPF


(Virendra Agrawal), DIG(Comn)
CRPF


(Ravideep Singh Sahi)
IG(Comn&IT), CRPF


(Zulifiquar Hasan), IPS
SDG(HQ), CRPF

Approved/Not Approved


(Kuldiep Singh, IPS)
DG, CRPF

TRIAL DIRECTIVES OF CYBER SECURITY OPERATING CENTRE

A) SECURITY INFORMATION & EVEN MANAGEMENT (SIEM)

1. SECURITY INFORMATION AND EVENT MANAGEMENT

S.N	Description of Requirements	Trial Directives
General		
1	<p>Collection Methodology: The proposed solution must provide agent and agent-less solution that can automatically scan the list of server and other device to be monitored and will automatically accept events and start to monitor device without any administrator intervention. In case for any specific device/ application agent are required, it must have provision for same as well.</p>	BOO will check practically.
2	<p>Architecture: The capability in general of the components are given below:-</p> <p>(a) Collectors: Logs collectors will be deployed to collect logs from various device and application at a particular location. The main function (but not limited to) are:-</p> <ul style="list-style-type: none"> (i) Collection (ii) Compression (iii) Encryption (iv) Caching, where the solution must provide for storing of logs in case of no communication with consolidator / correlate for minimum period of 7 days. <p>(b) Consolidator. The main function (but not limited to) are:-</p> <ul style="list-style-type: none"> (i) Indexing and Searching. (ii) Reporting. (iii) Storage and Forensics. <p>(c) Correlators. Correlators will be deployed to process the event sent by various collectors/ consolidator. All logs collected should be analyzed and correlated. The main functions (but not limited to) are:-</p> <ul style="list-style-type: none"> (i) Real-Time Incident Monitoring. (ii) Threat Notification and Alerting (iii) Incident Case Workflow. (iv) User and Entry Behavior Analytics. 	BOO will check practically.

Handwritten signatures and initials at the bottom of the page.

S.N	Description of Requirements	Trial Directives
	<p>d) Centralized Management Server.</p> <p>(i) The solution must provide central Management of entire SOC from a particular site and provide access to SOC administrators from other location for managing the device in their respective areas.</p> <p>(ii) The proposed solution should provide all system-level administration through a single web User Interface.</p> <p>(e) All the software component of the SIEM solution must be from the same OEM .</p>	
3	<p>Total aggregated EPS across the deployment should be 10,000 or more sustained EPS and 25,000 Peak EPS from day 1 without rated license limit of integrated devices, no of assets, no of console users, security analysts. Hardware, Virtual Machines, Operation System and all related software for all the component at all location will be supplied by the Bidder as part of turnkey solution to meet the required functionalities. The system may be delivered as appliances or as server bundled with integrated bundle of OS, software and database. Collectors will separate device with all requisite OS and applications. Consolidator and Corralator can be either same device or a separate device offering their respective functionalities with all requisite OS and applications. High Availability of device must be ensured at all location. If a correlator at any location fails, all its logs should be diverted to be handled by the alternate correlator.</p>	BOO will check practically.
4	<p>Workflow Automation:</p> <p>The proposed solution must provide a SOC orchestration layer solution that can must facilitate incident Investigation and response workflow that must open tickets, assign the tickets to the appropriate team member while maintaining a complete audit trail for the incident handling process.</p>	BOO will check practically.
5	<p>Deploying Methodology:</p> <p>Solution must support Hybrid deployment including Hardware, Software, Physical and virtual environment.</p>	BOO will check practically.
6	<p>It should support any number of logs sources and devices without any licensing limitation. Solution must be designed for no log drops at any stage of the solution.</p>	BOO will check practically.

Handwritten initials/signatures

Handwritten signature and date: 3rd 11/12

S.N	Description of Requirements	Trial Directives
<u>Event Collection & Normalization</u>		
7	<u>Device Support:</u> The Proposed solution must provide a comprehensive coverage as cross all types of event sources (but not limited to) like Databases (SQL server 2005, 2008,2012, Oracle), ALX Server, Unix/Linux Server, Windows Server, Routers, Switches, Gateways, hubs, Windows OS 8.8.1,10, firewalls, for all types of OEM products	BOO will check practically.
8	<u>Application Logs:</u> The solution should be able to collect security logs generated by software products like databases, web and applications like ERP etc and custom built applications.	BOO will check practically.
9	<u>Distributed Event Processing:</u> The proposed solution must collect logs in a distributed manner, offloading the processing requirement of the logs management system for tasks such as filtering, aggregation, compression and encryption	BOO will check practically.
10	<u>Custom Collection API:</u> The proposed solution must have a software tools to allow customers to create integration with unsupported legacy or internally developed event sources. The software tool must allow customer to integrate with Syslog, log files and Databases.	BOO will check practically.
11	<u>Normalized Event Data:</u> The Proposed Solution must normalized all collected event data into a consistent format.	BOO will check practically.
12	<u>Categorized Event Data:</u> The Proposed solution must categorized log data into an easy-to- understand humanly- readable format that does not require knowledge of OEM-specific event IDs to conduct investigation, defines new correlation rules, and/or create new reports/dashboards.	BOO will check practically.
13	<u>Secure Transport:</u> The proposed solution must provide encrypted transmission of log data between all the collected/consolidators and correlators.	BOO will check practically.
14	<u>Reliable Transport:</u> Logs Transmission should use reliable TCP protocol that will ensure retransmission in the event of protocol failure to ensure that no log data is lost in transit.	BOO will check practically.

to m

of the ...

S.N	Description of Requirements	Trial Directives
15	<p>Collection Health Monitoring: Any failures of the event collection infrastructure must be detected immediately and operations personnel must be notified. Health monitoring must include the ability to validate that original event sources are still sending event.</p>	BOO will check practically.
16	<p>Event filtering: The Proposed solution must provide inline (user definable) options to reduce event data by filtering out unnecessary event data before it is tored or correlated.</p>	BOO will check practically.
17	<p>Event Aggregation: Aggression must be flexible in which normalized fields can be aggregated and provide the ability to aggregate in batches or time windows. An examole of aggregated would be every 1000 identical event be aggregated into one record with the necessary start and end timestamp and the aggregate count of 1000.</p>	BOO will check practically.
18	<p>Compression: The proposed solution must provide at least 70% compression.</p>	BOO will check practically.
19	<p>Raw Event data: Proposed Solution must support the option of colleting raw event data using Syslog, FTO, SCP, SNMP, and any other protocol required for collection of logs etc. This ensures original audit data is available for forensics.</p>	BOO will check practically.
20	<p>Windows and Event Logs: The proposed solution must be integrated with a Windows Domain in an agent- less fashion and collect the vent logs from multiple systems without requiring any agent to be installed on the end device.</p>	BOO will check practically.
21	<p>Time Synchronization: The SIEM solution components along with the log source should be synchronized to single time.</p>	BOO will check practically.
22	<p>Centralized Management: The proposed Solution must be managed centrally allowing users to configure all features; backup configuration and push software update etc. Using one centralized creation.</p>	BOO will check practically.
23	<p>Event replay: The Proposed solution must provide a software based tool or facility which allows production event data to be exported and replayed into the system for testing and content creation.</p>	BOO will check practically.

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements	Trial Directives
Log Management- General		
24	Scalability: The proposed Solution must be scale to large environment (upto 1,00,000 EPS) with additional EPS licenses and additional hardware. This should be software based solution.	BOO will check practically.
25	Storage integrity: The proposed solution must utilize storage RAID levels for Local data redundancy with the ability to reinitialize a failed disk from data stored in the RAID cluster.	BOO will check practically.
26	Storage Flexibility: The proposed solution must be able to store log data both locally and with SAN/NAS/Tape Drive Integration.	BOO will check practically.
27	Retention Policies: The Proposed Solution must provide the Ability to create multiple policies for the automated retention and disposal of log data.	BOO will check practically.
28	Log Data Integrity: The proposed solution must provide audit quality integrity mechanisms.	BOO will check practically.
29	Search interface: The proposed solution must provide a simple intuitive search interface usable by different users with varying skill sets.	BOO will check practically.
30	Search Drilldown: The Proposed solution search interface must provide the ability to drill down on output data and alter the search filter by simply click on fields within an event.	BOO will check practically.
31	Search Patterns: The proposed search interface must provide support for simple Boolean-Style search patterns as well as complex regular expressions.	BOO will check practically.
32	Search Operators: The Proposed solution must provide a comprehensive list of search operators with expandable Syntax, and allow users to "grow" into complex patterns, as and when required.	BOO will check practically.
33	Flow-based Searches: The proposed solution must allow easy and intuitive query structures which allow to compound search Expression into Complex patterns, Similar to what would otherwise required "piping" Multiple commands into Scripts using traditional tools, without requiring any knowledge of scripting languages.	BOO will check practically.

Handwritten signature

Handwritten signature

S.N	Description of Requirements	Trial Directives
34	<p>Search- Structured and unstructured Data: The proposed Solution Search Performance must be capable of searching through structured (index) events as well as unstructured (natural Language) log messages.</p>	BOO will check practically.
35	<p>Search Method Combination: The proposed solution search interface must provide the option to allow combined search queries using a combination of Methods such as index and in-indexed event data and regular expression and full unstructured text search simultaneously without impacting search performance.</p>	BOO will check practically.
36	<p>Search Time Range: The proposed solution search interface must provide the option to search interface using either a custom time (data/ time start, end) or dynamic time (last 2 hours).</p>	BOO will check practically.
37	<p>Search Result View: The proposed solution search interface must provide option to customize the output columns of the queries result. The option may include constraining the view to only normalized data or filtering the view to only see raw data.</p>	BOO will check practically.
38	<p>Search Export: The log manager System must provide the ability to export the search result to the user's local system, a mounted files system or locally on the log management system for other users to view. The Export should be saved in either a csv or pdf format.</p>	BOO will check practically.
39	<p>Save search Filters: The proposed solution must provide a simple, intuitive ways of allowing users to save search filters for later use and to be shared with other authorized users.</p>	BOO will check practically.
40	<p>Historical Analysis: The proposed Solution must be capable of processing and storing large volume of historical log data that can be restored and analyzed for forensic investigation purpose.</p>	BOO will check practically.

Handwritten initials/signatures: Jw, Mr

Handwritten signature: S. J. Sme. A. S.

S.N	Description of Requirements	Trial Directives
Log Management-Archiving		
41	Schedule Archive: The proposed solution must provide a simple interface to schedule the compression and archiving of log data.	BOO will check practically.
42	Manual Archive: The proposed solution must provide a simple interface to manually archiving log data.	BOO will check practically.
43	Retention: Solution will be capable of retaining online logs for 3 months with consolidator and correlate.	BOO will check practically.
Log Management -Alerting		
44	Real-Time Alerts: The proposed Solution must be capable of generating alerts based on filter pattern matches for operation health monitoring.	BOO will check practically.
45	Threshold Alerts: In addition to real-time alerts, the system must provide historical, threshold alerts, configuration from saved search queries.	BOO will check practically.
46	Alert Filters: The proposed solution must provide per-defined alert and provide the ability to re-use pry-defined filters and own created filters as alert criteria.	BOO will check practically.
47	Alert Delivery: The proposed Solution must provide options of how alerts are delivered to operations or security personnel or reporting to the web consol, send an email or generate an SNMP trap to an external management system. The solution must be capable of doing all three concurrently for each alert.	BOO will check practically.
Log Management - Reporting		
48	Per-Defined Report: The proposed solution must provide per-defined reports for Operations, Security and Compliance that can easily be modified.	BOO will check practically.
49	Compliance Report: Solution should provide compliance auditing, alerting and reporting.	BOO will check practically.

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements	Trial Directives
50	<p>Customized Reports: The proposed solution must provide the ability for customers to create their own reports with reports template, reporting wizards as well as an advance interface for power users to create their own custom report queries.</p>	BOO will check practically.
51	<p>Report Export: The proposed solution reporting function must be capable of exporting reports in various formats. At a minimum, the report formats should be Excel Spreadsheet (.Xls), Adobe Acrobat (.pdf), Word Document (.doc), web Page (.Html), and Comma-Separate Values (.csv). The reporting functions should also allow the report to be run and viewed ad-hoc by user as well.</p>	BOO will check practically.
52	<p>Report Scheduling: The proposed solution must provide the ability for customer to schedule and email reports to run hourly, daily, weekly or monthly as either an attachment or a URL path for users who have system access.</p>	BOO will check practically.
53	<p>Drilldown report: The proposed solution reporting engine must provide tenability to generate linked report with a master report that allows users to drill down into the data within the report dynamically.</p>	BOO will check practically.
54	<p>Run-Time Report Options: The proposed solution reporting engine must provide the ability to filter, highlight, and modify various report functions at runtime. This should include the ability to selectively define device group or storage portion to report upon.</p>	BOO will check practically.
Log Management-Dashboards		
55	<p>Customizable dashboards: The Proposed solution should provide dashboards specific to each user and should be user configurable. The dashboard must be capable of displaying multiple daily reports specific top each user job function.</p>	BOO will check practically.

Handwritten initials: Jw, Mn

Handwritten notes: A →, Dme A. de

S.N	Description of Requirements	Trial Directives
Log Management Integration		
56	Syslog Forwarding: The proposed solution must be able to receive raw (i.e. unprocessed) event data in the form of syslog message or text log files, in addition to receive the raw original event data from collectors.	BOO will check practically.
57	Correlation- Analysis and Workflow	
58	Correlation Rules: The proposed solution must provide many correlation rules to automate the incident detection and workflow process	BOO will check practically.
59	Cross-Device Correlation: The proposed solution must be capable of correlating activity across multiple devices to detect authentication failures, perimeter security, worm outbreak and operational event in real-time without the need to specify particular device type.	BOO will check practically.
60	Statistical Correlation: the proposed solution must be capable of keeping a statistical baseline of "normal" monitored activity. This includes attacker, Target, Ports, Protocols and session data.	BOO will check practically.
61	Correlation Flexibility: Solution must be capable of running crops device correlation, advance correlation real time correlation and historical correlation at the same time.	BOO will check practically.
62	Historical Correlation: The proposed solution must be capable of monitoring attack history against critical assets or by particular users.	BOO will check practically.
63	Session Correlation: The proposed Solution must provide the ability to correlate DHCP,VPN and active Directory event to provide session tracking for every user in the enterprise. This is essential for pinpointing who was using a particular workstation historically during an incident investigation.	BOO will check practically.
64	Identity Correlation: The proposed solution must natively integrate with existing authentication directories to import context related to users and role which will then correlate and attribute every event to an actual user, regardless of the event source.	BOO will check practically.

