TECHNICAL SPECIFICATION
IDENTITY AND ACCESS MANAGEMENT SYSTEM (IDAM)

Ser No	Description of Requirements	Compliance (Yes/No)	Remarks
	GENERAL		
1	The proposed solution should have a central identity manager		
2	The multi data centre authentication/access capability should be such that that the session created at one data centre should be synced and respected at a remote data centre while traversing from a locally protected app to a centrally deployed centrally protected application.		
3	Proposed Solution should have a LDAP Directory with Directory Replication Capabilities to maintain a read only copy in remote data centres.		
4	Solution should provide Single Sign On (SSO) with role based access control to users of application.		
5	The solution implemented should offer customizable landing page which can be accessible over Army Data Network. User once authenticated, the landing page should display the list of all applications authorized to him. On choosing any application, the user should be directed to that application with the correct credentials without having to separately login/ sign in. The page should also allow users to manage own attributes e.g. change password, contact details etc.		
6	Solution should integrate all websites/ applications deployed over ADN (approx 500) – to incl static/ dynamic websites and applications (predominantly web based)		
7	The proposed solution should be able to seamlessly integrate with existing Application		
8	Solution should have the capability to integrate with Active Directory.		
9	The solution should run in High Availability (HA)		
10	Solution should support integration with the applications running across different web/ application sever which will be hosted on different OS such as Windows/ Linux/ Solaris.		
11	The sys software should be completely scalable to accommodate the changing Nos of users and applications.		
12	System shall have complete web based administration module		
13	The proposed solution should be FIDO Compliance		
14	Support for interoperability with cross platforms specifically Windows and Linux		
15	IDENTITY and ACCESS MANAGEMENT SOFTWARE provider should be certifying authority under CCA		
16	Support SSL/ TLS of latest version		

17	Solution should have undergone third party Vulnerability Assessment and Penetration Testing (VAPT) and proof of audit certificate should be produced		
18	**IDENTITY MANAGEMENT SOFTWARE**		
19	Management of Identity profiles should be central with a single repository of identity data.		
20	Entire management of identities should be web based.		
21	Solution should be able to create, update, and delete user accounts across the enterprise environment both manually and automatically.		
22	The solution should enable assignment of users to single/ multiple roles.		
23	The solution should have a workflow for provisioning/ de-provisioning of identities.		
24	Solution should provide a graphical interface that allows creating and managing workflows.		
25	Solution should automatically route access requests of users for approval to the destined administrator.		
26	Solution should have ability to delegate approval authority to another person.		
27	Solution should have ability to escalate a request to an alternative approver if the allotted time elapses.		
28	Provisioning solution should provide capability to the approver to provide comments.		
29	Should support withdrawal of non-approved requests		
30	Solution should be able to generate unique user IDs.		
31	Should integrate with PKI to complete user creation process.		
32	Solution should provide auto requisition of PKI token personalization for new users being created		
33	Should support provisioning/ de-provisioning on joining/ movement of personnel on transfers and temporary assignment of roles.		
34	Solution should provide delegated administration.		
35	Solution should be able to define delegated administration by way of both administration (which users, which resources) and capabilities (full account administration, password administration only, etc.).		
36	Solution must support web-based self-service in terms of changing passwords, resetting forgotten passwords retrieving forgotten user login etc		
37	Solution must allow users to view their profile and the resources and the corresponding entitlements they have got access to.		
38	Must have capability to provision user accounts to target systems and applications.		
39	Must have out-of-box connectors available for target systems to carry out user provisioning and reconciliation operations.		

40	The proposed solution should more then 15 Factors of Authentication based on policies defined		
41	Should have connector development framework to extend support to additional target systems for which out of box connectors are not available.		
42	Should have capability to allow administrators to define and enforce global password policy that includes password composition rules like -minimum length- minimum password age- warn after expires, disallow past passwords		
43	Should support complex password rules including maximum repeated characters, minimum numeric characters, alphanumeric characters, uppercase & lowercase characters etc		
44	Should support validation of password provided against the defined password policy.		
45	As part of forgotten password, the solution should have support to challenge the user for security answers to the questions that must have been configured at the time of user creation or self-registration. The manager of the user whose password is being reset must be notified of this password reset.		
46	Solution should allow users to manage their own passwords.		
47	Should have ability to synchronize passwords for multiple systems to the same value to reduce the number of different passwords to be remembered by the user.		
48	Should support delivery of password-change success/ failure status to requestor using mechanisms like email		
49	Users should be able to update personal attribute information, such as address, cell phone number, etc.		
50	Solution should provide a web based front-end for help-desk administrators to use.		
51	Solution should provide a password exclusion list and allow restriction of using old passwords.		
52	Solution should support Role Based Access Control (RBAC).		
53	Solution should report on who had access to what on a given date.		
54	Solution should support the creation of custom audit policies (eg. Separation of Duties) that can be applied during access scans.		

55	Solution should support reporting grouped by the following: by administrator (accounts created, accounts modified, accounts deleted, password changes, complete audit history per administrator, administrative capabilities per administrator) 1. By platform or application (users per platform, provisioning history per platform, who performed the provisioning actions on target platform) 2. By workflow (requests made by user, requests approved by approver, requests denied by approver, requests escalated, delegation of approvals including to whom and for what period of time) 3. By user (audit history per user, accounts/privileges by user, self-service activity by user)		
56	Should support reports related to access policy, request, certification, approval, role, organization, password, resource & entitlement, user.		
57	Should support reports like list of all the rogue accounts existing in a resource, list all orphaned accounts etc.		
58	Should support SSL/TCS digital certificate based secure encrypted communication.		
59	Solution should not impose a physical or logical limitation on creation of number of users, while concurrency factor will drive the proposed hardware.		
60	Solution should have the capability of configuring applications for single factor as well as multi factor authentication.		
61	The solution should support all types of web browsers like Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, etc.		
62	**ACCESS MANAGEMENT SOFTWARE**		
63	Should have capability to provide centralized logout		
64	Must support integration with PKI Technologies to support certificate based authentication		
65	PKI and Digital Certificates is madatory requirement for Ensure Legal Non-Repudiation		
66	Must support OSCP based live certification validation from the CA Authority under CCA		
67	Should support Certificate Validation against CRL Export Dump		
68	Must give administrators complete visibility and control over real-time user session data including ability to search for and terminate specific sessions		
69	Must support delegated administration at each datacenter location to have visibility on local users		
70	Should allow administrators to enforce constraints on session lifetime idle timeout max number of concurrent sessions		

71	Should be compatible with a variety of web/app servers including Apache, IIS, IBM HTTP, Oracle HTTP, Node JS, Tomcat, Jboss, Web logic, Web sphere			
72	Should have support to log authentication success and failure			
73	Behavioral and Risk based Parameter Detection for user-login to provoke authentication layers in line with real-time adjusted risk profile.			
74	Identity and Access Management Software provider should be certifying authority under CCA.			
75	Support SSL/ TLS of latest version			
76	**HCI Server**			
77	**Hyper-Converged Solution for Cloud**			
(a)	Analyst Ratings	The bidder shall propose Hyper Converged Integrated System from vendors placed in the leader's wave in the Forrester Wave (or equivalent) : Hyper converged Infrastructure (HCI). (The bidder will submit the supporting documents for the proposed solution listed in The Forrester Wave Report.)		
(b)	Analyst Ratings	The bidder shall propose Hyper Converged Integrated System from vendors placed in the leader's quadrant in the Gartner Magic Quadrant (or equivalent) report latest. (The bidder will submit the supporting documents for the proposed solution listed in Gartner Magic Report latest)		
(c)	Benchmarks	Should have a Validated by Login VSI Benchmark for Cloud for both Citrix Xen Desktop and Vm ware Horizon View environments.		
78	**HARDWARE AND PERFORMANCE REQUIREMENTS**			
(a)	Offered Hyper-Converged Capacity	The offered appliance shall be based on modular building blocks of up to one compute node. Each block shall be built using a 2U modular chassis / enclosure housing the compute with respective storage capacity. Each of the Server nodes should be individually serviceable, without shutting down the other Server nodes		

(b)	Hardware Support	Solution must be x86 infrastructure agnostic and available to be deployed on a choice of atleast 3 server OEMs		
(c)	Hyper-Converged Infrastructure	Proposed solution must be based on converged IT infrastructure platform that integrates storage, compute, networking, hypervisor, real-time deduplication, compression, and optimization along with powerful data management, data protection, and disaster recovery capabilities in a standard x86 server building block.		
(d)	Functionality	Proposed hardware must be capable to Deduplicate, Compress & Optimize ALL data inline, in real-time, across all storage tiers: All handled with fine data granularity of 8KB data blocks		
(e)	Hardware Specifications	Each Compute Block must come with the following specifications: Dual Intel Intel® Xeon® Gold 5120 Processor or higher Use of All SSD Drives for Caching and Persistent storage. Minimum 5*1.92TB SSD for data storage Minimum 256GB of DDR4 RAM at 2400 Mhz or above 2*40GbE NIC		
(f)	Resiliency	Proposed solution must be able to support multiple points of failure with no loss of function or data.		
		During a single component failure (of any type) production services are not affected / degraded in anyway		
		Solution will be deployed as a stretched cluster with Zero RTO. Solution should support stretched cluster deployment in a near site metro DC deployment.		
		Each node should have dedicated non-shared dual-PSU's and should be able to sustain single power supply failure. Solution should not utilize micro-server architecture with shared PSU's and other components.		
		Must be able to sustain minimum of simultaneous 2-HDDs failures per node without DU/DL		
		Must be able to sustain minimum of simultaneous 1-HDDs failures in each node of a cluster and across all nodes in the cluster without DU/DL		
		Must be able to sustain one node failure in the cluster		
		Must be able to sustain 1 NIC port failure		