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements	Trial Directives
65	<p><u>Role Correlation:</u> The proposed solution must provide the ability to use real-time context from authentication directories in order to determine whether a user's activities are aligned with their role. This function must automatically alter the monitoring process when a user changes roles within the organization.</p>	BOO will check practically.
66	<p><u>Geo-Spatial Location Correlation:</u> The proposed Solution must provide the ability to monitor activity between multiple geographical locations.</p>	BOO will check practically.
67	<p><u>Dynamic/Static Lists:</u> The proposed solution must allow users to define either white list or blacklist that can be used as inclusion or exemption during the correlation process. Additionally, the correlation engine should utilize dynamic lists to provide important information such as shared user monitoring, secession tracking, attack history and privileged system access. Products must support import capability to create/ update monitoring list which can be dynamically add/removed values without manual intervention.</p>	BOO will check practically.
68	<p><u>Correlation Tracking :</u> The proposed Solution must be able to correlate event data against static lists of items that the user either allows or doesn't allow on the network (i.e. list of insecure protocols). Additionally, lists should be automatically populated by the system for Tracking things such as attacks, user's session and other policy violation.</p>	BOO will check practically.
69	<p><u>Pattern Detection:</u> The system must be capable of discovering patterns of subverted activities that would otherwise go unnoticed (i.e. slow and low attacks).</p>	BOO will check practically.
70	<p><u>Correlation Performance:</u> The proposed solution must be capable of efficiently presenting categorized data to the correlation engine to allow real-time detection and response.</p>	BOO will check practically.

Handwritten signature

Handwritten signature

S.N	Description of Requirements	Trial Directives
71	<p><u>Rule Chains:</u> The system must provide the ability to allow rules to be triggered in a series, matching various correlation activity before an alert is generated.</p>	BOO will check practically.
72	<p><u>Vulnerability Based Correlation:</u> The proposed solution must be capable of assessing attack vector and the targeted system to determine the susceptibility of a threat and lower the priority if the target is not susceptibility and raise the severity if the target is susceptibility or the user is not Vulnerability data of each asset monitored should be imported/generated into the system which can then be used by the SIEM to manage false positive reduction or generated remediation activity to secure the system.</p>	BOO will check practically.
73	<p><u>Asset Intelligence:</u> The proposed solution must provide the ability to generate/record context and keep and inventory of all data as it relates to assets. This includes hostname, IP Address, MAC, location Purpose, Owner, patch, Vulnerability data, exemption, compliance critically and other related data. The asset profile should be created for all monitored system which can be searched and correlated on.</p>	BOO will check practically.
74	<p><u>Role Based Intelligence:</u> The proposed solution must provide a mechanism to logically segregate data by role, department, domain or customer.</p>	BOO will check practically.
75	<p><u>Conditional Analysis:</u> The Proposed solution must allow the ability to define conditional or variable statement to derive additional information from "hard" event data to provide dynamic context during correlation and reporting. This conditional analysis must be globally available throughout the system.</p>	BOO will check practically.
76	<p><u>Alert Thresholds:</u> The Proposed solution must provide the ability to aggregate and suppress alerting with granular option and use conditional logic to determine if any alert should be generated.</p>	BOO will check practically.
77	<p><u>Re-usable Content:</u> The solution must allow users to create objective such as filters or search queries that are reusable throughout the system.</p>	BOO will check practically.

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements	Trial Directives
78	<p><u>Content Editor:</u> The proposed solution must provide a common interface to create or modify resources within the system. All Aspects of this editor must apply to the development of rules, reports, dashboards and other resource that will be created in the system.</p>	BOO will check practically.
79	<p><u>SOC Orchestration:</u> There should not be separate rated license for orchestration engine (SOAR)</p>	BOO will check practically.
80	<p><u>Case Management:</u> The proposed solution must provide complete process framework for integrating security monitoring and investigation with existing workflow procedures. Workflow should involve escalating and incident to other users within the same team or within other teams etc.</p>	BOO will check practically.
81	<p><u>Workflow:</u> The process solution must provide a complete lifecycle management, audit trail and accountability (SLA management) during the incident handling or forensic category. The workflow should be customizable using tools provided in the system.</p>	BOO will check practically.
<u>Colleration - Reporting and Visualization</u>		
85	The system should allow configuring the parser to support any new system introduced in the future.	BOO will check practically.
86	<p><u>Ad Hoc Report Performance:</u> The proposed solution must have a mechanism to collect meta-data used by reports that track information over long periods of the time so that running these reports ad hoc does not take considerably longer than any other reports.</p>	BOO will check practically.
87	<p><u>Dash board Drill-Down:</u> The proposed solution must provide the ability to allow analysts to drill-down from graphical dashboards to the underlying event data.</p>	BOO will check practically.
88	<p><u>Attack Visualization:</u> The proposed solution must provide the ability visually represent event data into a dynamically updated graph. This will assist analysts in determining the expanse of attack and pin point the original attacker during incident response and remediation for example, -Event Graph. -Last State.</p>	BOO will check practically.

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements	Trial Directives
89	<p><u>Content Management:</u> The proposed solution must provide the ability to synchronize its resource contents (i.e. rules dashboard, reports, filters, etc) automatically across multiple instances of the product, to support multi-instance/high -event rate deployments.</p>	BOO will check practically.
<u>Correlation -Advance use Cases.</u>		
90	<p><u>Compliance Automation:</u> The proposed solution must provide value in assisting in adhering to audit requirements, alerting of non-compliance and providing necessary reports that can be used during an audit.</p>	BOO will check practically.
91	<p><u>Physical/ Logically Convergence:</u> The proposed solution must be capable of collecting log data from physically access devices such as card readers, biometrical and security cameras and correlate this information with logical network and security devices to detect such patterns as building access after office hours by contractors or users logged in through VPN and physically accessing the building within the same period.</p>	BOO will check practically.
92	<p><u>Insider Threat Detection:</u> The proposed solution must be able to detect suspicious activity, such as printing large numbers of files outside working hours emailing large attachments to personal email accounts employee communication with competitors or the clearing of system audit logs to cover up malicious activity.</p>	BOO will check practically.
93	<p><u>Forensic Investigators:</u> The proposed solution must be capable of allowing investigators to analyze 90 days worth of historical logs files and then perform complex pattern searches and reporting.</p>	BOO will check practically.
94	<p><u>Real-Time Responses:</u> The proposed solution must be capable of triggering scripts or execute integration commands with third party solutions such as IPS or next generation intrusion prevention systems in order to quarantine or block nefarious activity in real-time.</p>	BOO will check practically.

AS
M

A & One Ar. b

S.N	Description of Requirements	Trial Directives
95	<u>Investigation & Remediation</u>	
96	Solution should have grouping common events for analysis.	BOO will check practically.
97	Solutions should be capable of gathering information about the full context of the attack such as :- (i) Who conducted the attack? (ii) What did they try to accomplish? (iii) When did they make the attempt? (iv) Where they attack?	BOO will check practically.
98	Solution should provide the information necessary to make a decision about how to remediate the threat .The solution should be able to provide incident response that consist of phases and tasks that guides the user on how to adequately responses to the incident ;integrating people processes and technology.	BOO will check practically.
	<u>Analytics -User Behavior.</u>	
99	<u>User Activity Baseline:</u> The proposed solution must provide the ability to monitor user network and application activity to create baseline and then use these baseline to identify anomalous user behavior. User Behavior analysis: the solution should be able to detect anomalous behavior based on rules and behavioral anomalies.	BOO will check practically.
100	<u>State or Terminated User Activity:</u> The proposed solution must be capable of automatically identifying when user accounts are terminated or state and then monitor for any activity from these accounts.	BOO will check practically.
101	<u>Unaccountable User Activity:</u> The proposed solution must able to alert or report on any activity for identities that are not automatically synchronized with the authentication directories. This will help to detect rogue user accounts on critical systems.	BOO will check practically.
102	<u>User Role Monitoring:</u> The proposed solution must provide the ability to synchronized with the authentication directories to collect information regarding user roles and responsibilities and correlate this data with all user activity .Users that violate their roles within the organization should be recorded for alerting and reporting purposes.	BOO will check practically.

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements	Trial Directives
103	<p>User Activity Monitoring: The proposed solutions must be able to track user activity and ultimately bind an individual to an action Analysts must be able to generate ad-hoc reports that will detail what a particular user or group of users has accessed in the enterprise for defined period of time.</p>	BOO will check practically.
104	<p>Generic Account Monitoring: The proposed solution must provide the ability to correlate information regarding users that are logged into the domain where ever exists) and their accounts usage within the enterprise. The proposed solution must provide a mechanism whereby in the event of generic account violations the solution can contain the threat in real -time using quarantine methods such as disabling the user's switch ports adding filters to firewalls disabling user accounts etc.</p>	BOO will check practically.
105	<p>Miscellaneous. Correlate identity attributes to a single user profile from IAM systems flat files, AD/LDAP, and HR repositories.</p>	BOO will check practically.
106	Correlate activity data to users through a common identifier (account, IP address MAC etc.).	BOO will check practically.
107	<p>Account Management : Uncorrelated vs correlated account identification & account tagging.</p>	BOO will check practically.
108	User based views (identify activity access policy violations risk scoreboard)	BOO will check practically.
109	Resource based views [correlated and uncorrelated accounts asset meta data (owner/hours/IP address) resource activity risk scorecard data management of historical transactions].	BOO will check practically.
110	<p>Lookup Data: Static data sets from flat files that the customers want to use in the policy engine (critical accounts resources assets list of domain admin).</p>	BOO will check practically.

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements	Trial Directives
111	Network Map: Import network information (IP address metadata) to be unused in the policy violation and behavior violation engine.	BOO will check practically.
112	Organization Hierarchy & Management: Ability to create and view activities by organizations. User will belong to one organization and many peer groups.	BOO will check practically.
113	Peer groups creation & management.	BOO will check practically.
114	Master- Child node architecture.	BOO will check practically.
115	Data Masking: Encryption in web interface controlled by privacy manager.	BOO will check practically.
116	Role Based Access Control Support: Only user with specific permission can access menus, dashboards and reports control the functional control.	BOO will check practically.
117	Case management Manage, White list resolve and act on user related incidents.	BOO will check practically.
118	User Watch List: User accounts IP address and systems for targeted monitoring.	BOO will check practically.
119	Policy Violation Engine: Flexibility to create rule based violations spanning data identity Access Peer Organization activity network classification time watch list lookup.	BOO will check practically.
120	Rule based content for all devices and applications like (but not limited to) Windows, Proxy, Cisco, VPN, Citrix, Iron port, Juniper VPN, Oracle, Proxy SG, Squid Web Proxy Websense.	BOO will check practically.
121	User Behavior content based content for all devices and applications like (but not limited to) Windows, Proxy, Cisco, VPN, Citrix, Iron Port, Juniper VPN, oracle, proxy SG, Squid web Proxy, Websense.	BOO will check practically.

Handwritten initials: AW, Mr

Handwritten signature: A. S. [unclear] [unclear]

2.LOG COLLECTOR (SIEM)

S.No	Description of Requirements		Trial Directives
1	Chassis	4U Tower Server	BOO will check practically.
2	CPU	1 x Intel Xeon E-2226G (3.4GHz/6-core) Processor or Higher	BOO will check practically.
3	Memory	8 GB DDR-4 RAM - 2666 MTs	BOO will check practically.
4	Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance	BOO will check practically.
5	HDD Bays	Up to 4 HDD Bays. The drive carrier should have intuitive icon based display along with "DO NOT REMOVE" caution indicator that gets activated automatically in order to avoid data loss/downtime due to wrong drive removal.	BOO will check practically.
6	Hard disk drive	1 TB SATA HDD	BOO will check practically.
7	Interfaces	VGA Port: 1 standard (rear) Serial Port:1 optional (rear) Network Port (RJ-45): 2 x 1 GB ports as standard (rear, 1 shared for HPE iLO) Dedicated iLO Management Port (RJ-45): 1 optional (rear) USB 3.0 Port: 6 (1 front, 4 rear, 1 internal) USB 2.0 Port: 1 (1 front)	BOO will check practically.
8	Power Supply	Should support hot plug redundant low halogen power supplies minimum 2 x 500 Watt	BOO will check practically.
9	Fans	Redundant hot-plug system fans	BOO will check practically.

Handwritten signature/initials

Handwritten signature/initials

S.No	Description of Requirements		Trial Directives
10	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support Energy Star ASHRAE A3/A4 UEFI 2.6 SMBIOS Redfish API SNMP v3 TLS 1.2 DMTF Systems Management Architecture	BOO will check practically.
11	Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable 2. Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware	BOO will check practically.

3. LOG CONSOLIDATOR (SIEM)

S.No	Description of Requirements		Trial Directives
1	Chassis	1U Rack Mountable	BOO will check practically.
2	CPU	2 x Intel Silver Processor 4124R	BOO will check practically.
3	Memory	16 DIMM slots. 4 x 32 GB	BOO will check practically.
4	Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance	BOO will check practically.
5	HDD Bays	Up to 8 HDD Bays The drive carrier should have intuitive icon based display along with "DO NOT REMOVE" caution indicator that gets activated automatically in order to avoid data loss/downtime due to wrong drive removal.	BOO will check practically.