	SOFTWARE AND FUNCTIONALITY REQUIREMENTS			
(g)	Common Features Included	The proposed solution must be able to provide enhanced functionality by including the following available without compromise in function or performance in both Hybrid as well as All Flash Nodes:		
		Global dedupe, compression and optimization with minimum impact to production workloads and guaranteed CPU and RAM available to user applications		
		VM-centric policy-based backup/recovery/DR		
		WAN-optimized data protection for VM mobility		
		Unlimited real time data Deduplication Function - licenses Included		
		Unlimited real-time data Compression Function -licenses Included		
		Unlimited capacity Backup Function-Included		
		Should include licenses for multi-site deployments of atleast 3 sites		
(h)	Global Unified Management	Proposed solution must be able to support the following Global Unified Management features		
		VM-centric management through a single pane of glass via the virtualization manager		
		Programmatic interface to enable automated tasks like failover / failback		
		The ability for a single administrator to manage all aspects of the Hyper-convergence from within the Virtualization Manager for all sites		
		Leverage existing investment of servers for hosting VMs and applications while taking advantage of the functionality of the solution		
		Globally manage Backup Policies per Datastore or per VM		
(j)	VM-Centricity and Mobility	Proposed solution must be able to support the following VM-Centricity and Mobility feature		
		Backups for specific VMs		
		Ability to Move specific VMs between datacenters		
		Cloning specific VMs		
		VM-level backup instead of forcing protection at the datastore or protection domain level		

(k)	Data Protection	Proposed solution must be able to support the following Data Protection features		
		Backup functionality as a feature instead of a separate server / software license		
		Backup must be an independent copy of source Virtual Server and must allow restore of deleted or corrupted source Virtual Server		
		Backup to disk functionality as a feature instead of a separate license or appliance		
		Replication across separate datacenter as a feature instead of a separate server / software license.		
		Replication across separate datacenters should be optimized with minimum additional overheads. Data should not need to be rehydrated before being transferred to target datacenter.		
		The ability to carry simultaneous out bi-directional replication between two data centers		
		The ability to replicate Any-to-Any in a Mesh Data Center deployment of more than 3 DC's		
		The ability to define backup policy per datastore, a group of VMs or specific VM		
		Data Protection should have RPO of 10 minutes for local backups		
		The ability to execute backup tasks during office hours without impacting to production workloads		
		Data loss protection against a minimum of 2 simultaneous local hard disks failures per node		
		Data loss protection against a minimum of 1 simultaneous local hard disc failures in all nodes of the cluster		
		Data loss protection against single node failure in cluster		
		The proposed solution must be able to provide backup reports for audit purpose		
(l)	Data Recovery	Proposed solution must be able to support the following Data Recovery features		
		Data recovery should be indepent of source Virtual Server		
		Solution should provide a backup catalog to allow any Virtual Server to be recovered to any specific point-in-time		
		Data recovery process should be simple with an RTO in minutes		

(m)	Disaster Recovery	Proposed solution must be able to support the following Disaster Recovery features		
		The solution must provide a simple failover operation		
		The solution must allow creation of a Runbook to automate recovery of Virtual Servers		
		The solution must allow changing of IP address of recovered Virtual Servers to match target datacenter		
		The solution should allow changing Virtual Server settings (example vCPU, vRAM, VMSwitch) if required		
		The solution must allow the option to test DR failover to separate network with no impact to production workloads		
		The solution should have feature to assist in failback process to Primary datacenter		
(n)	Private Cloud License	The Proposed solution must be offered with cloud-ready operating system that is ideal for highly virtualized and software defined datacenter environments.		
		It must include Shielded Virtual Machines, software defined networking, Storage Spaces Direct, and Storage Replica; customers receive rights to unlimited Operating System Environments (OSEs)		
		The proposed solution must provide following features: Computing environment: The virtual machine includes the same basic parts as a physical computer, such as memory, processor, storage, and networking. Disaster recovery and backup, Optimization.		

		Solution must have features such as live migration, storage migration, and import/export to move or distribute a virtual machine.		
		It must offer a remote connection tool for use with both Windows and Linux.		
		The solution should have Secure boot and shielded virtual machines that protects against malware and other unauthorized access to a virtual machine and its data.		
		The solution must give virtual machine direct and exclusive access to some PCIe hardware devices. Using a device in this way bypasses the virtualization stack, which results in faster access.		
		The solution must prevent a virtual machine's excessive activity from degrading the performance of the host or other virtual machines.		
		A virtual machine can be used as a host and create virtual machines within that virtualized host.		
		The solution must have option to set up Remote direct memory access (RDMA) on network adapters bound to a virtual switch, regardless of whether switch embedded teaming (SET) is also used.		
		The solution must have features to make it harder for virtualisation administrators and malware on the host to inspect, tamper with, or steal data from the state of a shielded virtual machine.		
79	**Core Switch**			
(a)	**Architecture**			
	Shall be 19" Rack Mountable			
	The switch should have dual hot-swappable power supplies			
	Switch shall have minimum 24 x 1/10G SFP+ ports, populated with 8x10G SR,8x1G SX and 8x1G BaseT transceiver.			
	1 RJ-45 serial console port			
	1 RJ-45 out-of-band management port			
	Should have minimum 2GB SDRAM and 512 MB flash and 13 MB Packet buffer size			

	Shall have switching capacity of minimum 480 Gbps		
	Shall have up to 350 million pps switching throughput		
	The Switch should support minimum 64000 MAC address		
(b)	**Software Defined Networking (SDN) Capability**		
	OpenFlow protocol capability to enable software-defined networking		
(c)	**Features**		
	The switch should support HTTP redirect function		
	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		
(d)	**Quality of Service (QoS)**		
	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		
	The switch should support Layer 4 prioritization to enable prioritization based on TCP/UDP port numbers		
	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		
	The switch should support Port-based rate limiting to provide per-port ingress-/egress-enforced increased bandwidth		
	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		
	The switch should support Reduced bandwidth to provides per-port, per-queue egress-based reduced bandwidth		
	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		
	The switch should support Remote monitoring (RMON), Extended RMON (XRMON), and sFlow v5 to provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events		
	The switch should support Traffic prioritization allows real-time traffic classification into eight priority levels that will mapped to eight queues		

(e)	**Management**		
	The switch should allow assignment of descriptive names to ports		
	The switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)		
	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		
	The switch should support Multiple configuration files to store easily to the flash image		
	The switch should support Dual flash images to provide independent primary and secondary operating system files for backup while upgrading		
	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		
	The switch should support Unidirectional Link Detection (UDLD)		
(f)	**Connectivity**		
	The switch should support Jumbo frames on Gigabit Ethernet and 10-Gigabit Ethernet ports		
	The switch should support follwing IPv6 feature		
	IPv6 host: enables switch management in an IPv6 network		
	Dual stack (IPv4 and IPv6): transition IPv4 to IPv6, supporting connectivity for both protocols		
	MLD snooping: forward IPv6 multicast traffic to the appropriate interface		
	IPv6 ACL/QoS: support ACL and QoS for IPv6 traffic		
	IPv6 routing: support static, RIPng, OSPFv3 routing protocols		
	6in4 tunneling: support encapsulation of IPv6 traffic in IPv4 packets		
	Security: provide RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping		
(g)	**Performance**		
	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		
	The switch should support Energy-efficient Ethernet (EEE) support: reduces power consumption in accordance with IEEE 802.3az		
(h)	**Resiliency and high availability**		
	The Switch should support stacking up to 9 Switch and support up to 336 Gb/s of stacking throughput. The Switch support Ring, chain, and mesh stacking topologies. Stacking not required from day-1.		

	The Switch should support Virtualized switching to provide simplified management as the switches appear as a single chassis when stacked		
	The switch should support Virtual Router Redundancy Protocol (VRRP)		
	The switch should support Nonstop switching and routing		
	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		
	The switch should support IEEE 802.1s Multiple Spanning Tree		
	The switch should enable loop-free and redundant network topology without using Spanning Tree Protocol; allows a server or switch to connect to two switches using one logical trunk for redundancy and load sharing		
	The switch should provide easy-to-configure link redundancy of active and standby links		
(j)	**Layer 2 switching**		
	The switch should support IEEE 802.1ad QinQ		
	The switch should support VLAN and tagging and support the IEEE 802.1Q standard and 4096 VLANs simultaneously		
	The switch should support IEEE 802.1v protocol VLANs		
	The switch should support MAC-based VLAN		
	The switch should support Rapid Per-VLAN Spanning Tree (RPVST+)		
	The Switch should dynamically load balances across multiple active redundant links to increase available aggregate bandwidth and allow concurrent Layer 3 routing		
	The switch should support GVRP and MVRP		
(k)	**Layer 3 services**		
	The switch should support Loopback interface address		
	The switch should support Route maps		
	The switch should support User datagram protocol (UDP) helper function		
	The switch should support DHCP server		
	The switch should support Bidirectional Forwarding Detection (BFD) to enable link connectivity monitoring and reduces network convergence time for static routing, OSPFv2, and VRRP		
(l)	**Layer 3 routing - Should support from Day-1**		
	The switch should support Static IP routing for both IPv4 and IPv6 networks		
	The switch should support OSPFv2 for IPv4 routing and OSPFv3 for IPv6 routing		

	The switch should support Policy-based routing		
	The switch should support Border Gateway Protocol (BGP)		
	The switch should support RIPv1, RIPv2, and RIPng routing		
(m)	**Security**		
	The switch should support Source-port filtering		
	The switch should support RADIUS/TACACS+		
	The switch should support Secure shell		
	The switch should support Secure Sockets Layer (SSL)		
	The switch should support Port security		
	The switch should support MAC address lockout		
	The switch should support Detection of malicious attacks		
	The switch should support Secure FTP		
	The switch should support Switch management logon security		
	The switch should support Secure management access to deliver secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3		
	The switch should support ICMP throttling		
	The switch should support Identity-driven ACL		
	The switch should support STP BPDU port protection		
	The switch should support Dynamic IP lockdown		
	The switch should support DHCP protection		
	The switch should support Dynamic ARP protection		
	The switch should support STP root guard		
	The Switch should secure management interfaces such as SNMP, Telnet, SSH, SSL, Web, and USB at the desired level		
	The Switch should display a customized security policy when users log in to the switch		
	The switch should support CPU protection		
	The switch should provide filtering based on the IP field, source/destination IP address/subnet and source/destination TCP/UDP port number on a per-VLAN or per-port basis		
	The switch should support IEEE 802.1X		
	The switch should support Web-based authentication		
	The switch should support MAC-based authentication		
	authenticates client with the RADIUS server based on client's MAC address		
	The switch should support Concurrent authentication modes to enables a switch port to accept up to 32 sessions of 802.1X, Web, and MAC authentication		
	The switch should support Private VLAN		

(n)	**Convergence**		
	The switch should support IP multicast snooping (data-driven IGMP)		
	The switch should support LLDP-MED (Media Endpoint Discovery)		
	The switch should support IP multicast routing including PIM sparse and dense modes to route IP multicast traffic		
	The switch should support Auto VLAN configuration for voice		
	The switch should support RADIUS VLAN		
	The switch should support Local MAC Authentication to assign attributes such as VLAN and QoS using locally configured profile that can be a list of MAC prefixes		
(o)	**Environmental Features**		
	Shall support IEEE 802.3az Energy-efficient Ethernet (EEE) to reduce power consumption		
	Operating temperature of 0°C to 45°C		
	Safety and Emission standards including EN 60950; IEC 60950; VCCI Class A; FCC Class A		
(p)	**Warranty and Support**		
	The below Warranty shall be offered directly from the switch OEM.		
	Software upgrades/updates shall be included as part of the warranty		
80	**UTM**		
General Requirements			
(a)	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.		
(b)	The proposed vendor must have a track record of continuous improvement in threat detection (IPS) and must have successfully completed NSS Labs' (or equivalent) NGFW Methodology v7.0 testing with a minimum exploit blocking rate of 99%		
(c)	OEM should be in Leaders quadrant of Gartner's(or equivalent) – in Enterprise Firewall Magic Quadrant as per the latest report		
(d)	Appliance shall be ICSA certified for Firewall, IPS & Gateway Anti Virus functionalities		
81	**Hardware & Interface requirements**		
(a)	14 x 1GE RJ45 inbuilt interfaces, 12 x 1GE SFP interface slots from day one		
(b)	The Appliance should have USB & Console Ports		

82	**Performance and Availability**		
(a)	The Firewall should be on multiprocessor architecture with minimum 20Gbps of Firewall throughput & support of 3,500,000 concurrent sessions, and 200,000 new sessions per second from day one and Firewall Latency should not be more than 3µs		
(b)	Minimum IPS throughput of 4500 Mbps for real world traffic or enterprise mix traffic		
(c)	Minimum Threat Prevention Throughput (measured with Application Control and IPS and Anti-Malware enabled) of 3000 Mbps for real world traffic or enterprise mix traffic		
(d)	IPSec VPN throughput: minimum 10 Gbps		
(e)	Simultaneous VPN tunnels: 1000		
(f)	Proposed solution must support minimum 3.2 Gbps of SSL Inspection throughput		
(g)	Proposed solution must support minimum 10 virtual firewall from day one		
83	**Routing Protocols**		
(a)	Static Routing		
(b)	Policy Based Routing		
(c)	The Firewall should support dynamic routing protocol like RIP, OSPF, BGP, ISIS		
84	**Firewall Features**		
(a)	Firewall should provide application inspection for LDAP, SIP, H.323, SNMP, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, IMAP, NFS etc		
(b)	IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP		
(c)	Allows secure deployment of next-generation IPv6 networks, as well as hybrid environments that require simultaneous, dual stack support of IPv4 and IPv6		
(d)	The firewall should support transparent (Layer 2) firewall or routed (Layer 3) firewall Operation		
(e)	The Firewall should support ISP link load balancing.		
(f)	Firewall should support link aggregation functionality to group multiple ports as single port.		
(g)	Firewall should support minimum VLANS 2048		
(h)	Firewall should support static NAT, policy based NAT and PAT		
(j)	Firewall should support IPSec data encryption		
(k)	It should support the IPSec VPN for both site-site and remote access VPN		
(l)	Firewall should support IPSec NAT traversal.		

(m)	Support for standard access lists and extended access lists to provide supervision and control		
(n)	Control SNMP access through the use of SNMP and MD5 authentication.		
(o)	Firewall system should support virtual tunnel interfaces to provision route-based IPSec VPN		
(p)	The Firewall should have integrated solution for SSL VPN		
(q)	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		
(r)	The solution should have basic server load balancing functinality as an inbuilt feature		
(s)	Licensing should be a per device and not user or IP based (should support unlimited users)		
85	**Integrated IPS Features Set**		
(a)	IPS should have DDoS and DoS anomaly detection and protection mechanism with threshold configuration.		
(b)	Support SYN detection and protection for both targets and IPS devices.		
(c)	The device shall allow administrators to create Custom IPS signatures		
(d)	Should have a built-in Signature and Anomaly based IPS engine on the same unit		
(e)	Signature based detection using real time updated database & should have minimum 10000+ IPS signature database from day one		
(f)	Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)		
(g)	Signature updates do not require reboot of the unit.		
(h)	Configurable IPS filters to selectively implement signatures based on severity, target (client/server) and operating systems		
(j)	IPS Actions: Default, monitor, block, reset, or quarantine		
(k)	Should support packet capture option		
(l)	IP(s) exemption from specified IPS signatures		
(m)	Should support IDS sniffer mode		

86	**AntiVirus & AntiBot**		
(a)	Firewall should support antimalware capabilities, including antivirus, botnet traffic filter and antispyware		
(b)	Solution should be able to detect and prevent unique communication patterns used by BOTs i.e. information about botnet family		
(c)	Solution should be able to block traffic between infected host and remote operator and not to legitimate destination		
(d)	Should have antivirus protection for protocols like HTTP, HTTPS, IMAPS, POP3S, SMTPS protocols etc.		
(e)	Solution should have an option of packet capture for further analysis of the incident		
(f)	Solution should uncover threats hidden in SSL links and communications		
(g)	The AV should scan files that are passing on CIFS protocol		
(h)	The proposed system shall provide ability to allow, block attachments or downloads according to file extensions and/or file types		
(j)	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.		
87	**Other support**		
(a)	Should support features like Web-Filtering, Application-Control & Gateway level DLP from day one		
(b)	The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should support over 250 million webpages in 72+ categories and 68+ languages without external solution, devices or hardware modules.		
(c)	Should support detection over 3,000+ applications in multiple Categories: Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)		
(d)	The product must supports Layer-7 based UTM/Firewall virtualization, and all UTM features should be supported in each virtual firewall like Threat Prevention, IPS, Web filter, Application Control, content filtering etc.		

(e)	The solution should have the flexibility to write security policies based on IP Address & User Name & Endpoint Operating System		
(f)	QoS features like traffic prioritization, differentiated services,. Should support for QoS features for defining the QoS policies.		
(g)	It should support the VOIP traffic filtering		
(h)	Appliance should have identity awareness capabilities		
(j)	The firewall must support Active-Active as well as Active-Passive redundancy.		
(k)	Solution must support VRRP clustering protocol.		
88	**Management & Reporting functionality**		
(a)	Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI.		
(b)	Support accessible through variety of methods, including console port, Telnet, and SSHv2		
(c)	Support for both SNMPv2 and SNMPv2c, providing in-depth visibility into the status of appliances.		
(d)	Should have capability to import configuration and software files for rapid provisioning and deployment using Trivial File Transfer Protocol (TFTP), HTTP, HTTPS		
(e)	The solution should have option for firewall configuration audit & compliance check to be done in automated or manula process		
(f)	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		
(g)	Solution must allow administrator to choose to login in read only or read-write mode		
89	**Lightning Protection System**		
(a)	The Lightening protection should have radius of protection of 79 meters in Zone-I at 5 mtr height.		
(b)	The Lightening Arrestor Should have profiled, in alterable and good conductor structure to generate a forced air circulation at its tip and in prolonged (Venturi System) air intakes and peripheral ejectors.		
(c)	The Lightening should have mechanical stimulation system, no battery or electronics is to be used.		
(d)	Lightening Arrestor should be equally effective of both positive and negative lightning strikes.		

(e)	The necessary fixing bracing PCC/grouting above the building/installation with testing commissioning to entire satisfaction of Engineer- in —charge			
(f)	The installation of the system shall be carried out under the supervision of certified trained engineer from OEM of complete all as specified and directed.			
(g)	The certified Engineer have to produce the Certificate of Certified Engineer from OEM and having knowledge of International Standards.			
(h)	Supply and installation of gun metal elevation rod 2 mtrs long from OEM with necessary bracing clamps, drilling, 1 fixing and grouting arrangement etc complete all as specified and directed			
(j)	Supply and laying underground LT cable PVC insulated, PVC sheathed copper conductor single core,70 sqmm with necessary connection, laying, clipping on insulated pads, saddles all as specified and directed			
(k)	Should provide M&L for Gel compound earthing with earth enhancing compound with 25kgs including copper earth strip of size 25x3 mm with necessary clipping on insulated pads/saddles with earth pit to minimum resistance value complete all as specified and directed			
90	**Network Traffic Manager**			
	BANDWIDTH CONTROLLER			
A	**An additional device for bandwidth control should be provided along with the system. The features are as follows.**			
	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	**(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		
		(ii) Policy-Based Shaping: The system should have the feature to prioritize how and when users, applications and websites can consume bandwidth on network.		
		(iii)Interactive Analytics: Intuitive dashboard feature should be there to visualize activities by all users.		
		(iv)Application Acceleration: The system should support acceleration and caching features.		
		(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.		
		(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.		
	Hardware Features	**(i)Traffic shaping and Acceleration**		
		(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		
		(ii) Interface Capability		
		(a) The system should have 1 x RJ45 based dedicated console port for management purpose.		