Handwritten signature/initials

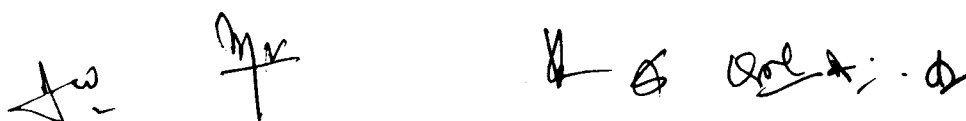
Handwritten initials

Handwritten signature/initials

S.No	Description of Requirements		Trial Directives
6	Hard disk drive	6 x 2.4 TB SAS 10K RPM	BOO will check practically.
7	Controller	Hard Controller Should SUPPORT RAID 0.1 5.	BOO will check practically.
8	Networking features	Server should support below networking cards: (i) 1Gb 4-port network adaptors (ii) 10Gb 2-port Ethernet adaptor (iii) 10GBaseT 4- port Ethernet adaptor (iv) 4x25Gb Ethernet adaptor (v) 10/25Gb 2- port Ethernet adaptor (vi) 100Gb Ethernet Infinib and Options: 40Gb dual port or 100Gb Single or Dual port Adapter 100Gb Single port Omni path adaptor Also 1G x dual Port Should be Provided from Day 1	BOO will check practically.
9	Interfaces	Serial - 1 Micro SD slot - 1 USB 3.0 support With Up to 4 total: 1 front, 1 internal, 2 rear	BOO will check practically.
10	Bus Slots	Two PCI-Express 3.0 slots, at least one x16 PCIe slots	BOO will check practically.
11	Power Supply	Should support hot plug redundant low halogen power supplies minimum 2 x 500 Watt	BOO will check practically.
12	Fans	Redundant hot-plug system fans	BOO will check practically.
13	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support Energy Star ASHRAE A3/A4 UEFI 2.6 SMBIOS Redfish API SNMP v3 TLS 1.2 DMTF Systems Management Architecture	BOO will check practically.



19

S.No	Description of Requirements		Trial Directives
14	System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Support for Commercial National Security Algorithms (CNSA) Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 TPM (Trusted Platform Module) 2.0 Smart card (PIV/CAC) and Kerberos based 2-factor Authentication Configurable for PCI DSS compliance Chassis Intrusion detection	BOO will check practically.
15	System tuning for performance	(i) System should support feature for improved workload throughput for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode "ON" without the frequency fluctuations associated with running in turbo mode. (ii) System should support workload Profiles for simple performance optimization	BOO will check practically.
16	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.	BOO will check practically.
17	Firmware security	(i) For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable. (ii) Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware	BOO will check practically.



S.No	Description of Requirements		Trial Directives
4.	LOG CORRELATOR (SIEM)		
1	Chassis	1U Rack Mountable	BOO will check practically.
2	CPU	2 x Intel Silver Processor 4124R	BOO will check practically.
3	Memory	16 DIMM slots. 6x 32 GB	BOO will check practically.
4	Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance	BOO will check practically.
5	HDD Bays	Up to 8 HDD Bays. The drive carrier should have intuitive icon based display along with "DO NOT REMOVE" caution indicator that gets activated automatically in order to avoid data loss/downtime due to wrong drive removal.	BOO will check practically.
6	Hard disk drive	2 x1.2 TB SAS 10K RPM	BOO will check practically.
7	Controller	Hard Controller Should SUPPORT RAID 0.1 5.	BOO will check practically.
8	Networking features	Server should support below networking cards: (a) 1Gb 4-port network adaptors (b) 10Gb 2-port Ethernet adaptor (c) 10GBaseT 4-port Ethernet adaptor (d) 4x25Gb Ethernet adaptor (e) 10/25Gb 2-port Ethernet adaptor (f) 100Gb Ethernet Infiniband Options: 40Gb dual port or 100Gb Single or Dual port Adapter 100Gb Single port Omni path adaptor Also 1G x dual Port Should be Provided from Day 1	BOO will check practically.





S.No	Description of Requirements		Trial Directives
9	Interfaces	Serial - 1 Micro SD slot - 1 USB 3.0 support With Up to 4 total: 1 front, 1 internal, 2 rear	BOO will check practically.
10	Bus Slots	Two PCI-Express 3.0 slots, at least one x16 PCIe slots	BOO will check practically.
11	Power Supply	Should support hot plug redundant low halogen power supplies minimum 2 x 500 Watt	BOO will check practically.
12	Fans	Redundant hot-plug system fans	BOO will check practically.
13	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support Energy Star ASHRAE A3/A4 UEFI 2.6 SMBIOS Redfish API SNMP v3 TLS 1.2 DMTF Systems Management Architecture	BOO will check practically.
14	System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Support for Commercial National Security Algorithms (CNSA) Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 TPM (Trusted Platform Module) 2.0 Smart card (PIV/CAC) and Kerberos based 2-factor Authentication Configurable for PCI DSS compliance Chassis Intrusion detection	BOO will check practically.



S.N	Description of Requirements		Trial Directives
15	System tuning for performance	<p>(a) System should support feature for improved workload throughput for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode "ON" without the frequency fluctuations associated with running in turbo mode.</p> <p>(b) System should support workload Profiles for simple performance optimization.</p>	BOO will check practically.
16	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.	BOO will check practically.
17	Firmware security	<p>(a) For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable.</p> <p>(b) Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware.</p>	BOO will check practically.

Handwritten signature

Handwritten signature

5. HYPER CONVERGENT INFRASTRUCTURE WITH VIRTUALIZATION LICENSE

S.No	Description of Requirements		Trial Directives
1	Make/Brand	HCI appliance OEM shall be in the Leaders category consecutively in last two published Gartner's Magic Quadrant (or equivalent) reports on "Hyper converged Infrastructure".	BOO will check practically.
2	Hyper Converged Appliance	Hyper converged appliance, which comes Factory Installed with various software including Software Defined Storage and hypervisor. SDS should NOT be top-up or add-on software license bundled on generic x 86 servers. It should be an integral part of appliance.	BOO will check practically.
3		Proposed HCI Appliance should be in all flash drive configurations using not more than 2TB capacity drives. Usable capacity per-node should be after all overheads in respect of core/memory/storage being used for reduplication, compression and optimization.	BOO will check practically.
4		Solution must be able to integrate storage, compute, networking, hypervisor, real-time reduplication, compression, and optimization along with powerful data management, data protection, and disaster recovery capabilities in a standard x86 server building block.	BOO will check practically.
5		Nodes should offer Storage Features such as De-duplication and Compression. Replication / backup license(s) should be provided for the full capacity of the system. Storage performance monitoring software should be included. Future capacity growth shall not warrant any additional software license on the storage landscape.	BOO will check practically.

Jw Mw

*V S Dml * . d*

S.N	Description of Requirements		Trial Directives
6		Proposed hardware must be capable to de-duplicate, compress & optimize all data inline, in real-time with fine data granularity of minimum 8KB data blocks.	BOO will check practically.
7		Solution should ensure minimum impact to production workloads and guaranteed CPU and RAM available to user applications while doing global deduce, compression and optimization.	BOO will check practically.
8		The Hypervisors are to be installed in the nodes along with Cloud / Virtualization Management. The management node requirements, if any should be included by default and management node to be considered outside of the HCI nodes. All offered licenses for virtualization manager are to be of non-embedded type and should have no limitation of functionality.	BOO will check practically.
9		HCI Solution should have minimum 2 types of data copies across Cluster available in the offered solution.	BOO will check practically.
10		HCI appliance hardware OEM shall provide a single TAC support for underlying virtualization and virtualization manager.	BOO will check practically.
11	Processor	Latest Generation Intel® Xeon Processors product family, >=2.00 GHz per Core. Populated with minimum 2 sockets per node.	BOO will check practically.
12	Total Physical Cores	48 Cores (Per-Node)	BOO will check practically.
13	Processor Cache	Min. 35 MB L3 Cache	BOO will check practically.
14	Total Physical RAM	Min. 500GB DDR4. Scalability to double or more of provisioned RAM	BOO will check practically.

Aw 2 Mn

↓ ⊕ Date * d

S.No	Description of Requirements		Trial Directives
15	Total Usable Storage	Min. 20 TB usable capacity post Reduplication and compression per node. The proposed solution must be able to sustain one node failure and it should in no way affect/degrade the production services & usable resources, to the end user application.	BOO will check practically.
16	Network	Minimum 4 x 10/25/40Gb SFP28 (10G SR optics populated) Ethernet ports (each Node) and 2 x 1Gb RJ45 Ethernet ports (Additional ports to be configured by bidders as per their solution requirement). Additionally, Minimum 1' no 1Gb RJ45 Ethernet OOB dedicated management port.	BOO will check practically.
17	Data Protection Features	Backup functionality as an integrated feature or separate server / software license to be offered.	BOO will check practically.
18		Backup must be an independent copy of source Virtual Server and must allow restore of deleted or corrupted source Virtual Server.	BOO will check practically.
19		Support for Replication across separate data centre with the ability to carry simultaneous out bi-directional replication between two data centres and with the ability to replicate Any-to-Any in a Mesh Data Centre deployment of more than 3 DC's.	BOO will check practically.
20		The ability to define backup policy per data store, a group of VMs or specific VM.	BOO will check practically.
21		Data Protection should have RPO of 10 minutes for local backups	BOO will check practically.
22		The ability to execute backup tasks during office hours without impacting to production workloads.	BOO will check practically.
23		Data loss protection against single node failure in cluster.	BOO will check practically.
24		The proposed solution must be able to provide backup reports for audit purpose.	BOO will check practically.

to Mr

1

2

Done A. D

S.No	Description of Requirements		Trial Directives
25	Private Cloud License	Virtualisation license for the complete solution needs to be proposed with the HCI Appliance for this requirement.	BOO will check practically and Firm will submit undertaking certificate.
26		Proposed solution must be able to support the following VM-Centricity and Mobility feature:-	
27		i) Backups for specific VMs and Clone specific VMs.	
28		ii) Ability to move specific VMs between data centres.	
29		iii) VM-level backup instead of forcing protection at the data store or protection domain level.	
30	Data Recovery Features	Data recovery should be independent of source Virtual Server.	BOO will check practically.
31		Solution should provide a backup catalogue to allow any Virtual Server to be recovered to any specific point-in-time.	BOO will check practically.
32		Data recovery process should be simple with an RTO in minutes.	
33	Storage Controller in Nodes	SAS RAID controller with minimum 4GB cache for RAID 0, 1 and 5	BOO will check practically.
34	Rack Unit	Minimum 2U or higher rack unit (RU) configuration Appliance with Sliding Rails	BOO will check practically.
35	Redundancy & Business Continuity	Dedicated non-shared Redundant platinum rated AC power supplies on each of the proposed HCI appliance nodes and should be able to sustain single power supply failure per-node.	BOO will check practically and Firm will submit undertaking certificate.
36		Solution should be able to sustain one node failure per cluster.	
37		Solution should be able to sustain 1 NIC port failure per node.	
38		During a single component failure of any type in any node, production services should not be affected or degraded in anyway.	

Jo
2

A *to* *Amel* *H.* *2*

S.No	Description of Requirements	Trial Directives
39	Solution should be able to sustain multiple points of failure with no loss of functionalities or data.	
40	Availability of Data Store with zero RPO for all VMs is to be ensured in the event up to 2 Node failures for the stretch clusters at D3 domain.	
41	In the event of a Hard drive failure, appliance should not be affected and virtual machines should continue to run on the appliance. Drive replacement should be seamless to virtual machines hosted on the appliance.	
42	Solution should be able to sustain 2 SSD Disk failures per physical node, and 1 HDD failure simultaneously in each node of cluster across all nodes in cluster.	
43	Disaster Recovery Features	
44	The solution must provide a simple failover operation.	BOO will check practically and Firm will submit undertaking certificate.
45	The solution must allow changing of IP address of recovered Virtual Servers to match target data centre.	
46	The solution should allow changing Virtual Server settings (example vCPU, vRAM, vSwitch) if required.	
47	The solution must allow the option to test DR failover to separate network with no impact to production workloads.	
48	The solution should have feature to assist in failback process to Primary data centre.	
49	Hyper converged solution should have a guaranteed local cluster backup time of 1 minute.	
50	Data Protection should have a minimum RPO of 10 minutes for local backups.	
	Data recovery process should be simple with an RTO in minutes.	

Handwritten signature/initials

Handwritten signature/initials

S.No	Description of Requirements		Trial Directives
51	Manageability	The ability for a single administrator to manage all aspects of the Hyper-convergence from within the Virtualization Manager or server OEM browser based software for all sites.	BOO will check practically and Firm will submit undertaking certificate.
52		Globally manage Backup Policies per Data store or per VM.	
53		VM-centric management through a single pane of glass via the virtualization manager or server OEM browser based software.	
54		Programmatic/API interface to enable automated tasks like failover/failback.	
55		System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder.	
56		Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.	
57		System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support	
58	Scalability	Minimum scalability of 16 nodes in the same cluster.	BOO will check practically and Firm will submit undertaking certificate.
59		Hyper-converged solution must be able to allow in-box upgrade of CPU, RAM and storage capacity as well as scale-out expansion	
60		Hyper-converged solution should support addition of compute/access nodes to provide additional compute resources	

Handwritten signature/initials

Handwritten signature/initials

S.No	Description of Requirements		Trial Directives
61	Server Security	Should maintain repository for firmware and drivers recipes in the flash drive associated to management port. This is to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware	BOO will check practically and Firm will submit undertaking certificate.
62		For firmware security, Hyper converged system should support remote management chip creating a fingerprint in the silicon, preventing system from booting up unless the firmware matches the fingerprint. This feature should be immutable	
63		Directory services (AD/LDAP) compliance, CNSA compliance, HTML5 remote console, Workload Performance Advisor, Support for external key managers, Security Dashboard for assessment of important security features, the Overall Security Status for the system, and the current configuration for the Security State including Server Configuration Lock features	
64	OS Support	Windows 2012, 2016 and latest Standard/Data Centre, SUSE Enterprise Linux, RHEL 6.x, (All latest flavours of Linux and Windows) in Virtual Machines	BOO will check practically and Firm will submit undertaking certificate.
65	Serviceability	Proposed Nodes shall provide insights, forecasting and recommendations for quicker problem resolutions including automating case creation or alternate onsite solution on proactive support services with proactive parts dispatch directly from OEM.	
66	Warranty	On-site Comprehensive Warranty and Service including all spares, and service offering with NBD on-site for parts as well as telephone support 24 hours.	



S. N	Description of Requirements	Trial Directives
Following devices should provide with the system (Number will be decided by the user organization)		
1	Architecture (a) Shall be 19" Rack Mountable (b) The switch should have dual hot-swappable power supplies (c) Switch shall have minimum 24 x 1/10G SFP+ ports, populated with 8x10G SR, 8x1G SX and 8x1G BaseT transceiver. (d) 1 RJ-45 serial console port (e) 1 RJ-45 out-of-band management port (f) Should have minimum 2GB SDRAM and 512 MB flash and 32 MB or higher packet buffer size (g) Shall have switching capacity of minimum 480 Gbps (h) Shall have up to 350 million pps switching throughput (j) The Switch should support minimum 64000 MAC address.	BOO will check practically. Firm will submit OEM certificate.
2	Software Defined Networking (SDN) Capability (a) Open Flow protocol capability to enable software-defined networking	Firm will submit OEM certificate.
3	Features (a) The switch should support HTTP redirect function (b) 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	Firm will submit OEM certificate.
4	Quality of Service (QoS) (a) 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 (b) The switch should support Layer 4 prioritization to enable prioritization based on TCP/UDP port numbers (c) 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	Firm will submit OEM certificate.