		(b) The system should have at least 3 x 1G (Copper) bypass bridge pair and 2x 1G (Fiber) bypass bridge pair. Also, the system should have one additional NIC slot for future expansion.			
		(iii) Physical Parameters			
		(a) Form Factor: -1U rack mountable			
		(b) Power Rating: - 17W @ 0.13A, 22W @ 0.16A (Max)			
		(c) Environment: - 0 deg cel to 40 deg cel, 5% to 90% operating humidity.			
B		**SYSTEM PARAMETERS**			
		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 frame	256		
		Bit rate	2048 Kbps ± 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		
	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		
C	**Interface Support: - The system shall support below mentioned interfaces/Cards.**			
	<u>Network Line Interface-E1 should comply with the following specifications:-</u>			

	Number of ports	1E1 / 4E1 / 3E1		
	Line Rate	2.048 Mbps ± 50 ppm		
	Line Code	AMI or HDB3		
	Input Signal	ITU G.703		
	Output Signal	ITU G.703		
	Framing	ITU G.704		
	Connector	BNC/RJ48C , DB25S for Mini Quad E1		
	Electrical	120 ohm twisted pair		
	Jitter	ITU G.823		
	2* 10/100 Ethernet Router Card with capability to handle 64 WANs should comply with the following specifications			
	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:-		
	(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 (i) Signaling : Type 1,Type 2,Type 3,Type 4,Type 5 transmit only		
	Voice card (12 FXS/ 12 FXO/ 24 FXS/24 FXO) port (interfaces) should comply with the following specifications:-		
	(a) 12 FXS/FXO Connector : Twelve RJ11 (b) 24 FXS/FXO Connector : One RJ21X (c) Alarm conditioning : CGA busy after 2.5 seconds of LOS ,LOF (d) Encoding : A-law or μ-law, user selectable together for all (e) AC Impedance: : balanced 600 or 900 ohms (f) Longitudinal Conversion Loss : > 46dB (g) Cross talk measure : Max -70dBm0 (h) Gain Adjustment : -21 to +10 dB / 0.1dB step transmit & receive (i) Signal/ Distortion : > 25dB with 1004 Hz, 0dBm input (j) Frequency Response : - 0.25 to -1 dB from 300 to 3400 Hz, coincide with ITU-T G.712 (k) Loss adjustment: -21 to +10 dB/ 0.1 dB step transmit and receive (l) Signal / Distortion:. 46 dB with 1004 Hz , 0dBm input (m) Frequency response: - 0 .25 to -1 dB from 300 to 3400 Hz , coincide with ITU-T. (n) Ideal channel noise : Max -65 dB Mop (o) Inter- modulation : coincide with ITU-T B.712 (p) 2Wire return loss : > 2 dB echo , > 20 dB signing (q) FXS loop feed : Nominal -48 V dc with 20 mA current limit (r) Signaling : Loop Start, DTMF, pulse, PLAR, Battery Reverse		

	G.SHDSL Line port (interfaces) should comply with the following specifications:-			
	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		
	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		
	Loopack	DTE Payload Loopback, Local Loopback		
	Voice Card 12 MAG (Magneto)			
	(a) Connector : Twelve RJ11 (b) Alarm Conditioning CGA busy after 2.5 seconds of LOS, LOF. (c) Encoding A-law or μ-law, user selectable together for all. (d) Impedance Balanced 600 or magneto telephone impedance match. (e) Longitudinal Conversion Loss > 46dB. (f) Gain Adjustment -21 to +10 dB / 0.1dB step transmit & receive. (g) Signal/ Distortion > 25dB with 1004 Hz, 0dBm input. (h) Frequency Response - 0.25 to -1 dB from 300 to 3400 Hz, coincide with ITU-T G.712. (i) Idle Channel Noise Max. –65 dBm0p.			

	(j) Min Detectable Ringing Voltage 16 Vrms. (k) Ringing Detectable Across L1 and L2 (Tip and Ring), L1 and GND (Tip and GND) (l) Single Ring Type: ring for 2 sec. and stop, or ring for 4 sec. and stop. (m) Continuous Ring Type: 1 sec on 2 sec off, or 2 sec on 4 sec off (n) Ringing Send across L1 and L2 (Tip and Ring), L1 and GND (Tip and GND). (o) Signaling Magneto MRD (Ringing across Tip and Ring or Tip and Ground). (p) Signaling Bit A, B, C, D Programmable. Signaling is carried transparently by the digitizing process.			
D	**Clock Source**	Internal, E1/T1 Line, External		
E	**Alarm Relay**	Alarm Relay: max. Voltage 3 Vdc/ max. current: 1A Fuse alarm, and performance alarm		
F	**System Configuration Parameters**	Active Configuration, Stored Configuration, and Default Configuration		
G	**Supervisor**			
	RS232 Console Port (VT100)	10 Base-T, Ethernet, SNMP In-band 64 Kbps supports HDLC/PPP, SSH		
H	**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		
	Threshold	Bursty Seconds, Severely Errored Second, Degraded Minutes		
J	**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-bye user define pattern		

K	**Front Panel**			
	LED	1 per V.35-interface, ACO, Power, SYNC/TEST, LOF, BPV, RAI/AIS		
L	**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	0-55°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			
M	**Certification**	EN55022 Class A, EN50024, FCC Part 15 ,Class A, FCC Part 68, CS-03, IEC60950, UL60950, IEC 61850-3, IEEE 1613		
N	**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		
O	**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		
P	**DC Power Source (-48V)**	**(j)** Input 230 VAC (Range 170-264 VAC, single phase, 50 Hz).		
		(k) Output Current :- 8 Amp		
		(l) Size: - 485(W) x385(D) x165(H) mm with screw terminals at front		
		(m) Should have short circuit protection.		

91	**Network Time Server**			
(a)	**Power Supply:**			
	Voltage	230 +/- 10% V AC		
	Frequency	47-55 Hz		
(b)	**Functions / Features :**			
	Time Facility	Using Universal Time co-ordination(UTC)		
	Propagation delay Complensation	Supported		
	Accuracy	# +/- 250 Nanosecond		
	Time Accuracy	Better than 1 PPM		
	LCD Display	Front panel LCD display to show status,time and no. of satellites		
(c)	**Inputs**	GPS Antenna input through BNC connector.		
		Power Supply		
(d)	**Outputs**			
	NTP output (2 nos. customizable) for NTP client access through RJ-45 .Both Ports shall be independent			
	RS232 serial port output (2 Nos)			
	Pulse output: 1 PPS, ½PPM, 1PPM (Configurable).			
	Support Client request per Second	10,000		
(e)	**Antenna**			
	Length of GPS	50 meters		
	Gain	Over 30 DB		
	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			

92	**Smart Rack**				
(a)	System specifications	(WxDxH)	Maximum 800x1200x2150mm(42U)		
		Power supply input	Minimum Dual Feed AC 230V/1P/50Hz.		
		IT Load	3kW		
		Minimum Usable U space for IT Equipments	34 U		
		Installation Site	Should be suitable for Elevated floor installation / general ground installation		
		Utility Entry	Should have provision for both Top/Bottom as Standard		
		System supported languages	Should support English as language for operation by default		
		Cabinet interior lighting	LED - with door limit switch		
		Exterior colors	Black or as per OEM standard		
		Front & back door	Front toughened glass, rear plain dual door		
		Local interface	Colour TouchScreen Display		
		Monitoring	Power, Cooling, Smoke, WLD, temperature and humidity, UPS, door sensor to be integrated for monitoring		
		Sensor	Minimum 1 No. Spot sensor for water leak detection		
			Minimum 1 No. Temperature and humidity sensors		
			Minimum 1 No. Smoke sensor		
			Minimum 1 No. Proximity sensors for doors		
			Minimum 1 No. Beacon- for local alarm		
(b)	Power subsystem	UPS capacity	Minimum 6 kVA UPS		
		UPS rated input	230VAC		
		Input Voltage Range	160 V - 285 V		
		Input Frequency Range	40-70Hz		
		Input Power Factor	0.98		
		Input power consumption meter	Energy meter with digital display should be installed at input to monitor		

		Output Max Power	6kVA/5.4kW		
		Efficiency	94% at 100 % Load in online & 98%in Green Mode		
		Backup Time	15 Mins - 1 Battery Pack		
		RPDU parameters	Basic Rack PDU should be provided, Zero U, 32A, 230V, (20)C13 & (4)C19		
(c)	Cooling subsystem	Total air conditioning cooling Capacity	3.5kW		
		Minimum Air flow	700CMH		
		Air conditioning installation	Should be Rack mount type, not more than 5U		
		Outdoor ambient temperature	-20℃ ~ +45℃		
		Refrigerant	Environmental Friendly R410A		
		Emergency fan module	Minimum 1 No. at front (Inlet) and top (Exhaust)		
			OEM for UPS, Racks, PDU, Sensors should be same including the monitoring software. OEM should be minimum ISO 9001, ISO 14001 and ISO 50001.		

(Lt Col Smita Bagbande)
SO1 (Comn& IT)
HQ DGAR

(Maj Gen Alok Nayesh)
IG AR (S)
HQ DGAR

(Kamlesh Kumar)
Team Commander
NSG

(Dy Comdt Madhvendra Singh)
ITBP

(SI/T Pardeep Kumar)
CRPF

(Asst Comdt Sandesh Kumar)
SSB

(HS Sri Hari)
Dy Director
DCPW

Approved/ ~~Not Approved~~

30/03/21

(Sukhdeep Sangwan)
Lt Gen
Director General Assam Rifles

COUNTER SIGNATURE

(KULDIEP SINGH)
D.G. CRPF, DTE. GENL.

TRAIL DIRECTIVES

IDENTITY AND ACCESS MANAGEMENT SYSTEM

All parameters/ specifications mentioned in QRs will be checked by the Board of Officers by ascertaining/ verifying following checks in the presence of Vendor/ Supplier/Manufacturer. In case of any discrepancies/ problem, the representative of firm will demonstrate the features to the Board of Officers. Further, if proper testing Instruments for testing these parameters are not available with customer, same will be arranged by the firm:

(i) Physical Check :- In this category, specifications of the equipment will be checked by B.O.O. Physical check as per QRs.

(ii) Functional Check :- In this category, supplier will show practically all features/ configuration to the board of officers during trial.

(iii) Submission of Certificate:- Specifications which cannot be checked due to lack of testing facilities/ expertise, certificate of any Govt lab or NABL/ILAC accredited laboratory be submitted by the firm.

Ser No	Description of Requirements	Trial Directives
	GENERAL	
1	The proposed solution should have a central identity manager	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable
2	The multi data centre authentication/access capability should be such that that the session created at one data centre should be synced and respected at a remote data centre while traversing from a locally protected app to a centrally deployed centrally protected application.	
3	Proposed Solution should have a LDAP Directory with Directory Replication Capabilities to maintain a read only copy in remote data centres.	
4	Solution should provide Single Sign On (SSO) with role based access control to users of application.	
5	The solution implemented should offer customizable landing page which can be accessible over Army Data Network. User once authenticated, the landing page should display the list of all applications authorized to him. On choosing any application, the user should be directed to that application with the correct credentials without having to separately login/ sign in. The page should also allow users to manage own attributes e.g. change password, contact details etc.	
6	Solution should integrate all websites/ applications deployed over ADN (approx 500) – to incl static/ dynamic websites and applications (predominantly web based)	
7	The proposed solution should be able to seamlessly integrate with existing Application	
8	Solution should have the capability to integrate with Active Directory.	
9	The solution should run in High Availability (HA)	

10	Solution should support integration with the applications running across different web/ application sever which will be hosted on different OS such as Windows/ Linux/ Solaris.	
11	The sys software should be completely scalable to accommodate the changing Nos of users and applications.	
12	System shall have complete web based administration module	
13	The proposed solution should be FIDO Compliance	
14	Support for interoperability with cross platforms specifically Windows and Linux	
15	IDENTITY and ACCESS MANAGEMENT SOFTWARE provider should be certifying authority under CCA	
16	Support SSL/ TLS of latest version	
17	Solution should have undergone third party Vulnerability Assessment and Penetration Testing (VAPT) and proof of audit certificate should be produced	BOO to check practically on ground
18	**IDENTITY MANAGEMENT SOFTWARE**	
19	Management of Identity profiles should be central with a single repository of identity data.	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable
20	Entire management of identities should be web based.	
21	Solution should be able to create, update, and delete user accounts across the enterprise environment both manually and automatically.	
22	The solution should enable assignment of users to single/ multiple roles.	
23	The solution should have a workflow for provisioning/ de-provisioning of identities.	
24	Solution should provide a graphical interface that allows creating and managing workflows.	
25	Solution should automatically route access requests of users for approval to the destined administrator.	
26	Solution should have ability to delegate approval authority to another person.	
27	Solution should have ability to escalate a request to an alternative approver if the allotted time elapses.	
28	Provisioning solution should provide capability to the approver to provide comments.	
29	Should support withdrawal of non-approved requests	
30	Solution should be able to generate unique user IDs.	
31	Should integrate with PKI to complete user creation process.	
32	Solution should provide auto requisition of PKI token personalization for new users being created	
33	Should support provisioning/ de-provisioning on joining/ movement of personnel on transfers and temporary assignment of roles.	
34	Solution should provide delegated administration.	

35	Solution should be able to define delegated administration by way of both administration (which users, which resources) and capabilities (full account administration, password administration only, etc.).	
36	Solution must support web-based self-service in terms of changing passwords, resetting forgotten passwords retrieving forgotten user login etc	
37	Solution must allow users to view their profile and the resources and the corresponding entitlements they have got access to.	
38	Must have capability to provision user accounts to target systems and applications.	
39	Must have out-of-box connectors available for target systems to carry out user provisioning and reconciliation operations.	
40	The proposed solution should more then 15 Factors of Authentication based on policies defined	BOO to check practically on ground
41	Should have connector development framework to extend support to additional target systems for which out of box connectors are not available.	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable
42	Should have capability to allow administrators to define and enforce global password policy that includes password composition rules like -minimum length- minimum password age- warn after expires, disallow past passwords	
43	Should support complex password rules including maximum repeated characters, minimum numeric characters, alphanumeric characters, uppercase & lowercase characters etc	
44	Should support validation of password provided against the defined password policy.	
45	As part of forgotten password, the solution should have support to challenge the user for security answers to the questions that must have been configured at the time of user creation or self-registration. The manager of the user whose password is being reset must be notified of this password reset.	
46	Solution should allow users to manage their own passwords.	
47	Should have ability to synchronize passwords for multiple systems to the same value to reduce the number of different passwords to be remembered by the user.	
48	Should support delivery of password-change success/ failure status to requestor using mechanisms like email	
49	Users should be able to update personal attribute information, such as address, cell phone number, etc.	
50	Solution should provide a web based front-end for help-desk administrators to use.	
51	Solution should provide a password exclusion list and allow restriction of using old passwords.	
52	Solution should support Role Based Access Control (RBAC).	

53	Solution should report on who had access to what on a given date.	
54	Solution should support the creation of custom audit policies (eg. Separation of Duties) that can be applied during access scans.	
55	Solution should support reporting grouped by the following: by administrator (accounts created, accounts modified, accounts deleted, password changes, complete audit history per administrator, administrative capabilities per administrator) 1. By platform or application (users per platform, provisioning history per platform, who performed the provisioning actions on target platform) 2. By workflow (requests made by user, requests approved by approver, requests denied by approver, requests escalated, delegation of approvals including to whom and for what period of time) 3. By user (audit history per user, accounts/privileges by user, self-service activity by user)	
56	Should support reports related to access policy, request, certification, approval, role, organization, password, resource & entitlement, user.	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable
57	Should support reports like list of all the rogue accounts existing in a resource, list all orphaned accounts etc.	
58	Should support SSL/TCS digital certificate based secure encrypted communication.	
59	Solution should not impose a physical or logical limitation on creation of number of users, while concurrency factor will drive the proposed hardware.	
60	Solution should have the capability of configuring applications for single factor as well as multi factor authentication.	
61	The solution should support all types of web browsers like Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, etc.	
62	**ACCESS MANAGEMENT SOFTWARE**	
63	Should have capability to provide centralized logout	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable
64	Must support integration with PKI Technologies to support certificate based authentication	
65	PKI and Digital Certificates is madatory requirement for Ensure Legal Non-Repudiation	
66	Must support OSCP based live certification validation from the CA Authority under CCA	
67	Should support Certificate Validation against CRL Export Dump	
68	Must give administrators complete visibility and control over real-time user session data including ability to search for and terminate specific sessions	
69	Must support delegated administration at each datacenter location to have visibility on local users	

70	Should allow administrators to enforce constraints on ~~session lifetime idle timeout max number of concurrent~~ sessions		
71	Should be compatible with a variety of web/app servers including Apache, IIS, IBM HTTP, Oracle HTTP, Node JS, Tomcat, Jboss, Web logic, Web sphere		
72	Should have support to log authentication success and failure		
73	Behavioral and Risk based Parameter Detection for user-login to provoke authentication layers in line with real-time adjusted risk profile.		
74	Identity and Access Management Software provider should be certifying authority under CCA.		
75	Support SSL/ TLS of latest version		
76	**HCI Server**		
77	**Hyper-Converged Solution for Cloud**		
(a)	Analyst Ratings	The bidder shall propose Hyper Converged Integrated System from vendors placed in the leader's wave in the Forrester Wave (or equivalent): Hyper converged Infrastructure (HCI). (The bidder will submit the supporting documents for the proposed solution listed in The Forrester Wave Report.)	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
(b)	Analyst Ratings	The bidder shall propose Hyper Converged Integrated System from vendors placed in the leader's quadrant in the Gartner Magic Quadrant (or equivalent) report latest. (The bidder will submit the supporting documents for the proposed solution listed in Gartner Magic Report latest)	
(c)	Benchmarks	Should have a Validated by Login VSI Benchmark for Cloud for both Citrix Xen Desktop and Vm ware Horizon View environments.	
78	**HARDWARE AND PERFORMANCE REQUIREMENTS**		
(a)	Offered Hyper-Converged Capacity	The offered appliance shall be based on modular building blocks of up to one compute node. Each block shall be built using a 2U modular chassis / enclosure housing the compute with respective storage capacity. Each of the Server nodes should be individually serviceable, without shutting down the other Server nodes	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked

(b)	Hardware Support	Solution must be x86 infrastructure agnostic and available to be deployed on a choice of atleast 3 server OEMs	
(c)	Hyper-Converged Infrastructure	Proposed solution must be based on converged IT infrastructure platform that integrates storage, compute, networking, hypervisor, real-time deduplication, compression, and optimization along with powerful data management, data protection, and disaster recovery capabilities in a standard x86 server building block.	
(d)	Functionality	Proposed hardware must be capable to Deduplicate, Compress & Optimize ALL data inline, in real-time, across all storage tiers: All handled with fine data granularity of 8KB data blocks	
(e)	Hardware Specifications	Each Compute Block must come with the following specifications: Dual Intel Intel® Xeon® Gold 5120 Processor or higher Use of All SSD Drives for Caching and Persistent storage. Minimum 5*1.92TB SSD for data storage Minimum 256GB of DDR4 RAM at 2400 Mhz or above 2*40GbE NIC	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
(f)	Resiliency	Proposed solution must be able to support multiple points of failure with no loss of function or data.	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
		During a single component failure (of any type) production services are not affected / degraded in anyway	
		Solution will be deployed as a stretched cluster with Zero RTO. Solution should support stretched cluster deployment in a near site metro DC deployment.	
		Each node should have dedicated non-shared dual-PSU's and should be able to sustain single power supply failure. Solution should not utilize micro-server architecture with shared PSU's and other components.	
		Must be able to sustain minimum of simultaneous 2-HDDs failures per node without DU/DL	
		Must be able to sustain minimum of simultaneous 1-HDDs failures in each node of a cluster and across all nodes in the cluster without DU/DL	
		Must be able to sustain one node failure in the cluster	
		Must be able to sustain 1 NIC port failure	
	SOFTWARE AND FUNCTIONALITY REQUIREMENTS		