Handwritten signatures and initials at the bottom of the page, including what appears to be 'JW', 'MP', and several other illegible marks.

S.N	Description of Requirements	Trial Directives
	(d) The switch should support Port-based rate limiting to provide per-port ingress-/egress-enforced increased bandwidth.	BOO will check practically and
	(e) 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.	Firm will submit OEM certificate.
	(f) The switch should support Reduced bandwidth to provide per-port, per-queue egress-based reduced bandwidth.	
	(g) 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.	
	(h) The switch should support Remote monitoring (RMON), Extended RMON (XRMON), and Flow v5 to provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events.	BOO will check practically.
	(j) The switch should support Traffic prioritization allows real-time traffic classification into eight priority levels that will mapped to eight queues.	BOO will check practically.
5	Management	
	(a) The switch should allow assignment of descriptive names to ports.	BOO will check practically.
	(b) The switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP).	BOO will check practically.
	(c) 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.	BOO will check practically.
	(d) The switch should support Multiple configuration files to store easily to the flash image.	BOO will check practically.
	(e) The switch should support Dual flash images to provide independent primary and secondary operating system files for backup while upgrading.	BOO will check practically.
	(f) 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.	BOO will check practically.
	(g) The switch should support Unidirectional Link Detection (UDLD).	BOO will check practically.

fw *M*

A *\$* *Qual* *dr* *dr*

S.N	Description of Requirements	Trial Directives
6	Connectivity	
	(a) The switch should support Jumbo frames on Gigabit Ethernet and 10-Gigabit Ethernet ports	BOO will check practically.
	(i) The switch should support following IPv6 feature	
	(a) IPv6 host: enables switch management in an IPv6 network.	Firm will submit OEM Certificate.
	(b) Dual stack (IPv4 and IPv6): transition IPv4 to IPv6, supporting connectivity for both protocols.	
	(c) MLD snooping: forward IPv6 multicast traffic to the appropriate interface.	
	(d) IPv6 ACL/QoS: support ACL and QoS for IPv6 traffic.	
	(e) IPv6 routing: support static, RIPng, OSPFv3 routing protocols.	
	(f) 6in4 tunneling: support encapsulation of IPv6 traffic in IPv4 packets.	
	(g) Security: provide RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping.	
7	Performance	
	(a) 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	BOO will check practically and Firm will submit OEM certificate.
	(b) The switch should support Energy-efficient Ethernet (EEE) support: reduces power consumption in accordance with IEEE 802.3az	
8	Resiliency and high Availability	
	(a) The Switch should support 9 Switch or more stacking and support up to 336 Gb/s of stacking throughput. The Switch support Ring, chain, and mesh stacking topologies. Stacking required from day-1.	BOO will check practically and Firm will submit OEM certificate.
	(b) The Switch should support Virtualized switching to provide simplified management as the switches appear as a single chassis when stacked.	
	(c) The switch should support Virtual Router Redundancy Protocol (VRRP).	
	(d) The switch should support Nonstop switching and routing.	



S. N	Description of Requirements	Trial Directives
	<p>(e) 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.</p> <p>(f) The switch should support IEEE 802.1s Multiple Spanning Tree.</p> <p>(g) 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.</p> <p>(h) The switch should provide easy-to-configure link redundancy of active and standby links.</p>	BOO will check practically and Firm will submit OEM certificate.
9	<p>Layer 2 switching</p> <p>(a) The switch should support IEEE 802.1ad QinQ</p> <p>(b) The switch should support VLAN and tagging and support the IEEE 802.1Q standard and 4096 VLANs simultaneously.</p> <p>(c) The switch should support IEEE 802.1v protocol VLANs.</p> <p>(d) The switch should support MAC-based VLAN.</p> <p>(e) The switch should support Rapid Per-VLAN Spanning Tree (RPVST+)</p> <p>(f) The Switch should dynamically load balances across multiple active redundant links to increase available aggregate bandwidth and allow concurrent Layer 3 routing</p> <p>(g) The switch should support GVRP and MVRP</p>	BOO will check practically and Firm will submit OEM certificate.
10	<p>Layer 3 Services</p> <p>(a) The switch should support Loopback interface address.</p> <p>(b) The switch should support Route maps.</p> <p>(c) The switch should support User datagram protocol (UDP) helper function.</p> <p>(d) The switch should support DHCP server.</p> <p>(e) The switch should support Bidirectional Forwarding Detection (BFD) to enable link connectivity monitoring and reduces network convergence time for static routing, OSPFv2, and VRRP.</p>	BOO will check practically and Firm will submit OEM certificate.
11	<p>Layer 3 routing - Should support from Day-1</p> <p>(a) The switch should support Static IP routing for both IPv4 and IPv6 networks</p> <p>(b) The switch should support OSPFv2 for IPv4 routing and OSPFv3 for IPv6 routing</p>	BOO will check practically and Firm will submit OEM certificate.

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements	Trial Directives
	(c) The switch should support Policy-based routing (d) The switch should support Border Gateway Protocol (BGP) (e) The switch should support RIPv1, RIPv2, and RIPv6 routing	BOO will check practically and Firm will submit OEM certificate.
12	Security (a) The switch should support Source-port filtering. (b) The switch should support RADIUS/TACACS+ (c) The switch should support Secure shell. (d) The switch should support Secure Sockets Layer (SSL). (e) The switch should support Port security. (f) The switch should support MAC address lockout. (g) The switch should support Detection of malicious attacks. (h) The switch should support Secure FTP. (j) The switch should support Switch management logon security. (k) 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 (l) The switch should support ICMP throttling. (m) The switch should support Identity-driven ACL. (n) The switch should support STP BPDU port protection. (o) The switch should support Dynamic IP lockdown. (p) The switch should support DHCP protection. (q) The switch should support Dynamic ARP protection. r) The switch should support STP root guard. (s) The Switch should secure management interfaces such as SNMP, Telnet, SSH, SSL, Web, and USB at the desired level. (t) The Switch should display a customized security policy when users log in to the switch. (u) The switch should support CPU protection. (v) 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. (w) The switch should support IEEE 802.1X (x) The switch should support Web-based authentication. (y) The switch should support MAC-based authentication.	BOO will check practically and Firm will submit OEM certificate.

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements	Trial Directives	
	(z) Authenticates client with the RADIUS server based on client's MAC address.	BOO will check practically and Firm will submit OEM certificate.	
	(aa) The switch should support Concurrent authentication modes to enables a switch port to accept up to 32 sessions of 802.1X, Web and MAC authentication.		
	(ab) The switch should support Private VLAN.		
13	Convergence		
	(a) The switch should support IP multicast snooping (data-driven IGMP).	BOO will check practically and Firm will submit OEM certificate.	
	(b) The switch should support LLDP-MED (Media Endpoint Discovery).		
	(c) The switch should support IP multicast routing including PIM sparse and dense modes to route IP multicast traffic.		
	(d) The switch should support Auto VLAN configuration for voice.	BOO will check practically and Firm will submit OEM certificate.	
	(e) The switch should support RADIUS VLAN.		
	(f) 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		
	(a) Shall support IEEE 802.3az Energy-efficient Ethernet (EEE) to reduce power consumption.	Firm will submit certificate of Govt. Lab. or NABL/ILAC accredited laboratory.	
	(b) Operating temperature of 0°C to 45°C		
	(c) Safety and Emission standards including EN 60950; IEC 60950; VCCI Class A; FCC Class A		
15	Warranty and Support		
	(a) The below Warranty shall be offered directly from the switch OEM.	Firm will submit OEM certificate.	
	(b) Software upgrades/updates shall be included as part of the warranty.		
	Following devices should provide with the system (Number will be decided by the user organization)		
1	Chassis	1U Rack Mountable	BOO will check practically.
2	CPU	2 x Intel Bronze Processor 3204	
3	Memory	16 DIMM slots. 2x 32 GB	
4	Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance	

Handwritten signature/initials

Handwritten signature/initials

S.N	Description of Requirements		Trial Directives
5	HDD Bays	Up to 8 HDD Bays The drive carrier should have intuitive icon based display along with "DO NOT REMOVE" caution indicator that gets activated automatically in order to avoid data loss/downtime due to wrong drive removal.	BOO will check practically.
6	Hard disk drive	2 x1.2 TB SAS 10K RPM	
7	Controller	Hard Controller Should SUPPORT RAID 0.1 5.	
8	Networking features	Server should support below networking cards: 1. 1Gb 4-port network adaptors 2. 10Gb 2-port Ethernet adaptor 3. 10GBaseT 4-port Ethernet adaptor 4. 4x25Gb Ethernet adaptor 5. 10/25Gb 2-port Ethernt adaptor 6. 100Gb Ethernet Infiniband Options: 40Gb dual port or 100Gb Single or Dual port Adapter 100Gb Single port Omni path adaptor Also 1G x dual Port Should be Provided from Day 1	
9	Interfaces	Serial - 1, Micro SD slot - 1, USB 3.0 support With Up to 4 total: 1 front, 1 internal, 2 rear	
10	Bus Slots	Two PCI-Express 3.0 slots, at least one x16 PCIe slots	
11	Power Supply	Should support hot plug redundant low halogen power supplies minimum 2 x 500 Watt	
12	Fans	Redundant hot-plug system fans	
13	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support Energy Star ASHRAE A3/A4 UEFI 2.6 SMBIOS Redfish API SNMP v3 TLS 1.2 DMTF Systems Management Architecture	

Mr

A B Doe

S. N	Description of Requirements		Trial Directives
14	System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Support for Commercial National Security Algorithms (CNSA) Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Tamper free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 TPM (Trusted Platform Module) 2.0 Smart card (PIV/CAC) and Kerberos based 2-factor Authentication Configurable for PCI DSS compliance Chassis Intrusion detection.	BOO will check practically.
15	System tuning for performance	1. System should support feature for improved workload throughput for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode "ON" without the frequency fluctuations associated with running in turbo mode. 2. System should support workload Profiles for simple performance optimization	BOO will check practically.
16	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.	BOO will check practically.
17	Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable. 2. Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware	BOO will check practically.

Handwritten signature/initials

Handwritten signature/initials

6. NETWORK TRAFFIC MANAGER

S.N	Description of Requirements	Trial Directives				
BANDWIDTH CONTROLLER						
An additional device for bandwidth control should be provided along with the system. The features are as follows.						
1	<table border="1"> <tr> <td data-bbox="300 456 501 1025">General Features</td> <td data-bbox="501 456 1252 1025"> <p>(i) The system should ensure reliable performance for network dependent applications.</p> <p>(ii)The system should reduce the impact of non-strategic traffic, and diagnose and resolve network problems</p> <p>(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.</p> <p>(iv) The system should have the feature to easily monitor recreational traffic like video streaming and P2P sharing.</p> </td> </tr> <tr> <td data-bbox="300 1025 501 1841">Technical Features</td> <td data-bbox="501 1025 1252 1841"> <p>(i) Real-time Monitoring: 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</p> <p>(ii) Policy-Based Shaping: The system should have the feature to prioritize how and when users, applications and websites can consume bandwidth on network.</p> <p>(iii) Interactive Analytics: Intuitive dashboard feature should be there to visualize activities by all users.</p> <p>(iv) Application Acceleration: The system should support acceleration and caching features.</p> <p>(v) Predictive Recommendations: 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.</p> </td> </tr> </table>	General Features	<p>(i) The system should ensure reliable performance for network dependent applications.</p> <p>(ii)The system should reduce the impact of non-strategic traffic, and diagnose and resolve network problems</p> <p>(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.</p> <p>(iv) The system should have the feature to easily monitor recreational traffic like video streaming and P2P sharing.</p>	Technical Features	<p>(i) Real-time Monitoring: 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</p> <p>(ii) Policy-Based Shaping: The system should have the feature to prioritize how and when users, applications and websites can consume bandwidth on network.</p> <p>(iii) Interactive Analytics: Intuitive dashboard feature should be there to visualize activities by all users.</p> <p>(iv) Application Acceleration: The system should support acceleration and caching features.</p> <p>(v) Predictive Recommendations: 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.</p>	BOO will check practically and Firm will submit OEM certificate.
General Features	<p>(i) The system should ensure reliable performance for network dependent applications.</p> <p>(ii)The system should reduce the impact of non-strategic traffic, and diagnose and resolve network problems</p> <p>(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.</p> <p>(iv) The system should have the feature to easily monitor recreational traffic like video streaming and P2P sharing.</p>					
Technical Features	<p>(i) Real-time Monitoring: 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</p> <p>(ii) Policy-Based Shaping: The system should have the feature to prioritize how and when users, applications and websites can consume bandwidth on network.</p> <p>(iii) Interactive Analytics: Intuitive dashboard feature should be there to visualize activities by all users.</p> <p>(iv) Application Acceleration: The system should support acceleration and caching features.</p> <p>(v) Predictive Recommendations: 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.</p>					

Handwritten signature/initials

Handwritten signature/initials

S.No	Description of Requirements	Trial Directives
	<p>(vi) QX Boost for Skype Application: 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.</p>	BOO will check practically.
Hardware Features	<p>(i) Traffic shaping and Acceleration</p>	BOO will check practically and Firm will submit OEM certificate.
	(a) Shaping Throughput: - 1 Gbps	
	(b) Concurrent Flows: - 220,000	
	(c) Packets per second: - 200,000/s	
	(d) New Connection Rates: - 10,000/s	
	(e) Acceleration Throughout: - 30 Mbps	
	(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	
	<p>(ii) Interface Capability</p>	
	<p>(a) The system should have 1 x RJ45 based dedicated console port for management purpose.</p> <p>(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.</p>	
	<p>(iii) Physical Parameters</p>	
(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.	Firm will submit certificate of Govt. Lab. or NABL/ILAC accredited laboratory.	