(g)	Common Features Included	The proposed solution must be able to provide enhanced functionality by including the following available without compromise in function or performance in both Hybrid as well as All Flash Nodes:	
		Global dedupe, compression and optimization with minimum impact to production workloads and guaranteed CPU and RAM available to user applications	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
		VM-centric policy-based backup/recovery/DR	
		WAN-optimized data protection for VM mobility	
		Unlimited real time data Deduplication Function - licenses Included	
		Unlimited real-time data Compression Function -licenses Included	
		Unlimited capacity Backup Function-Included	
		Should include licenses for multi-site deployments of atleast 3 sites	
(h)	Global Unified Management	Proposed solution must be able to support the following Global Unified Management features	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
		VM-centric management through a single pane of glass via the virtualization manager	
		Programmatic interface to enable automated tasks like failover / failback	
		The ability for a single administrator to manage all aspects of the Hyper-convergence from within the Virtualization Manager for all sites	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
		Leverage existing investment of servers for hosting VMs and applications while taking advantage of the functionality of the solution	
		Globally manage Backup Policies per Datastore or per VM	
(j)	VM-Centricity and Mobility	Proposed solution must be able to support the following VM-Centricity and Mobility feature	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
		Backups for specific VMs	
		Ability to Move specific VMs between datacenters	
		Cloning specific VMs	
		VM-level backup instead of forcing protection at the datastore or protection domain level	
(k)	Data Protection	Proposed solution must be able to support the following Data Protection features	

		Backup functionality as a feature instead of a separate server / software license	
		Backup must be an independent copy of source Virtual Server and must allow restore of deleted or corrupted source Virtual Server	
		Backup to disk functionality as a feature instead of a separate license or appliance	
		Replication across separate datacenter as a feature instead of a separate server / software license.	
		Replication across separate datacenters should be optimized with minimum additional overheads. Data should not need to be rehydrated before being transferred to target datacenter.	
		The ability to carry simultaneous out bi-directional replication between two data centers	
		The ability to replicate Any-to-Any in a Mesh Data Center deployment of more than 3 DC's	
		The ability to define backup policy per datastore, a group of VMs or specific VM	
		Data Protection should have RPO of 10 minutes for local backups	
		The ability to execute backup tasks during office hours without impacting to production workloads	
		Data loss protection against a minimum of 2 simultaneous local hard disks failures per node	
		Data loss protection against a minimum of 1 simultaneous local hard disc failures in all nodes of the cluster	
		Data loss protection against single node failure in cluster	
		The proposed solution must be able to provide backup reports for audit purpose	
(l)	Data Recovery	Proposed solution must be able to support the following Data Recovery features	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
		Data recovery should be indepent of source Virtual Server	
		Solution should provide a backup catalog to allow any Virtual Server to be recovered to any specific point-in-time	
		Data recovery process should be simple with an RTO in minutes	
(m)	Disaster Recovery	Proposed solution must be able to support the following Disaster Recovery features	
		The solution must provide a simple failover operation	
		The solution must allow creation of a	BOO to check

		Runbook to automate recovery of Virtual Servers	practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
		The solution must allow changing of IP address of recovered Virtual Servers to match target datacenter	
		The solution should allow changing Virtual Server settings (example vCPU, vRAM, VMSwitch) if required	
		The solution must allow the option to test DR failover to separate network with no impact to production workloads	
		The solution should have feature to assist in failback process to Primary datacenter	
(n)	Private Cloud License	The Proposed solution must be offered with cloud-ready operating system that is ideal for highly virtualized and software defined datacenter environments.	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
		It must include Shielded Virtual Machines, software defined networking, Storage Spaces Direct, and Storage Replica; customers receive rights to unlimited Operating System Environments (OSEs)	
		The proposed solution must provide following features: Computing environment: The virtual machine includes the same basic parts as a physical computer, such as memory, processor, storage, and networking. Disaster recovery and backup, Optimization.	
		Solution must have features such as live migration, storage migration, and import/export to move or distribute a virtual machine.	
		It must offer a remote connection tool for use with both Windows and Linux.	
		The solution should have Secure boot and shielded virtual machines that protects against malware and other unauthorized access to a virtual machine and its data.	
		The solution must give virtual machine direct and exclusive access to some PCIe hardware devices. Using a device in this way bypasses the virtualization stack, which results in faster access.	
		The solution must prevent a virtual machine's excessive activity from degrading the performance of the host or other virtual machines.	
		A virtual machine can be used as a host and create virtual machines within that virtualized host.	
		The solution must have option to set up Remote direct memory access (RDMA) on network adapters bound to a virtual switch, regardless of whether switch embedded	

		teaming (SET) is also used.	
		The solution must have features to make it harder for virtualisation administrators and malware on the host to inspect, tamper with, or steal data from the state of a shielded virtual machine.	
79	**Core Switch**		
(a)	**Architecture**		
	Shall be 19" Rack Mountable		BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	The switch should have dual hot-swappable power supplies		
	Switch shall have minimum 24 x 1/10G SFP+ ports, populated with 8x10G SR,8x1G SX and 8x1G BaseT transceiver.		
	1 RJ-45 serial console port		
	1 RJ-45 out-of-band management port		
	Should have minimum 2GB SDRAM and 512 MB flash and 13 MB Packet buffer size		
	Shall have switching capacity of minimum 480 Gbps		
	Shall have up to 350 million pps switching throughput		
	The Switch should support minimum 64000 MAC address		
(b)	**Software Defined Networking (SDN) Capability**		
	OpenFlow protocol capability to enable software-defined networking		BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
(c)	**Features**		
	The switch should support HTTP redirect function		
	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		
(d)	**Quality of Service (QoS)**		
	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		
	The switch should support Layer 4 prioritization to enable prioritization based on TCP/UDP port numbers		
	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		
	The switch should support Port-based rate limiting to provide per-port ingress-/egress-enforced increased bandwidth		
	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		BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is
	The switch should support Reduced bandwidth to provides per-port, per-queue egress-based reduced bandwidth		
	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	applicable. Certification to be checked
	The switch should support Remote monitoring (RMON), Extended RMON (XRMON), and sFlow v5 to provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events	
	The switch should support Traffic prioritization allows real-time traffic classification into eight priority levels that will mapped to eight queues	
(e)	**Management**	
	The switch should allow assignment of descriptive names to ports	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	The switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)	
	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	
	The switch should support Multiple configuration files to store easily to the flash image	
	The switch should support Dual flash images to provide independent primary and secondary operating system files for backup while upgrading	
	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	
	The switch should support Unidirectional Link Detection (UDLD)	
(f)	**Connectivity**	
	The switch should support Jumbo frames on Gigabit Ethernet and 10-Gigabit Ethernet ports	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	The switch should support follwing IPv6 feature	
	IPv6 host: enables switch management in an IPv6 network	
	Dual stack (IPv4 and IPv6): transition IPv4 to IPv6, supporting connectivity for both protocols	
	MLD snooping: forward IPv6 multicast traffic to the appropriate interface	
	IPv6 ACL/QoS: support ACL and QoS for IPv6 traffic	
	IPv6 routing: support static, RIPng, OSPFv3 routing protocols	
	6in4 tunneling: support encapsulation of IPv6 traffic in IPv4 packets	
	Security: provide RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping	
(g)	**Performance**	
	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 to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is
	The switch should support Energy-efficient Ethernet (EEE) support: reduces power consumption in accordance with IEEE 802.3az	
(h)	**Resiliency and high availability**	

	The Switch should support stacking up to 9 Switch and support up to 336 Gb/s of stacking throughput. The Switch support Ring, chain, and mesh stacking topologies. Stacking not required from day-1.	applicable. Certification to be checked
	The Switch should support Virtualized switching to provide simplified management as the switches appear as a single chassis when stacked	
	The switch should support Virtual Router Redundancy Protocol (VRRP)	BOO to check practically on ground.
	The switch should support Nonstop switching and routing	
	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	BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	The switch should support IEEE 802.1s Multiple Spanning Tree	BOO to check practically on ground.
	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	BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	The switch should provide easy-to-configure link redundancy of active and standby links	
(j)	**Layer 2 switching**	
	The switch should support IEEE 802.1ad QinQ	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	The switch should support VLAN and tagging and support the IEEE 802.1Q standard and 4096 VLANs simultaneously	
	The switch should support IEEE 802.1v protocol VLANs	
	The switch should support MAC-based VLAN	
	The switch should support Rapid Per-VLAN Spanning Tree (RPVST+)	
	The Switch should dynamically load balances across multiple active redundant links to increase available aggregate bandwidth and allow concurrent Layer 3 routing	
	The switch should support GVRP and MVRP	
(k)	**Layer 3 services**	
	The switch should support Loopback interface address	
	The switch should support Route maps	
	The switch should support User datagram protocol (UDP) helper function	
	The switch should support DHCP server	
	The switch should support Bidirectional Forwarding Detection (BFD) to enable link connectivity monitoring and reduces network convergence time for static routing, OSPFv2, and VRRP	
(l)	**Layer 3 routing - Should support from Day-1**	
	The switch should support Static IP routing for both IPv4 and IPv6 networks	

	The switch should support OSPFv2 for IPv4 routing and OSPFv3 for IPv6 routing	
	The switch should support Policy-based routing	
	The switch should support Border Gateway Protocol (BGP)	
	The switch should support RIPv1, RIPv2, and RIPng routing	
(m)	**Security**	
	The switch should support Source-port filtering	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	The switch should support RADIUS/TACACS+	
	The switch should support Secure shell	
	The switch should support Secure Sockets Layer (SSL)	
	The switch should support Port security	
	The switch should support MAC address lockout	
	The switch should support Detection of malicious attacks	
	The switch should support Secure FTP	
	The switch should support Switch management logon security	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	The switch should support Secure management access to deliver secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3	
	The switch should support ICMP throttling	
	The switch should support Identity-driven ACL	
	The switch should support STP BPDU port protection	
	The switch should support Dynamic IP lockdown	
	The switch should support DHCP protection	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	The switch should support Dynamic ARP protection	
	The switch should support STP root guard	
	The Switch should secure management interfaces such as SNMP, Telnet, SSH, SSL, Web, and USB at the desired level	
	The Switch should display a customized security policy when users log in to the switch	
	The switch should support CPU protection	
	The switch should provide filtering based on the IP field, source/destination IP address/subnet and source/destination TCP/UDP port number on a per-VLAN or per-port basis	
	The switch should support IEEE 802.1X	
	The switch should support Web-based authentication	
	The switch should support MAC-based authentication	
	authenticates client with the RADIUS server based on client's MAC address	
	The switch should support Concurrent authentication modes to enables a switch port to accept up to 32 sessions of 802.1X, Web, and MAC authentication	
	The switch should support Private VLAN	
(n)	**Convergence**	
	The switch should support IP multicast snooping (data-driven IGMP)	BOO to check practically on ground. BOO to check each
	The switch should support LLDP-MED (Media Endpoint Discovery)	

	The switch should support IP multicast routing including PIM sparse and dense modes to route IP multicast traffic	feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	The switch should support Auto VLAN configuration for voice	
	The switch should support RADIUS VLAN	
	The switch should support Local MAC Authentication to assign attributes such as VLAN and QoS using locally configured profile that can be a list of MAC prefixes	
(o)	**Environmental Features**	
	Shall support IEEE 802.3az Energy-efficient Ethernet (EEE) to reduce power consumption	
	Operating temperature of 0°C to 45°C	
	Safety and Emission standards including EN 60950; IEC 60950; VCCI Class A; FCC Class A	
(p)	**Warranty and Support**	
	The below Warranty shall be offered directly from the switch OEM.	
	Software upgrades/updates shall be included as part of the warranty	
80	**UTM**	
	General Requirements	
(a)	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.	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
(b)	The proposed vendor must have a track record of continuous improvement in threat detection (IPS) and must have successfully completed NSS Labs' (or equivalent)NGFW Methodology v7.0 testing with a minimum exploit blocking rate of 99%	
(c)	OEM should be in Leaders quadrant of Gartner's (or equivalent) – in Enterprise Firewall Magic Quadrant as per the latest report	
(d)	Appliance shall be ICSA certified for Firewall, IPS & Gateway Anti Virus functionalities	
81	**Hardware & Interface requirements**	
(a)	14 x 1GE RJ45 inbuilt interfaces, 12 x 1GE SFP interface slots from day one	
(b)	The Appliance should have USB & Console Ports	
82	**Performance and Availability**	
(a)	The Firewall should be on multiprocessor architecture with minimum 20 Gbps of Firewall throughput & support of 3,500,000 concurrent sessions, and 200,000 new sessions per second from day one and Firewall Latency should not be more than 3µs	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
(b)	Minimum IPS throughput of 4500 Mbps for real world traffic or enterprise mix traffic	
(c)	Minimum Threat Prevention Throughput (measured with Application Control and IPS and Anti-Malware enabled) of 3000 Mbps for real world traffic or enterprise mix traffic	
(d)	IPSec VPN throughput: minimum 10 Gbps	
(e)	Simultaneous VPN tunnels: 1000	
(f)	Proposed solution must support minimum 3.2 Gbps of SSL Inspection throughput	
(g)	Proposed solution must support minimum 10 virtual firewall from day one	

83	**Routing Protocols**	
(a)	Static Routing	
(b)	Policy Based Routing	
(c)	The Firewall should support dynamic routing protocol like RIP, OSPF, BGP, ISIS	
84	**Firewall Features**	
(a)	Firewall should provide application inspection for LDAP, SIP, H.323, SNMP, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, IMAP, NFS etc	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
(b)	IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP	
(c)	Allows secure deployment of next-generation IPv6 networks, as well as hybrid environments that require simultaneous, dual stack support of IPv4 and IPv6	
(d)	The firewall should support transparent (Layer 2) firewall or routed (Layer 3) firewall Operation	
(e)	The Firewall should support ISP link load balancing.	
(f)	Firewall should support link aggregation functionality to group multiple ports as single port.	
(g)	Firewall should support minimum VLANS 2048	
(h)	Firewall should support static NAT, policy based NAT and PAT	
(j)	Firewall should support IPSec data encryption	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
(k)	It should support the IPSec VPN for both site-site and remote access VPN	
(l)	Firewall should support IPSec NAT traversal.	
(m)	Support for standard access lists and extended access lists to provide supervision and control	
(n)	Control SNMP access through the use of SNMP and MD5 authentication.	
(o)	Firewall system should support virtual tunnel interfaces to provision route-based IPSec VPN	
(p)	The Firewall should have integrated solution for SSL VPN	
(q)	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	
(r)	The solution should have basic server load balancing functinality as an inbuilt feature	
(s)	Licensing should be a per device and not user or IP based (should support unlimited users)	

85	**Integrated IPS Features Set**	
(a)	IPS should have DDoS and DoS anomaly detection and protection mechanism with threshold configuration.	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
(b)	Support SYN detection and protection for both targets and IPS devices.	
(c)	The device shall allow administrators to create Custom IPS signatures	
(d)	Should have a built-in Signature and Anomaly based IPS engine on the same unit	
(e)	Signature based detection using real time updated database & should have minimum 10000+ IPS signature database from day one	
(f)	Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)	
(g)	Signature updates do not require reboot of the unit.	
(h)	Configurable IPS filters to selectively implement signatures based on severity, target (client/server) and operating systems	
(j)	IPS Actions: Default, monitor, block, reset, or quarantine	
(k)	Should support packet capture option	
(l)	IP(s) exemption from specified IPS signatures	
(m)	Should support IDS sniffer mode	
86	**AntiVirus & AntiBot**	
(a)	Firewall should support antimalware capabilities , including antivirus, botnet traffic filter and antispyware	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
(b)	Solution should be able to detect and prevent unique communication patterns used by BOTs i.e. information about botnet family	
(c)	Solution should be able to block traffic between infected host and remote operator and not to legitimate destination	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
(d)	Should have antivirus protection for protocols like HTTP, HTTPS, IMAPS, POP3S, SMTPS protocols etc.	
(e)	Solution should have an option of packet capture for further analysis of the incident	
(f)	Solution should uncover threats hidden in SSL links and communications	
(g)	The AV should scan files that are passing on CIFS protocol	
(h)	The proposed system shall provide ability to allow, block attachments or downloads according to file extensions and/or file types	

(j)	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.	
87	**Other support**	
(a)	Should support features like Web-Filtering, Application-Control & Gateway level DLP from day one	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
(b)	The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should support over 250 million webpages in 72+ categories and 68+ languages without external solution, devices or hardware modules.	
(c)	Should support detection over 3,000+ applications in multiple Categories: Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)	
(d)	The product must supports Layer-7 based UTM/Firewall virtualization, and all UTM features should be supported in each virtual firewall like Threat Prevention, IPS, Web filter, Application Control, content filtering etc.	
(e)	The solution should have the flexibility to write security policies based on IP Address & User Name & Endpoint Operating System	
(f)	QoS features like traffic prioritization, differentiated services,. Should support for QoS features for defining the QoS policies.	
(g)	It should support the VOIP traffic filtering	
(h)	Appliance should have identity awareness capabilities	
(j)	The firewall must support Active-Active as well as Active-Passive redundancy.	
(k)	Solution must support VRRP clustering protocol.	
88	**Management & Reporting functionality**	
(a)	Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI.	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
(b)	Support accessible through variety of methods, including console port, Telnet, and SSHv2	
(c)	Support for both SNMPv2 and SNMPv2c, providing in-depth visibility into the status of appliances.	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is
(d)	Should have capability to import configuration and software files for rapid provisioning and deployment using Trivial File Transfer Protocol (TFTP), HTTP, HTTPS	
(e)	The solution should have option for firewall configuration audit & compliance check to be done in automated or manula process	

(f)	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		applicable. Certification to be checked
(g)	Solution must allow administrator to choose to login in read only or read-write mode		
89	**Lightning Protection System**		
(a)	The Lightening protection should have radius of protection of 79 meters in Zone-I at 5 mtr height.		BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
(b)	The Lightening Arrestor Should have profiled, in alterable and good conductor structure to generate a forced air circulation at its tip and in prolonged (Venturi System) air intakes and peripheral ejectors.		
(c)	The Lightening should have mechanical stimulation system, no battery or electronics is to be used.		
(d)	Lightening Arrestor should be equally effective of both positive and negative lightning strikes.		
(e)	The necessary fixing bracing PCC/grouting above the building/installation with testing commissioning to entire satisfaction of Engineer- in —charge		
(f)	The installation of the system shall be carried out under the supervision of certified trained engineer from OEM of complete all as specified and directed.		
(g)	The certified Engineer have to produce the Certificate of Certified Engineer from OEM and having knowledge of International Standards.		
(h)	Supply and installation of gun metal elevation rod 2 mtrs long from OEM with necessary bracing clamps, drilling, 1 fixing and grouting arrangement etc complete all as specified and directed		
(j)	Supply and laying underground LT cable PVC insulated, PVC sheathed copper conductor single core,70 sqmm with necessary connection, laying, clipping on insulated pads, saddles all as specified and directed		
(k)	Should provide M&L for Gel compound earthing with earth enhancing compound with 25kgs including copper earth strip of size 25x3 mm with necessary clipping on insulated pads/saddles with earth pit to minimum resistance value complete all as specified and directed		
90	**Network Traffic Manager**		
	BANDWIDTH CONTROLLER		
A	**An additional device for bandwidth control should be provided along with the system. The features are as follows.**		BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is
	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.	applicable. Certification to be checked
		(iv) The system should have the feature to easily monitor recreational traffic like video streaming and P2P sharing.	
	Technical Features	**(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	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
		(ii) Policy-Based Shaping: The system should have the feature to prioritize how and when users, applications and websites can consume bandwidth on network.	
		(iii)Interactive Analytics: Intuitive dashboard feature should be there to visualize activities by all users.	
		(iv)Application Acceleration: The system should support acceleration and caching features.	
		(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.	
		(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.	
	Hardware Features	**(i)Traffic shaping and Acceleration**	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
		(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	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report
		(g) Optimized Connections: - 6,000	
		(h) APS Objects 250	
		(i) SLA Objects 250	
		(j) PDF Reports 60	
		(k) Traffic Policies 1024	
		(ii) Interface Capability	