to 2 M

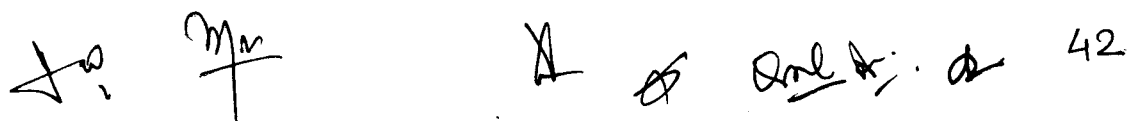
49 One * 4 40

S.N	Description of Requirements	Trial Directives																								
Following devices should provide with the system (Number will be decided by the user organization)																										
	<table border="1"> <tr> <td data-bbox="320 320 603 365">Speech band</td> <td data-bbox="603 320 1204 365">300 to 3400 Hz</td> </tr> <tr> <td data-bbox="320 365 603 409">Modulation</td> <td data-bbox="603 365 1204 409">Pulse Code Modulation</td> </tr> <tr> <td data-bbox="320 409 603 499">No. of channels per system</td> <td data-bbox="603 409 1204 499">32 (30 speech channels, 1 terminal Signaling and 1 Sync. Channel)</td> </tr> <tr> <td data-bbox="320 499 603 566">Sampling frequency</td> <td data-bbox="603 499 1204 566">8000 Hz</td> </tr> <tr> <td data-bbox="320 566 603 645">No of sample bits</td> <td data-bbox="603 566 1204 645">8 per channel</td> </tr> <tr> <td data-bbox="320 645 603 689">Total bits per</td> <td data-bbox="603 645 1204 689">256</td> </tr> <tr> <td data-bbox="320 689 603 734">Bit rate</td> <td data-bbox="603 689 1204 734">2048 Kbps \pm 50 ppm</td> </tr> <tr> <td data-bbox="320 734 603 891">Construction and Architecture</td> <td data-bbox="603 734 1204 891">Chassis based modular multiplexer shelf capable of supporting minimum 12 slots for integration of data, voice, fax and LAN traffic.</td> </tr> <tr> <td data-bbox="320 891 603 1081">Universal Slots</td> <td data-bbox="603 891 1204 1081">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> <tr> <td data-bbox="320 1081 603 1305">Add-Drop or Drop - Insert Function</td> <td data-bbox="603 1081 1204 1305">(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.</td> </tr> <tr> <td data-bbox="320 1305 603 1753">Digital Cross Connect function</td> <td data-bbox="603 1305 1204 1753">(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</td> </tr> <tr> <td data-bbox="320 1753 603 1836">Redundancy</td> <td data-bbox="603 1753 1204 1836">Dual controller, dual power with load sharing</td> </tr> </table>	Speech band	300 to 3400 Hz	Modulation	Pulse Code Modulation	No. of channels per system	32 (30 speech channels, 1 terminal Signaling and 1 Sync. Channel)	Sampling frequency	8000 Hz	No of sample bits	8 per channel	Total bits per	256	Bit rate	2048 Kbps \pm 50 ppm	Construction and Architecture	Chassis based modular multiplexer shelf capable of supporting minimum 12 slots for integration of data, voice, fax and LAN traffic.	Universal Slots	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.	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	Redundancy	Dual controller, dual power with load sharing	BOO will check practically and Firm will submit OEM certificate.
Speech band	300 to 3400 Hz																									
Modulation	Pulse Code Modulation																									
No. of channels per system	32 (30 speech channels, 1 terminal Signaling and 1 Sync. Channel)																									
Sampling frequency	8000 Hz																									
No of sample bits	8 per channel																									
Total bits per	256																									
Bit rate	2048 Kbps \pm 50 ppm																									
Construction and Architecture	Chassis based modular multiplexer shelf capable of supporting minimum 12 slots for integration of data, voice, fax and LAN traffic.																									
Universal Slots	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.																									
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																									
Redundancy	Dual controller, dual power with load sharing																									

Handwritten signature

Handwritten signature

S.N	Description of Requirements		Trial Directives
	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/24FXS 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	BOO will check practically and Firm will submit OEM certificate.
	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	



S.N	Description of Requirements	Trial Directives														
	<p><u>2* 10/100 Ethernet Router Card with capability to handle 64 WANs should comply with the following specifications</u></p> <table border="1"> <tr> <td data-bbox="331 443 539 584">Number of ports</td> <td data-bbox="539 443 1206 584">2 LAN ports, Max. 64 WAN ports, Each WAN port has data rate $n \times 64K$ bps, $1 \leq n \leq 32$ ($\leq 4Mbps$ for total of all 64 WAN ports)</td> </tr> <tr> <td data-bbox="331 584 539 667">Physical Interface</td> <td data-bbox="539 584 1206 667">10/100 BaseT x 2</td> </tr> <tr> <td data-bbox="331 667 539 707">Connector</td> <td data-bbox="539 667 1206 707">RJ45</td> </tr> <tr> <td data-bbox="331 707 539 790">Routing protocol</td> <td data-bbox="539 707 1206 790">RIP-I, RIP-II, OSPF, Static</td> </tr> <tr> <td data-bbox="331 790 539 898">Supporting Protocols</td> <td data-bbox="539 790 1206 898">PPP (IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT, DHCP</td> </tr> <tr> <td data-bbox="331 898 539 940">Diagnostic</td> <td data-bbox="539 898 1206 940">Ping, Trace route</td> </tr> <tr> <td data-bbox="331 940 539 981">QoS</td> <td data-bbox="539 940 1206 981">Rate limit</td> </tr> </table>	Number of ports	2 LAN ports, Max. 64 WAN ports, Each WAN port has data rate $n \times 64K$ bps, $1 \leq n \leq 32$ ($\leq 4Mbps$ for total of all 64 WAN ports)	Physical Interface	10/100 BaseT x 2	Connector	RJ45	Routing protocol	RIP-I, RIP-II, OSPF, Static	Supporting Protocols	PPP (IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT, DHCP	Diagnostic	Ping, Trace route	QoS	Rate limit	BOO will check practically and Firm will submit OEM certificate.
Number of ports	2 LAN ports, Max. 64 WAN ports, Each WAN port has data rate $n \times 64K$ bps, $1 \leq n \leq 32$ ($\leq 4Mbps$ for total of all 64 WAN ports)															
Physical Interface	10/100 BaseT x 2															
Connector	RJ45															
Routing protocol	RIP-I, RIP-II, OSPF, Static															
Supporting Protocols	PPP (IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT, DHCP															
Diagnostic	Ping, Trace route															
QoS	Rate limit															
	<p><u>8* 10/100 Ethernet Router Card with capability to handle 64 WANs</u></p> <table border="1"> <tr> <td data-bbox="331 1064 539 1171">Number of ports</td> <td data-bbox="539 1064 1206 1171">8 LAN ports, Max. 64 WAN ports. Each WAN port has data rate $n \times 64K$ bps.</td> </tr> <tr> <td data-bbox="331 1171 539 1254">Physical Interface</td> <td data-bbox="539 1171 1206 1254">10/100 BaseT x 8</td> </tr> <tr> <td data-bbox="331 1254 539 1294">Connector</td> <td data-bbox="539 1254 1206 1294">RJ45</td> </tr> <tr> <td data-bbox="331 1294 539 1377">Routing protocol</td> <td data-bbox="539 1294 1206 1377">RIP-I, RIP-II, OSPF, Static</td> </tr> <tr> <td data-bbox="331 1377 539 1485">Supporting Protocols</td> <td data-bbox="539 1377 1206 1485">PPP (IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT, DHCP</td> </tr> <tr> <td data-bbox="331 1485 539 1527">Diagnostic</td> <td data-bbox="539 1485 1206 1527">Ping, Trace route</td> </tr> <tr> <td data-bbox="331 1527 539 1576">QoS</td> <td data-bbox="539 1527 1206 1576">Rate limit</td> </tr> </table>	Number of ports	8 LAN ports, Max. 64 WAN ports. Each WAN port has data rate $n \times 64K$ bps.	Physical Interface	10/100 BaseT x 8	Connector	RJ45	Routing protocol	RIP-I, RIP-II, OSPF, Static	Supporting Protocols	PPP (IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT, DHCP	Diagnostic	Ping, Trace route	QoS	Rate limit	BOO will check practically and Firm will submit OEM certificate
Number of ports	8 LAN ports, Max. 64 WAN ports. Each WAN port has data rate $n \times 64K$ bps.															
Physical Interface	10/100 BaseT x 8															
Connector	RJ45															
Routing protocol	RIP-I, RIP-II, OSPF, Static															
Supporting Protocols	PPP (IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT, DHCP															
Diagnostic	Ping, Trace route															
QoS	Rate limit															

Jo *Mr*

*1 of 2nd * 2*

S.N	Description of Requirements	Trial Directives
Voice Card (SEM) port (interfaces) should comply with the following specifications:-		
	(a) Connector: RJ45 connector (b) Alarm conditioning: CGA busy after 2.5 seconds of LOS ,LOF (c) Encoding: a low or u low user selectable together for all. (d) Impedance: balanced 600 or 900 ohms. (e) Longitudinal rejection : 55 dB (f) Loss adjustment : -21 to +10 dB/0.1dB step transmit and receive (g) Single/ distortion: >46 dB with 1004 Hz, 0 dBm input (h) Frequency response: -0.25 to-1 dB from 300 to 3400Hz (j) Signaling : Type 1,Type 2,Type 3,Type 4,Type 5 transmit only	BOO will check practically and Firm will submit OEM certificate.
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 / 0.1dB step transmit & receive (j) Signal/ Distortion : > 25dB with 1004 Hz, 0dBm input (k) Frequency Response : - 0.25 to -1 dB from 300 to 3400 Hz, coincide with ITU-T G.712 (l) Loss adjustment: -21 to +10 dB/ 0.1 dB step transmit and receive (m) Signal / Distortion:. 46 dB with 1004 Hz , 0dBm input (n) Frequency response: - 0 .25 to -1 dB from 300 to 3400 Hz , coincide with ITU-T. (o) Ideal channel noise : Max -65 dB Mop (p) Inter- modulation : coincide with ITU-T B.712	BOO will check practically and Firm will submit OEM certificate.

J₂ *M₂*

V. S. Sule

S.N	Description of Requirements	Trial Directives
	(q) 2Wire return loss : > 2 dB echo , > 20 dB signing (r) FXS loop feed : Nominal -48 V dc with 20 mA current limit (s) Signaling : Loop Start, DTMF, pulse, PLAR, Battery Reverse	BOO will check practically and Firm will submit OEM certificate.
G.SHDSL Line port (interfaces) should comply with the following		
Number of ports	2 or 4	BOO will check practically and Firm will submit OEM certificate.
Line Rate for 4-channel G.shdsl	n x 64Kbps (n= 3 to 31)	
Line Rate for 2-channel G.shdsl	n x 64Kbps (n= 3 to 15)	
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		
Combo Gigabit Ethernet (GbE) Interface	-> Number of Ports 2 -> Speed 10/100/1000M bps -> Connector RJ45 for twisted pair GbE, LC for optical GbE, auto detection	BOO will check practically and Firm will submit OEM certificate.
Gigabit Ethernet (GbE) Interface	-> Number of Port 2 -> Speed 10/100/1000 BaseT -> Connector RJ45	
Ethernet Function	MDI/MDIX for 10/100/1000M BaseT auto-sensing Ping function contained ARP Per port, programmable MAC hardware address learn limiting (max. MAC table 8192 (8k) entry)	



S.N	Description of Requirements		Trial Directives
Basic Features:			
Packet Transparency	Packet transparency support for all types of packet types including IEEE 802.1q VLAN and 802.1ad (Q-in-Q)	BOO will check practically and Firm will submit OEM certificate.	
QoS	User configurable 802.1p CoS, ToS in outgoing IP frame.		
Traffic Control	(a) Ingress packet Rate limiting buckets per port for Ethernet port (b) Supporting Rate-based and Priority-based rate limiting for LAN port. (c) Pause frame issued when the traffic exceeding the limited rate before packet dropped following IEEE802.3X		
Link Aggregation	WAN support link aggregation		
Jitter & Wander	PPM: per G.823 Traffic PPB: per G.823 Synchronous*		
Standard Compliance			
IETF	TDMoIP (RFC5087), SAToP (RFC4553), CESoPSN (RFC5086)	Firm will submit OEM certificate.	
IEEE	802.1q, 802.1p, 802.1d, 802.3, 802.3u, 802.3x, 802.3z, 802.1s, 802.1w, 802.1AX		
Co-directional port (interfaces) should comply with the following specifications :-			
Interface	ITU G.703 64 Kbps co-directional interface	BOO will check practically and Firm will submit OEM certificate.	
Connector	120ohm, RJ48		
Line Distance	Up to 500 meters		
Loopback	DTE Payload Loopback, Local Loopback		

Handwritten marks: A checkmark and a signature-like scribble.

Handwritten notes: A checkmark, a circled 'X', and some illegible scribbles.

S. N	Description of Requirements		Trial Directives
Voice Card 12 MAG (Magneto)			
	(a) Connector : Twelve RJ11 (b) Alarm Conditioning CGA busy after 2.5 seconds of LOS, LOF. (a) Encoding A-law or μ -law, user selectable together for all. (b) Impedance Balanced 600 or magneto telephone impedance match. (c) Longitudinal Conversion Loss > 46dB. (d) Gain Adjustment -21 to +10 dB / 0.1dB step transmit & receive. (e) Signal/ Distortion > 25dB with 1004 Hz, 0dBm input. (f) Frequency Response - 0.25 to -1 dB from 300 to 3400 Hz, coincide with ITU-T G.712. (g) Idle Channel Noise Max. -65 dBmOp. (h) Min Detectable Ringing Voltage 16 Vrms. (i) Ringing Detectable Across L1 and L2 (Tip and Ring), L1 and GND (Tip and GND) (j) Single Ring Type: ring for 2 sec. and stop, or ring for 4 sec. and stop. (k) Continuous Ring Type: 1 sec on 2 sec off, or 2 sec on 4 sec off (l) Ringing Send across L1 and L2 (Tip and Ring), L1 and GND (Tip and GND). (m) Signaling Magneto MRD (Ringing across Tip and Ring or Tip and Ground). (n) Signaling Bit A, B, C, D Programmable. (o) Signaling is carried transparently by the digitizing process.		BOO will check practically and Firm will submit OEM certificate.
C	Clock Source	Internal, E1/T1 Line, External	BOO will check practically and Firm will submit OEM certificate.
D	Alarm Relay	Alarm Relay: max. Voltage 3 Vdc/ max. current: 1A Fuse alarm, and performance alarm	BOO will check practically and Firm will submit OEM certificate.