			(a) The system should have 1 x RJ45 based dedicated console port for management purpose.	where ever it is applicable. Certification to be checked
			(b) The system should have at least 3 x 1G (Copper) bypass bridge pair and 2x 1G (Fiber) bypass bridge pair. Also, the system should have one additional NIC slot for future expansion.	
			(iii) Physical Parameters	
			(a) Form Factor: -1U rack mountable	
			(b) Power Rating: - 17W @ 0.13A, 22W @ 0.16A (Max)	
			(c) Environment: - 0 deg cel to 40 deg cel, 5% to 90% operating humidity.	
B		**SYSTEM PARAMETERS**		
		Speech band	300 to 3400 Hz	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
		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 frame	256	
		Bit rate	2048 Kbps ± 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.	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
		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	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked

	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	
	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	
C	**Interface Support: - The system shall support below mentioned interfaces/Cards.**		BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable.
	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	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	Framing	ITU G.704	
	Connector	BNC/RJ48C , DB25S for Mini Quad E1	
	Electrical	120 ohm twisted pair	
	Jitter	ITU G.823	
	2* 10/100 Ethernet Router Card with capability to handle 64 WANs should comply with the following specifications		

	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	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	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.	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	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:-		
	(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 (i) Signaling : Type 1,Type 2,Type 3,Type 4,Type 5 transmit only		BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	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		BOO to check practically on ground. BOO to check each feature practically on ground and to

	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 (i) Signal/ Distortion : > 25dB with 1004 Hz, 0dBm input (j) Frequency Response : - 0.25 to -1 dB from 300 to 3400 Hz, coincide with ITU-T G.712 (k) Loss adjustment: -21 to +10 dB/ 0.1 dB step transmit and receive (l) Signal / Distortion:. 46 dB with 1004 Hz , 0dBm input (m) Frequency response: - 0 .25 to -1 dB from 300 to 3400 Hz , coincide with ITU-T. (n) Ideal channel noise : Max -65 dB Mop (o) Inter- modulation : coincide with ITU-T B.712 (p) 2Wire return loss : > 2 dB echo , > 20 dB signing (q) FXS loop feed : Nominal -48 V dc with 20 mA current limit (r) Signaling : Loop Start, DTMF, pulse, PLAR, Battery Reverse		generate report where ever it is applicable. Certification to be checked
	G.SHDSL Line port (interfaces) should comply with the following specifications:-		
	Number of ports	2 or 4	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	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 to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked

	Gigabit Ethernet (GbE) Interface	-> Number of Port 2 -> Speed 10/100/1000 BaseT -> Connector RJ45	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	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*	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	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	
	Loopack	DTE Payload Loopback, Local Loopback	
	Voice Card 12 MAG (Magneto)		
	(a) Connector : Twelve RJ11 (b) Alarm Conditioning CGA busy after 2.5 seconds of LOS, LOF. (c) Encoding A-law or μ-law, user selectable together for all. (d) Impedance Balanced 600 or magneto telephone impedance match. (e) Longitudinal Conversion Loss > 46dB. (f) Gain Adjustment -21 to +10 dB / 0.1dB step transmit & receive.		BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be

	(g) Signal/ Distortion > 25dB with 1004 Hz, 0dBm input. (h) Frequency Response - 0.25 to -1 dB from 300 to 3400 Hz, coincide with ITU-T G.712. (i) Idle Channel Noise Max. –65 dBm0p.		checked
	(j) Min Detectable Ringing Voltage 16 Vrms. (k) Ringing Detectable Across L1 and L2 (Tip and Ring), L1 and GND (Tip and GND) (l) Single Ring Type: ring for 2 sec. and stop, or ring for 4 sec. and stop. (m) Continuous Ring Type: 1 sec on 2 sec off, or 2 sec on 4 sec off (n) Ringing Send across L1 and L2 (Tip and Ring), L1 and GND (Tip and GND). (o) Signaling Magneto MRD (Ringing across Tip and Ring or Tip and Ground). (p) Signaling Bit A, B, C, D Programmable. (q) Signaling is carried transparently by the digitizing process.		
D	**Clock Source**	Internal, E1/T1 Line, External	
E	**Alarm Relay**	Alarm Relay: max. Voltage 3 Vdc/ max. current: 1A Fuse alarm, and performance alarm	
F	**System Configuration Parameters**	Active Configuration, Stored Configuration, and Default Configuration	
G	**Supervisor**		
	RS232 Console Port (VT100)	10 Base-T, Ethernet, SNMP In-band 64 Kbps supports HDLC/PPP, SSH	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
H	**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	
	Threshold	Bursty Seconds, Severely Errored Second, Degraded Minutes	
J	**Diagnostics**		
	Loopback	E1/T1 interface (Line Loopback, Payload Loopback, Local Loopback), DTE Loopback (DTE-to-DTE, DTE to Line)	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	Test Pattern	For Controller: 221-1, 215-1, 211-1, 29-1, and 4-bye user define pattern	

K	**Front Panel**		
	LED	1 per V.35-interface, ACO, Power, SYNC/TEST, LOF, BPV, RAI/AIS	
L	**Physical /Electrical**		
	Dimensions	432.4 x 220 x 223.5 mm (W×H×D)	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	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	0-55°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		
M	**Certification**	EN55022 Class A, EN50024, FCC Part 15 ,Class A, FCC Part 68, CS-03, IEC60950, UL60950, IEC 61850-3, IEEE 1613	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
N	**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	
O	**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	
P	**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.	
91	**Network Time Server**		

(a)	**Power Supply:**		BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	Voltage	230 +/- 10% V AC	
	Frequency	47-55 Hz	
(b)	**Functions / Features :**		
	Time Facility	Using Universal Time co-ordination(UTC)	
	Propagation delay Complensation	Supported	
	Accuracy	# +/- 250 Nanosecond	
	Time Accuracy	Better than 1 PPM	

	LCD Display		Front panel LCD display to show status,time and no. of satellites	
(c)	**Inputs**		GPS Antenna input through BNC connector.	
			Power Supply	
(d)	**Outputs**			
	NTP output (2 nos. customizable) for NTP client access through RJ-45 .Both Ports shall be independent			
	RS232 serial port output (2 Nos)			
	Pulse output: 1 PPS, ½PPM, 1PPM (Configurable).			
	Support Client request per Second		10,000	
(e)	**Antenna**			BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
	Length of GPS		50 meters	
	Gain		Over 30 DB	
	RECEIVER,GLOBAL POSITIONING SYSTEM,DISPLAY TYPE:LCD;DISPLAY SIZE:2 X 3.5 INCH;DISPLAY RESOLUTION:240X400 PIXELS;DATA INTERFACE:ETHERNET;PC INTERFACE:ETHERNET;;EX PANSION 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			
92	**Smart Rack**			
(a)	System specifications	(WxDxH)	Maximum 800x1200x2150mm(42U)	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
		Power supply input	Minimum Dual Feed AC 230V/1P/50Hz.	
		IT Load	3kW	
		Minimum Usable U space for IT Equipments	34 U	
		Installation Site	Should be suitable for Elevated floor installation / general ground	

			installation	
		Utility Entry	Should have provision for both Top/Bottom as Standard	
		System supported languages	Should support English as language for operation by default	
		Cabinet interior lighting	LED - with door limit switch	
		Exterior colors	Black or as per OEM standard	
		Front & back door	Front toughened glass, rear plain dual door	
		Local interface	Colour TouchScreen Display	
		Monitoring	Power, Cooling, Smoke, WLD, temperature and humidity, UPS, door sensor to be integrated for monitoring	
		Sensor	Minimum 1 No. Spot sensor for water leak detection	
			Minimum 1 No. Temperature and humidity sensors	
			Minimum 1 No. Smoke sensor	
			Minimum 1 No. Proximity sensors for doors	
			Minimum 1 No. Beacon-for local alarm	
(b)	Power subsystem	UPS capacity	Minimum 6 kVA UPS	BOO to check practically on ground. BOO to check each feature practically on ground and to generate report where ever it is applicable. Certification to be checked
		UPS rated input	230VAC	
		Input Voltage Range	160 V - 285 V	
		Input Frequency Range	40-70Hz	
		Input Power Factor	0.98	
		Input power consumption meter	Energy meter with digital display should be installed at input to monitor	
		Output Max Power	6kVA/5.4kW	
		Efficiency	94% at 100 % Load in online & 98%in Green Mode	
		Backup Time	15 Mins - 1 Battery Pack	

		RPDU parameters	Basic Rack PDU should be provided, Zero U, 32A, 230V, (20)C13 & (4)C19	
(c)	Cooling subsystem	Total air conditioning cooling Capacity	3.5kW	
		Minimum Air flow	700CMH	
		Air conditioning installation	Should be Rack mount type, not more than 5U	
		Outdoor ambient temperature	-20□ ~ +45□	
		Refrigerant	Environmental Friendly R410A	
		Emergency fan module	Minimum 1 No. at front (Inlet) and top (Exhaust)	
			OEM for UPS, Racks, PDU, Sensors should be same including the monitoring software. OEM should be minimum ISO 9001, ISO 14001 and ISO 50001.	

(Lt Col Smita Bagbande)
SO1 (Comn & IT)
HQ DGAR

(Maj Gen Alok Naresh)
IG AR (S)
HQ DGAR

(Kamlesh Kumar)
Team Commander
NSG

(Dy Comdt Madhvendra Singh)
ITBP

(SI/T Pardeep Kumar)
CRPF

(Asst Comdt Sandesh Kumar)
SSB

(HS Sri Hari)
Dy Director
DCPW

Approved/ ~~Not Approved~~

30/03/21

(Sukhdeep Sangwan)
Lt Gen
Director General Assam Rifles

COUNTER SIGNATURE

(KULDIEP SINGH)
D.G. CRPF, DTE. GENL.