 A series of handwritten signatures and initials in black ink, including a large 'J', a signature that appears to be 'M', and several other initials and marks.

S.N	Description of Requirements			Trial Directives
E	System Configuration Parameters	Active Configuration, Configuration, and Configuration	Stored Default	BOO will check practically and Firm will submit OEM certificate.
F	Supervisor			
	RS232 Console Port (VT100)	10 Base-T, Ethernet, In-band 64 supports HDLC/PPP, SSH	SNMP Kbps	BOO will check practically and Firm will submit OEM certificate
G	Performance Monitor			
	Separate Registers	Network, user, and remote site		BOO will check practically and Firm will submit OEM certificate.
	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 & time		
H	Diagnostics			
	Loopback	E1/T1 interface (Line Loopback, Payload Loopback, Local Loopback), DTE Loopback (DTE-to-DTE, DTE to Line)		BOO will check practically and Firm will submit OEM certificate.
	Test Pattern	For Controller: 221-1, 215-1, 211-1, 29-1, and 4-byte user define pattern		
J	Front Panel			
	LED	1 per V.35-interface, ACO, Power, SYNC/TEST, LOF, BPV, RAI/AIS		BOO will check practically and Firm will submit OEM certificate.

to *g*

V *\$* *One* *+* *de*

S.N	Description of Requirements		Trial Directives
K	Physical / Electrical		BOO will check practically and Firm will submit OEM certificate. Firm will submit certificate of Govt. Lab. or NABL/ILAC accredited laboratory. BOO will check practically.
	Dimensions	432.4 x 220 x 223.5 mm (W×H×D)	
	Power	Single/ Dual -48 Vdc: -36 to -75 Vdc, 100 Watts max.	
		Single/ Dual -48 Vdc: -36 to -75 Vdc, 150 Watts max.	
		Single/ Dual -24 Vdc: -18 to -36 Vdc, 150 Watts max	
	Temperature	0°C -55°C	
	Humidity	0-95%RH (non-condensing)	
	Mounting	Desk-top stackable, 19" /23" rack mountable	
Line Power supply	Available only with DC power for G.SHDSL card only		
Power Consumption	Max 110 Watts		
The OEM should have authorized R & D & Repair/Replacement center in India with presence in India of about 10 Years		Firm will submit OEM certificate.	
L	Certification	EN55022 Class A, EN50024, FCC Part 15 ,Class A, FCC Part 68, CS-03, IEC60950, UL60950, IEC 61850-3, IEEE 1613	Firm will submit OEM certificate.
M	Compliance	ITU G.703, G.704, G.706, G.732, G.736, G.823, G.826, G.711, G.712, G.775, O.151, V.11, V.28, V.54	
N	Card Configuration required as part of supply.		BOO will check practically.
		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		
O	DC Power Source (-48V)	(a) Input 230 VAC (Range 170-264 VAC, single phase, 50 Hz).	
		(b) Output Current :- 8 Amp	
		(c) Size: - 485(W) x385(D) x165(H) mm with screw terminals at front	
		(d) Should have short circuit protection.	

Handwritten signature/initials

Handwritten signature/initials 49

7. 24" MONITOR

S.No	Description of Requirements	Trial Directives
1.	Screen Size: 24 inch Full HD (1920 X 1080) IPS Panel	BOO will check practically and Firm will submit OEM certificate.
2.	Connectivity Port: 1 VGA Port, 1 HDMI Port	
3.	Aspect Ratio: 16:9, Brightness (Typical): 250 cd/m ²	
4.	Number of Colour: 16.7 m Colours	
5.	Refresh Rate: 60 Hz (Analog),	
6.	Response Time: 4 ms	
7.	Viewing Angle: 178-degree horizontal 178-degree vertical	

8. KEYBOARD & MOUSE

S.No	Description of Requirements	Trial Directives
1.	104 Keys USB keyboard	BOO will check practically.
2.	2 Button USB Optical Scroll Mouse	
3.	The Keyboard and Mouse should be from the same OEM.	

INTRUSION & FIREWALL

1. UNIFIED THREAD MANAGEMENT

S.No	Description of Requirements	Trial Directives
General Requirements		
1	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.	Firm will submit OEM certificate.
2	The proposed vendor must have successfully completed NSS Labs' NGFW Methodology v8.0 testing with a minimum exploit blocking rate of 99%	
3	OEM should be in Leaders quadrant of Gartner's - in Enterprise Firewall Magic Quadrant (or equivalent) as per the latest report	
4	Appliance shall be EAL4 and ICSA certified for Firewall	Firm will submit certificate of Govt. Lab. or NABL/ILAC accredited laboratory.

Handwritten signature/initials

Handwritten signature/initials 50

S.No	Description of Requirements	Trial Directives
<u>Hardware & Interface requirements</u>		
1	The platform must be supplied with minimum 10 x GE RJ45 inbuilt interfaces & 4 x GE SFP interface slots from day one.	BOO will check practically.
2	The Appliance should have USB & Console Ports.	
<u>Performance and Availability</u>		
1	The Firewall should be on multiprocessor architecture with minimum 5Gbps (or more as per user requirement) of Firewall throughput & support of 1,500,000 concurrent sessions, and 130,000 new sessions per second from day one & latency should not be more than 3 μ s	BOO will check practically and Firm will submit OEM certificate.
2	Minimum IPS throughput of 2000 Mbps for real world traffic or enterprise mix traffic	
3	Minimum SSL Inspection Throughput of 500 Mbps	
4	Minimum Threat Prevention Throughput (measured with Application Control and IPS and Anti-Malware enabled) of 1000 Mbps for real world traffic or enterprise mix traffic.	
5	IPSec VPN throughput: minimum 5 Gbps	
6	Simultaneous Client-to-Site IPSec VPN tunnels: 300	
7	Proposed solution must support minimum 300 SSL VPN users from day one	
8	Proposed solution must support minimum 10 virtual firewall from day one	
<u>Routing Protocols</u>		
1	Static Routing	BOO will check practically and Firm will submit OEM certificate.
2	Policy Based Routing	
3	The Firewall should support dynamic routing protocol like RIP, OSPF, BGP, ISIS	
<u>Firewall Features</u>		
1	Firewall should provide application inspection for LDAP, SIP, H.323, SNMP, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, IMAP, NFS etc.	BOO will check practically and Firm will submit OEM certificate.
2	IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP	
3	Allows secure deployment of next-generation IPv6 networks, as well as hybrid environments that require simultaneous, dual stack support of IPv4 and IPv6	

Aw *Mr*

4 *\$* *One* *Ar* *de*

S.No	Description of Requirements	Trial Directives	
4	The firewall should support transparent (Layer 2) firewall or routed (Layer 3) firewall Operation	BOO will check practically and Firm will submit OEM certificate.	
5	The Firewall should support ISP link load balancing for outbound traffic & also should support SDWAN functionality for future scalability		
6	Firewall should support link aggregation functionality to group multiple ports as single port.		
7	Firewall should support minimum VLANS 2048		
8	Firewall should support static NAT, policy based NAT and PAT		
9	Firewall should support IPSec data encryption		
10	It should support the IPSec VPN for both site-site and remote access VPN		
11	Firewall should support IPSec NAT traversal.		
12	control SNMP access through the use of SNMP and MD5 authentication.		
13	Firewall system should support virtual tunnel interfaces to provision route-based IPSec VPN		
14	The Firewall should have integrated solution for SSL VPN & both IPSec & SSL VPN functionality should be ICSA certified		
15	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		
16	The solution should have basic server load balancing functionality as an inbuilt feature		
Integrated IPS Features Set			
1	IPS should have DDoS and DoS anomaly detection and protection mechanism with threshold configuration.		BOO will check practically and Firm will submit OEM certificate.
2	Support SYN detection and protection for both targets and IPS devices.		
3	The device shall allow administrators to create Custom IPS signatures		
4	Should have a built-in Signature and Anomaly based IPS engine on the same unit		
5	Signature based detection using real time updated database & should have minimum 10000+ IPS signature database from day one		

AS *M*

✓ *CS* *Done* *12*

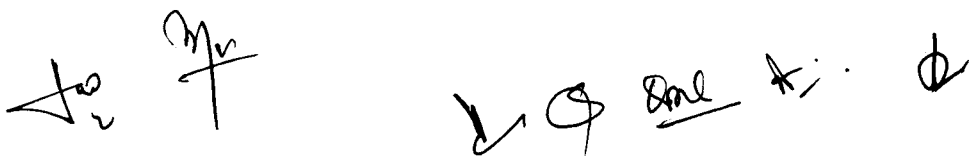
S.No	Description of Requirements	Trial Directives
6	Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)	BOO will check practically and Firm will submit OEM certificate.
7	Signature updates do not require reboot of the unit.	
8	Configurable IPS filters to selectively implement signatures based on severity, target (client/server) and operating systems	
9	IPS Actions: Default, monitor, block, reset, or quarantine	
10	Should support packet capture option	
11	IP(s) exemption from specified IPS signatures	
12	IPS should be ICSA Certified & should be recommended by NSS Labs	
Anti Virus & Anti Bot		
1	Firewall should support antimalware capabilities , including antivirus, botnet traffic filter and antispysware	BOO will check practically and Firm will submit OEM certificate.
2	Solution should be able to detect and prevent unique communication patterns used by BOTs i.e. information about botnet family	
3	Solution should be able to block traffic between infected host and remote operator and not to legitimate destination	
4	Should have antivirus protection for protocols like HTTP, HTTPS, IMAPS, POP3S, SMTPS protocols etc.	
5	Solution should have an option of packet capture for further analysis of the incident	
6	Solution should uncover threats hidden in SSL links and communications	
7	The AV should scan files that are passing on CIFS protocol	
8	The proposed system shall provide ability to allow, block attachments or downloads according to file extensions and/or file types	
9	The proposed system should provide cloud based sandboxing solution from day one to prevent from zero day threats	
10	The gateway Anti-Virus functionality should be ICSA certified	

to

M/W

V S Sol # 2

S.No	Description of Requirements	Trial Directives
	<u>Other support</u>	
1	Should support features like Web-Filtering, Application-Control & Gateway level DLP from day one	BOO will check practically and Firm will submit OEM certificate.
2	The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should support over 2 billion WebPages in 72+ categories and 68+ languages without external solution, devices or hardware modules.	
3	Should support detection over 4,000+ 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)	
4	The solution should have the flexibility to write security policies based on IP Address & User Name & Endpoint Operating System	
5	The product must supports Layer-7 based Firewall virtualization, and all Firewall features should be supported in each virtual firewall like Threat Prevention, IPS, Web filter, Application Control, content filtering etc.	
6	QoS features like traffic prioritization, differentiated services,. Should support for QoS features for defining the QoS policies.	
7	It should support the VOIP traffic filtering	
8	Appliance should have identity awareness capabilities	
9	The firewall must support Active-Active as well as Active-Passive redundancy.	
10	Solution must support VRRP clustering protocol.	
	<u>Management & Reporting functionality</u>	
1	Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI.	BOO will check practically and Firm will submit OEM certificate.
2	Support accessible through variety of methods, including console port, Telnet, and SSHv2	



S.No	Description of Requirements	Trial Directives
3	Support for both SNMPv2 and SNMPv2c, providing in-depth visibility into the status of appliances.	BOO will check practically and Firm will submit OEM certificate.
4	Should have capability to import configuration and software files for rapid provisioning and deployment using Trivial File Transfer Protocol (TFTP), HTTP, HTTPS	
5	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	
6	The Firewall appliance should have minimum 450GB of internal storage for logging & reporting functionalities	
7	Solution must allow administrator to choose to login in read only or read-write mode	

2. FIREWALL LOG ANALYZER

S.N	Description of Requirements	Trial Directives
1	The solution should have a separate appliance for storing logs & generating reports centrally for all connected Firewalls of the same OEM & should have minimum capacity of connecting 30 Firewalls	BOO will check practically and Firm will submit OEM certificate.
2	The proposed centralized logging & reporting solution should have a capacity of accepting minimum 200GB logs per day & a total storage capacity of 12TB.	
3	The solution should have support for RAID 0/1/5/10	
4	The reporting solution should have customizable interactive dashboard to rapidly pinpoint problems	
5	It should support drill-down to follow the trail of an attacker, trace transactions and gain new insights	
6	It should have minimum 25+ built-in templates with sample reports ready for use	
7	The solution should support to run report on-demand or on a schedule with automated email notification and Calendar view	
8	It should support customization with 300+ built-in charts ready for generating custom reports	
9	The solution should provide flexible report formats like HTML/CSV/XML/PDF	
10	It should support retrieving of archived logs to perform analytics against historic data	
11	The solution should support forwarding of logs to a Syslog server or a CEF log server for long-term storage, forensics or regulatory compliance	


55

3. FIREWALL POLICY MANAGER

S.N	Description of Requirements	Trial Directives
1	The solution should have a centralized management appliance for managing minimum 30 Firewall appliances of the same OEM from a single console	BOO will check practically and Firm will submit OEM certificate.
2	The management solution can collectively configure the device settings, objects and policies across the network from a single user interface	
3	The management solution can review, approve and audit policy changes from a central place	
4	It should support automated process to facilitate policy compliance and policy lifecycle management	
5	Should support enforcing workflow to reduce risk for policy changes	
6	The centralized management solution should support for: Application Control and Intrusion Prevention updates, Vulnerability Management, Antivirus and Web Filtering updates to all the connected Firewall appliances from a single console	
7	It should support for RESTful API which allows to create customized, branded web portals for policy and object administration	
8	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	
9	The solution should support ensuring common security baseline to be enforced and shared among multiple administrative domains (ADOMs).	

C. CYBER FORENSIC

1. Data Analysis Tool

S.N	Description of Requirements	Trial Directives
1.	Ability to automatically queue multiple acquisition and processing actions - to increase efficiencies and save time.	BOO will check practically and Firm will submit OEM certificate.
2.	End-to-end experience that brings together acquisition, processing and analysis, creating integration and a more navigable and manageable digital evidence database.	BOO will check practically and Firm will submit OEM certificate.

Ad Mr

Boo

S.N	Description of Requirements	Trial Directives
3.	Support for a broad array of artifact types, and support for the latest versions of those apps and artifact types.	BOO will check practically and Firm will submit OEM certificate.
4.	Access to file system, registry and artifacts data and trace artifact evidence to its source data efficiently for a better verification process.	
5.	The ability to present findings in a customizable way that fits their report needs and parameters.	
6.	Acquire images from any iOS or Android device, hard drives, and removable media.	
7.	Recovers evidence from 300+ types of Internet Artifacts from Windows and Mac computers.	
8.	Recovers 165+ types of Smartphone Artifacts from iOS, Android, and Windows Phone powered smart phones and tablets.	
9.	Get to relevant evidence faster using filters. Isolate evidence from a specific date or time range, or create filters to narrow results based on field values for any supported artifact type. Filter stacking allows you to layer on several dimensions of filter criteria to pinpoint specific items in a large dataset.	
10.	Create and manage a number of different tags to help you narrow down the results quickly and begin to see patterns in an individual's activity. Using the comments function, identify and share your thoughts with other key stakeholders. You can also create profiles that are associated with an individual and then associate other identifiers (email addresses, phone numbers, etc) with the profile, so that you can filter evidence to show only the evidence associated with the individual.	
11.	Create your own custom artifact definitions to find more artifact data or have Evidence Analyzer's Dynamic App Finder automatically identify new apps and create artifact definitions which can then be saved for future use.	
12.	Recovers more artifacts from both allocated and unallocated space by extracting data from full files or carving for deleted data and traces of data elements/fragments left behind by apps and websites, presenting it in an organized and easy to read format.	

Handwritten initials/signature

Handwritten signature: S. Dore

S.No	Description of Requirements	Trial Directives	
13.	Add hash sets to either filter out non-relevant files to enhance search performance and reduce false positives or add hash sets that will specifically call out and identify known bad pictures and videos.	BOO will check practically and Firm will submit OEM certificate.	
14.	Efficiently analyze large volumes of data		
15.	Explore file systems and registry hives for greater insights		
16.	Process and recover 500+ types of artifacts		
17.	Automate all acquisition and processing tasks required to prepare evidence for analysis.		
18.	Explore file systems and registry hives for greater insights		
19.	Trace artifact evidence back to its source data in seconds		
20.	Trace artifact evidence back to its source data in seconds.		
21.	built on the analysis capabilities allowing you to recover hundreds of types of digital forensic artifacts		
22.	Should be able able to extract data from cloud data source using Tokens from evidence		
23.	Easy-to-use interface that moves you through your investigation.		
32	EVIDENCE SEIZURE KIT		
1	Multipurpose, Portable Unit That Contains A Complete Array Of Hardware/ Software Solutions To Preview, Acquire Or Process Digital Evidence.		BOO will check practically and Firm will submit OEM certificate.
2	Kit Should Contain High End Forensic Laptop With The Following Minimum Configuration		
	(a) Intel Core i7-6700K Skylake Quad Core Processor or higher or equivalent, 4.0 GHz, 8MB Intel Smart Cache or higher		
	(b) 32 GB PC4-17000 DDR4 2133 Memory		
	(c) 256 GB Solid State Internal SATA Drive or higher		
	(d) Intel Z170 Express Chipset Or equivalent <i>or higher</i>		
	(e) 15.6" Full HD (1920x1080) IPS Display with G-Sync Technology, Matte Finish <i>or higher</i>		
	(f) NVIDIA GeForce GTX 1060 with 6 GB GDDR5 VRAM		
	(g) 1 RJ-45 LAN (10/100/1000Mbps)		
	(h) Intel Dual Band Wireless-AC 8260 - 802.11ac, Dual Band, 2x2 Wi-Fi + Bluetooth 4.2		

S.No	Description of Requirements	Trial Directives
	(j) Card Reader 6-in-1 (MMC/RSDMMC/SD/Mini-SD/SDHC/SDXC up to UHS-II) (k) 2.0 Megapixel FHD Video Camera (l) High Definition Audio (m) Microphone (n) Speakers (2) (o) 19mm Full-Size Keyboard with numeric keypad - Illuminated (p) Touch Pad pointing device(2 buttons)with multi-gesture and scrolling function (q) Finger Print Reader (r) 1 HDMI Port (s) 2 Mini DisplayPort 1.3 ports (t) 1 Thunderbolt 3 / USB 3.1 Gen 2 Combo Port (Type C) (u) 1 USB 3.1 Gen 2 Port (Type C) (v) 3 USB 3.0 ports (w) 1 USB 2.0 Port (x) 1 Headphone jack (2-in-1 Heasdphone/ S/PDIF Optical) (y) 1 Microphone jack (z) 1 Line-In jack (aa) 1 Line-out jack (ab) 8 Cell Smart Lithium -Ion, 82WH Battery Pack (ac) Kensington Lock Slot (ad) Universal AC Adapter (100~240V AC 50/60hz) (ae) Dimensions: 15.20 x 10.32 x 1.41 (inch) (af) Weight: 7.5 lbs (complete system + battery) (ag) Windows 10 Professional (64 bit)/ Other Operating Systems included: SUSE Professional Linux (64 bit) (ah) System Restore Media - Bootable Blu-ray disc containing restore environment and factory configured operating system images	BOO will check practically and Firm will submit OEM certificate.
3	KIT SHOULD CONTAIN PORTABLE FORENSIC WRITE BLOCKER WITH THE FOLLOWING INTERFACE	
	(a) USB 3.0 - IDE/SATA, SAS, USB 3.0, Firewire, USB 3.0 Forensic Card Reader and Writer has been designed specifically for forensic use and incorporates Super Speed USB3 (5Gb/s) technology. (b) Universal Power Supply and Power Adapter cables, Standard Cables and Adapters	BOO will check practically and Firm will submit OEM certificate.

Handwritten signature/initials

Handwritten signature/initials

S.No	Description of Requirements	Trial Directives
4	KIT SHOULD CONTAIN LATEST FORENSIC DUPLICATOR WITH FOLLOWING CONFIGURATION	
	<p>(a) Should have a Forensic Duplicator with capabilities to support Greater than 2TB HARD DRIVES</p> <p>(i) Image a 2TB HDD (2000GB)</p> <p>(ii) Clone HDDs with no size limit</p> <p>(b) Forensically duplicates HDD's faster than ever - up to 15 GB/min with hashing</p> <p>(c) Standard features include Disk-to-Disk (clone) and Disk-to-File (image) duplication, Format, Wipe, Hash (MD5 or SHA-1), HPA / DCO detection and removal, and Blank Disk Check.</p> <p>(d) Make one (1:1), two (1:2), or three (1:3) copies of evidence drives.</p> <p>(e) Acquisitions of USB 3.0, SATA, and IDE/PATA devices can be directed to either USB 3.0 or SATA output devices.</p> <p>(f) Option to acquire SAS drives with additional modules</p> <p>(g) Outputs to raw DD, .e01 (compressed), .ex01 (compressed), or .dmg formats</p> <p>(h) USB 3.0 convenience and speed built in</p> <p>(j) Extensive log files is easy to view and save</p> <p>(k) Built-in, user-selectable MD5 and SHA256 verification</p> <p>(l) Hash re-verification on read from destination(s) - user-selectable</p> <p>(m) Colour LCD user interface</p>	BOO will check practically and Firm will submit OEM certificate.
5	<p>EXTERNAL DEVICES AND ENCLOSURES</p> <p>(a) USB3 Read Only/Read Write switchable External Hard Drive Chassis with Power Supply</p> <p>(b) Digital Intelligence Integrated Forensic Media Card Reader - Read-Only and Read/Write Switchable</p>	
6	<p>EXTRAS</p> <p>(a) Hard Drive Adapter 2.5 Inch</p> <p>(b) Hard Drive Adapter 1.8 Inch</p> <p>(c) TDA5-ZIF ZIF HD Adapter w/case</p> <p>(d) TDA3-1 Micro SATA HD Adapter</p> <p>(e) SATA LIF Adapter</p> <p>(k) 2 TB SATA Hard Drive</p> <p>(l) Precision Electronic Tool Kit</p> <p>(m) Power Strip - 120v/240v Compatible</p> <p>(n) Universal Power Adapter</p>	BOO will check practically.

Handwritten signature/initials

Handwritten signature/initials and number 60

S.No	Description of Requirements	Trial Directives
7	<p>PELICAN CASE</p> <p>(a) Hard-sided with Padded Laptop Insert</p> <p>(b) Watertight / Airtight</p> <p>(c) High Impact</p> <p>(d) Custom Foam Lined</p> <p>(e) Custom Lid Organizer for Cables and Adapters</p> <p>(f) 24" x 20" x 14" - 58lbs</p>	<p>BOO will check practically and Firm will submit OEM certificate.</p>
8	<p>SOFTWARE</p> <p>(a) Microsoft Windows 98SE Standalone DOS (Configured & Pre-Installed)</p> <p>(b) Microsoft Windows 8 Professional 64 bit (Configured & Pre-Installed)</p> <p>(c) Microsoft Office 2016</p> <p>(d) Suse Linux Professional (Pre-Configured)</p> <p>(e) Symantec GHOST</p> <p>(f) DVD/CD Authoring Software</p> <p>(g) High-End Forensic laptop should come pre-installed with Forensic analysis software with Live Boot virtualization, Shadow Copy, Meta extraction, Carving, Hash Sets, Index and Keyword search, flexible graphic user interface (GUI) with advanced sorting, filtering, keyword searching, previewing and scripting technology and Bookmarking capability. The software should allow the investigator to Boot forensic image files and view electronic evidence in a forensically sound virtual environment. Boot both Windows (all versions) and Macintosh computers.</p> <p>(h) Product Offered should be of International Repute & Brand and should not be assembled Machine.</p> <p>(j) In case of Distributor/ Reseller; OEM/ Manufacturer's Authorization for Supply and Service should be attached with the Tender.</p> <p>(k) Bidder should have OEM trained Manpower for Product Installation and support, Supporting document for the same to be attached.</p>	<p>BOO will check practically and Firm will submit OEM certificate.</p> <p>Firm will submit OEM certificate.</p>

Handwritten signature/initials

Handwritten signature/initials

3. INTELLIGENT INVESTIGATION MANAGEMENT SYSTEM

S. N	Description of Requirements	Trial Directives
1	Tool should be collaborative end-to-end product that uses a clean, intuitive interface, allowing anyone get started with very little training. It should provide digital evidence and lab management, as well as archiving, which allows teams to understand how the evidence was handled and where to find it in the future.	BOO will check practically and Firm will submit OEM certificate.
2	Tool should works through common browsers on Windows, Mac, Linux, and mobile OSs and it builds statistics as you enter information. It should be able to incorporate case management stats into reporting tools.	
3	<p>Also have below features:</p> <ul style="list-style-type: none"> (a) Global Collaboration on Any Case (b) Unlimited Client Base (c) Permanent Case Archives (d) Chain of Custody Preservation (e) Complete Exam Documentation (d) Curriculum Vitae Management (e) Asset Management (f) Local or Remote Browser Access (g) Consolidation of All Case Information (h) Automatic Statistics Generation (j) ICAC and Cyber tip Management for Law (k) Financial Information Management (l) Lab Expenses Analysis (m) Grant Documentation Management (n) Project Expense Accountability (o) Invoice Generation (p) Process Review Facilitation (q) In- eld Evidence Triage (r) Scalability to Grow with Your Needs (s) Barcode Generation (t) Secure 256-bit Encryption (u) Standardized, repeatable process 	BOO will check practically and Firm will submit OEM certificate.

Handwritten signature/initials

Handwritten signature/initials

4. ARTIFICIAL INTELLIGENCE (Workstation)

S. No	Description of Requirements	Trial Directives
1	The system should have deep learning platform providing unprecedented performance with industry leading 1 GPUs, fast GPU interconnect, high bandwidth fabric and a configurable GPU topology to match your workloads.	BOO will check practically.
2	The system should have the ability to autonomously learn, predict, and adapt using massive data sets.	
3	Processor/ Cache <ul style="list-style-type: none"> • 2 x Intel Xeon Scalable Processors with 3UPI links, 2.4GHz Processor base frequency CPU <ul style="list-style-type: none"> • 20 cores with Intel HT Technology Cores <ul style="list-style-type: none"> • 4 NVIDIA TESLA V100 SXM2 GPUs GPU <ul style="list-style-type: none"> • 300 GB/s GPU-to-GPU NVIDIA NVLINK 	BOO will check practically and Firm will submit OEM certificate.
4	System Memory <ul style="list-style-type: none"> • 12 DIMM slots • 384GB DDR4- 2666 ECC DIMM • 2666/2400/2133MHz ECC DDR4 SDRAM Memory Capacity Memory Type	
5	SSD <ul style="list-style-type: none"> • 4 x 1.92TB 	
6	On-Board Devices <ul style="list-style-type: none"> • Intel C621 chipset or higher • SATA3 (6Gbps) with RAID 0, 1, 5, 10 • Intel X540 Dual Port 10GBase-T • Support for Intelligent Platform Management Interface v.2.0 Chipset SATA Network Connectivity IPMI	
7	Input/Output <ul style="list-style-type: none"> • 4 SATA3 (6Gbps) ports • 2 RJ45 10GBase-T ports and 1 RJ45 Dedicated IPMI LAN port • Minimum 2 USB 3.0 ports • 1 VGA port SATA LAN USB VGA	
8	Chassis <ul style="list-style-type: none"> • 4U Rack mount Form Factor	
9	Expansion Slots <ul style="list-style-type: none"> • 4 PCI-E 3.0 x 16 slots PCI-Express	
10	Drive Bays <ul style="list-style-type: none"> • 2 Hot-swap 2.5" SAS/SATA drive bays Hot-swap	
11	Power Supply <ul style="list-style-type: none"> • 2000W Redundant Power Supplies Titanium Level 	

CYBER MANAGEMENT AND MONITORING
1. 55" DISPLAY FOR CONTROL CENTRE

S.No	Description of Requirements		Trial Directives
1.	Supply Screen Size	55" or above.	BOO will check practically and Firm will submit OEM certificate.
2.	Panel Technology	IPS.	
3.	Back Light Type	Direct/Edge LED for Slim depth of display.	
4.	Aspect Ratio	16.9.	
5.	Native Resolution	1,920 X 1,080 (FHD) or High, display should support UHD resolution in Video wall application.	
6.	Brightness	700nits or Higher to get clear visibility in highlight condition of room if required.	
7.	Contrast Ratio Dynamic CR	450,000:1 or Better to ensure the contrast as per requirement of contents.	
8.	Viewing Angle(HxV)	178 X 178 angle to cover Max viewing angle from any location of Room. Response Time	
9.	Life time (Typ.) or High to ensure full performance of LED for Long period. Operation Hours:	24Hrs grade panel for ensure Heavy Duty cycle if required Portrait & Landscape suitable format to ensure zero gravity effect in case of customized installation for long period.	
10.	Orientation:	Portrait & Landscape suitable format to ensure zero gravity effect in case of customized installation for long period.	
11.	Input ports:	HDMI 1.DP1. DVI D1.USB RJ45(LAN1) or high to cover all types of inputs as per site requirements & future requirements.	
12.	Output ports.	Display port (DP) for daisy chain to run FHD contents without controller.	
13.	External Control:	RJ45 (LAN 1) for daisy chain to take control of video wall from remote location.	

AW

Mn

S. Sol. A. K. B.

S.No	Description of Requirements	Trial Directives
14.	Bezel to Bezel (Gap): 1 mm or less to get seamless picture/video experience.	BOO will check practically and Firm will submit OEM certificate.
15.	Key Feature required ; Temperature Sensor, Auto source selection, Energy Saving Calibration Mode, Failover, Wake on LAN, No signal Screen.	
16.	Power supply: 100 240V. 50/60Hz	BOO will check practically.
17.	Power Consumption 300 Watts or less.	
18.	Operation Humidity 10% to 80%. -	Firm will submit certificate of Govt. Lab. or NABL/ILAC accredited laboratory.
19.	Certification's UL for safety. FCC for Electro Magnetic Communication, Energy star rated for confirmation of power consumption & BIS.	

2. DATA WALL CONTROLLER

S.No	Description of Requirements	Trial Directives
1.	Supply of controller for video wall Display & Scaling,	BOO will check practically and Firm will submit OEM certificate.
2.	Display multiple sources anywhere on display up to any size,	
3.	All input sources should be displayed on the video wall in freely resizable and movable windows inputs.	
4.	Should have option to connect to 4 minimum sources through, HDMI.	
5.	Each in Full HD Format(1920x1080) output to connect to minimum 4 Displays. Each in Full HD Format (1920x1080)	

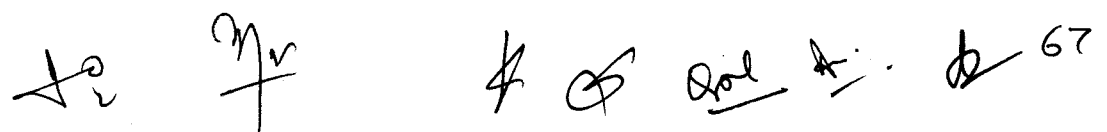
3. INCIDENT RESPONSE MANAGEMENT AND ALERT SYSTEM

S.No	Description of Requirements	Trial Directives
1.	General Requirement of IT Service Management Solution:	
	(a) Should able to support and handle large volume of incident	BOO will check practically and Firm will submit OEM certificate.
	(b) Should able to support and handle large volume of service requests	
(c) Should able to support and handle large volume of changes		

S.No	Description of Requirements	Trial Directives
	(d) Proposed Service desk/ HDMS must be ITIL certified	Firm will submit OEM certificate.
	(e) Native integration of processes i.e. Incident Management with Change Management and vice-versa	BOO will check practically and
	(f) Native integration of processes with Knowledge base i.e. automatically creation of knowledge base post closure of tickets	Firm will submit OEM certificate.
	(g) The solution should have a Single Architecture and leverage a single application instance across ITIL processes, including unique data and workflows segregated by business unit.	
	(h) Able to create and modify forms as per customer requirement	
	(j) Able to define different SLAs for different services / domains	
	(k) Solution should support multi-tenancy with complete data isolation as well as with ability for analysts based on access rights to view data for one, two or more organizational units	
	(l) Able to define different workflows for different processes	
	(m) Able to send automatic escalation mails as defined in workflow	
	(n) Should be able to integrate CMDB from different federated data sources and build a single CMDB	
	(o) Should provide email based interactions allowing ticket creation, update and approval of request.	
	(p) Should able to integrate with Active Directory and populate user information automatically	
	(q) The system should have graphical interface to define, visualize and update ITIL processes	
	(r) The solution should provide to browse through CMDB which should offer powerful search capabilities and auto-completion for configuration items and services, enabling to quickly find Cis as well as their relationships to other Cis.	



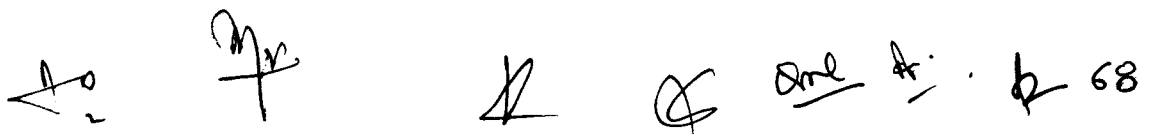
S.No	Description of Requirements	Trial Directives
2.	Incident and Problem Management	BOO will check practically and Firm will submit OEM certificate.
	(a) Service Desk solution should allow detailed multiple levels/tiers of categorization on the type of incident being logged for IT services that shall span across multiple domains.	
	(b) Service Desk solution should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.	
	(c) The solution should provide embedded and actionable best practices workflows i.e., best-practices process & views based upon implementations	
	(d) It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location.	
	(e) Solution should support fast service restoration leveraging previous incident data.	
	(f) It should have the ability to search multiple built-in knowledge bases like the incident, problem, and known-error database simultaneously without requiring the agent to search each knowledge base individually.	
	(g) Should support automatic assignment of ticket to the right skilled resource based on business priority Ex - Database crash issue need not be assigned to an L3 DBA unless the business service is completely down.	
	(h) It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.	
	(j) Should support text search capabilities	
	(k) Should centralize all known error and problem workarounds into a single, searchable knowledge base	
	(l) It should provide an interactive process flow bar that guides novice users through the ITIL process for incident management to ensure faster issue resolution.	
	(m) The incident Management solution should be completely integrated to the CMDB to ensure that Cis can be associated with the ticket to provide better visibility	
	(n) The incident management solution should have the ability to initiate the change request	
	(o) The solution should have the ability to associate an incident with an existing change request, a problem or known error for tracking purposes	
	(p) The service desk should have shift management capabilities for support staff wherein tickets are allocated based on shift availability.	
	(q) It should allow the CI to be associated with tickets.	



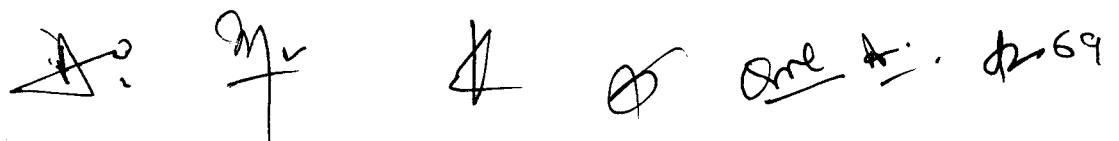
4.

CENTRAL NETWORK ASSET MANAGER

S.No	Description of Requirements	Trial Directives
1.	Should be a comprehensive management platform that delivers integrated, modular management capabilities across fault, configuration, accounting, performance, and security (FCAPS) needs	BOO will check practically and Firm will submit OEM certificate.
2.	Should support minimum 50 wired devices from day 1 and the solution should be scalable up to 1500 wired devices without any hardware or software up-gradation.	
3.	Should allow automatic topology discovery and creation of network maps for layer 2 as well as layer 3 networks including all the available VLANs	
4.	Should have network inventory polling capability for IP network nodes, available line cards, modules, ports, physical links, VLAN interfaces and all the other SNMP capable devices in the network.	
5.	Should allow extensive fault management with real time event and alarm notifications including system logs	
6.	Should allow centralized creation and management of VLAN and ACL policies	
7.	Should have scheduled device configuration back-up and restore functionality	
8.	Should have automatic detection of configuration changes for easy trouble shooting and isolation.	
9.	Should allow monitoring and management of 3rd party devices and end points.	
10.	Should have the functionality of scheduled configuration roll out	
11.	Should have the functionality to perform scheduled or unscheduled network wide software or firmware upgrades	
12.	Should have the ability to customize NMS dash board.	
13.	Should allow grouping of devices for applying any particular change/task	
15.	Should have 64-bit support	
16.	Should support centralized as well as distributed deployment.	
17.	Should support virtualization management; management and monitoring of both physical and virtual networks. It should provide insight into and management of virtual networks and reduce migration complexity by aligning and automatic network policies with virtual images.	


 A collection of handwritten signatures and initials at the bottom of the page, including a large 'A', 'M', 'K', 'Q', and 'D'. To the right, there is a date '21. 6. 68' and the number '68'.

S.No	Description of Requirements	Trial Directives
18.	Should support role based access control	BOO will check practically and Firm will submit OEM certificate.
19.	Should be with software update and upgrade assurance during the warranty period	
20.	Should have support for add-on modules on the same software platform for monitoring and management of routers, wireless controller, wireless access points and wireless client devices.	
21.	Should facilitate enable centralized management of proposed network elements with a variety of automated tasks, including discovery, categorization, baseline configurations, software images, configuration comparison tools, version tracking, change alerts, and more	
22.	Should support centralized VLAN Management to view current VLAN configuration, VLAN topology, bulk VLAN deployment etc.	
23.	(a) Should provide high-performance, scalable network log audit and analysis support with auditing online activities of internal users	
	(b) Should support various log formats such as NAT, flow, NetStream including log formats that allows audit security-sensitive operations and digest data from HTTP, FTP, and SMTP packets	
	(c) Should support policy driven log filtering	
	(d) Should support log collection from devices that do not otherwise support the standard protocols such as Flow, NAT, NetStream, sFlow/Netflow etc.	
	(e) Should support user activity auditing of at least 50 users from day 1 and this should be optionally extendable up to 1500 users.	
24.	Should offer following RADIUS/AAA features:	
	a) Shall support user identity authentication based on the access policies associated with infrastructure resources, such as routers, switches, license for 100 users from day 1.	
	b) Shall provide a full-featured RADIUS server that supports centralized authentication, authorization, and accounting management.	
	c) Network-agnostic device fingerprinting capabilities based on HTTP+MAC+DHCP device recognition for BYOD.	
	d) Shall support authentication modes like 802.1X, VPN, portal, and wireless access identity modes like PAP, CHAP, EAP-MD5, EAP-TLS, and PEAP to fit into applications with different security requirements.	



S.No	Description of Requirements	Trial Directives
	e) Shall provide centralized policy creation to set the appropriate access rights for each type of user and device across the network.	BOO will check practically and Firm will submit OEM certificate.
25.	Should be a ITILv3 compliant comprehensive management platform that delivers integrated, modular management capabilities across fault, configuration, accounting, performance, and security (FCAPS) needs.	
26.	Offered software should have compatibility with Microsoft Windows or Linux operating systems	
27.	Offered software should be scalable up to 1500 wired devices and 1500 users.	

E. COMMON HARDWARE

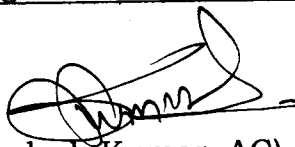
1. TIME SERVER

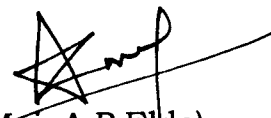
S.N	Description of Requirements	Trial Directives
Power Supply:		
1.	Voltage	230 +/- 10% V AC
2.	Frequency	47-55 Hz
Functions/ Features :		
3.	Time Facility	Using Universal Time co-ordination(UTC)
4.	Propagation delay Compensation	Supported
5.	Accuracy	+/- 250 Nanosecond
6.	Time Accuracy	Better than 1 PPM
7.	LCD Display	Front panel LCD display to show status, time and no. of satellites
8.	Inputs	GPS Antenna input through BNC connector.
9.		Power Supply
Outputs		
10.	NTP output (2 nos. customizable) for NTP client access through RJ-45 .Both Ports shall be independent	
11.	RS232 serial port output (2 Nos)	
12.	Pulse output: 1 PPS, ½PPM, 1PPM (Configurable).	
13.	Support Client request per Second	10,000 or higher
		BOO will check practically and Firm will submit OEM certificate.


Handwritten signatures and initials: M, S, and others, followed by the number 70.

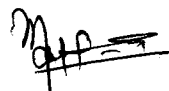
S.N	Description of Requirements		Trial Directives
Antenna			
14.	Length of GPS	50 meters	BOO will check practically.
15.	Gain	Over 30 DB	
16.	Receiver, Global Positioning System, Display Type: Lcd; Display Size: 2 X 3.5 Inch; Display Resolution: 240x400 Pixels; Data Interface: Ethernet; Pc Interface: Ethernet;; Expansion Slot Type: Usb; Way Points: 2; Server Frequency: 48-55 Hz; Operating Temperature: 0-55 Deg.C; Electrical Rating: 230 Vac; Additional Information: With Antenna And Surge Arrestor		

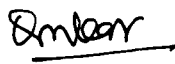

(Avirat Pandey, AC)
ITBP


(Sandesh Kumar, AC)
SSB

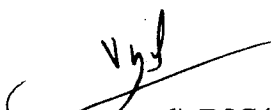

(Maj. A.P. Eldo)
NSG

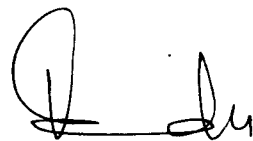

(Vipul, DC(IT))
CRPF



(P. R. Jha), DC(Comn)
CRPF


(Col. Omkar Singh)
Assam Rifles

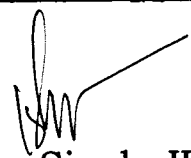

(Amit Taneja), DIG(Eqpt)
CRPF


(Virendra Agrawal), DIG(Comn)
CRPF


(Ravideep Singh Sahi)
IG(Comn&IT), CRPF


(Zulifiquar Hasan), IPS
SDG(HQ), CRPF

Approved/Not Approved


(Kuldieep Singh, IPS)
DG, CRPF