Annexure _1

Specification for rte Hardware and Scanning Services

a. Rack mount/Blade Server for Data centre:

Blade Chassis

1	Form Factor	Rack mountable/ blade chassis with minimum 14 blades per chassis max 10U form factor
2	Management modules	Should be configured with redundant management modules. Should support Hot Pluggable & Redundant Management Modules with onboard KVM functionality or KVM over IP. Solution Should provide management capabilities to manage controlling Power, Fan management, Chassis and compute node initialization, Switch management, Resource discovery and inventory management, Resource alerts and monitoring management, Chassis and compute node power management and diagnostics for elements including Chassis, I/O options and Computer nodes. Support simultaneous remote access for different servers in the enclosure.
3	Power Supply	Should be provided with N+N redundant hot swappable power supplies & fan modules. Power Supply should have 80 PLUS Platinum Efficiency Rating
4	Cooling	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics. Should be provided with the capability to set power consumption limit per blade as well as per enclosure basis, based on need. Fan Module should be controlled through temperature sensors for achieving variable speed with respect to environmental conditions
5	Midplane	Chassis should have a highly reliable passive mid plane for providing connectivity of the shared resources to the compute nodes in a highly reliable manner
6	I/O interconnect Switches	Should be populated with Redundant Converged DCB compliant L2 Switches and should have minimum 4 * 10Gbps SFP+ Uplink Ports and minimum 4 * 8Gbps FC Uplink Ports per switch
7	Management	The proposed solution should have an Integrated management where integration of Servers, Storage, Networking and other available hardware resources in the solution are managed using a common GUI. Management/controlling software have to be from the OEM itself. Should support automatic discovery, identification, and fault management. Should provide configuration & provisioning of Blade Servers
8	Monitoring & Alerting	Complete GUI with view of the individual blade chassis, multiple chassis in a rack, blade servers, power consumption at chassis level and blade level. Comprehensive web enabled system management tool that monitors the system health, environment, critical action etc. The system should be able to alert on maximum number of components. The components covered under alerting mechanism should at least include Server components, Storage components, Switch components and Chassis components.

9	Deployment & Remote Management	Complete Hardware based Remote Administration from a standard web-browser with Event logging, detailed server status, Logs, Alert Forwarding, virtual control, remote graphical console, Remote Power Control / Shutdown, Virtual Media for Remote boot and configuration, Virtual Text and Graphical Control. The blade system should have the capability of managing all the blades in the same enclosure simultaneously

b. Server

MS SQL Database servers -04 nos		
Sl. No	**Component**	**Specification**
1	Processor	2 * Intel Xeon Processor E5-2620v3 or higher, 6Core, 2.4 GHz
2	Chipset	Intel Chipset/ OEM Chipset
3	DIMM Support	24 DIMM Slots with support for 16GB/32GB DDR4 ECC Memory DIMMs, supporting minimum 1866 MT/s upgradable to minimum 768GB
4	Memory	Should be populated with minimum 32GB RAM using DDR4 Memory modules
5	Memory protection	Advanced ECC with multi-bit error protection supporting technologies of memory mirroring
6	Drive Bays	2x2.5" Hot-plug SAS or better
7	RAID Controller	Integrated hardware RAID Controllers that support RAID 0, 1
8	Hard Disk	2x300 GB, SAS, 15K RPM, 2.5" or higher
9	NIC	4 x 10Gbps Converged Network physical ports
10	Remote management	▪ Should be IPMI compliant ▪ Should be able to provide full out of band remote management capabilities, browser support, troubleshoot and remediate the Server from any location ▪ Should be able to power on & off the Server remotely ▪ Should be capable of remotely deploying, updating, monitor and maintaining servers with or without a systems management software agent installed and provide virtual KVM functionality ▪ Should be capable of remotely doing firmware, BIOS updates and roll back, independent of the OS installed ▪ Should be capable of providing power monitoring & power control at server hardware level for power savings ▪ Must have the ability to map the remote media to the server and ability to transfer files from the user's desktop/laptop folders to the remote server with only the network connectivity
11	Server Management S/w	Server management software should be from the same OEM brand as that of the server
12	OS Compatibility	Server should support operating systems such as Microsoft Windows Server (2012/2012R2), Red Hat Enterprise Linux 6.x
		Microsoft Hyper-V, VMware ESX 5.x & above, Citrix XenServer
13	Ports	USB ports: one external. One internal for boot device, security key, or mass storage device

14	Warranty	3 Yrs 24 x 7 on-site Comprehensive Warranty should be provided by OEM

c. **SPP Web Front-end Servers**

SPP Web Front-end Servers – 2 Nos		
Sl. No	**Component**	**Specification**
1	Processor	2 * Intel Xeon Processor E5-2640v3 or higher, 8Core, 2.6 GHz
2	Chipset	Intel Chipset/ OEM Chipset
3	DIMM Support	24 DIMM Slots with support for 16GB/32GB DDR4 ECC Memory DIMMs, supporting minimum 1866 MT/s upgradable to minimum 768GB
4	Memory	Should be populated with minimum 32GB RAM using DDR4 Memory modules
5	Memory protection	Advanced ECC with multi-bit error protection supporting technologies of memory mirroring
6	Drive Bays	2x2.5" Hot-plug SAS or better
7	RAID Controller	Integrated hardware RAID Controllers that support RAID 0, 1
8	Hard Disk	2x300 GB, SAS, 15K RPM, 2.5" or higher
9	NIC	4 x 10Gbps Converged Network physical ports
10	Remote management	▪ Should be IPMI compliant ▪ Should be able to provide full out of band remote management capabilities, browser support, troubleshoot and remediate the Server from any location ▪ Should be able to power on & off the Server remotely Should be capable of remotely deploying, updating, monitor and maintaining servers with or without a systems management software agent installed and provide virtual KVM functionality ▪ Should be capable of remotely doing firmware, BIOS updates and roll back, independent of the OS installed ▪ Should be capable of providing power monitoring & power control at server hardware level for power savings ▪ Must have the ability to map the remote media to the server and ability to transfer files from the user's desktop/laptop folders to the remote server with only the network connectivity
11	Server Management S/w	Server management software should be from the same OEM brand as that of the server
12	OS Compatibility	Server should support operating systems such as Microsoft Windows Server (2012/2012R2), Red Hat Enterprise Linux 6.x
		Microsoft Hyper-V, VMware ESX 5.x & above, Citrix XenServer
13	Ports	USB ports: one external. One internal for boot device, security key, or mass storage device
14	Warranty	3 Yrs 24 x 7 on-site Comprehensive Warranty should be provided by OEM

d. **Application cum Web servers**

Application cum Web servers – 3 Nos		
Sl. No	**Component**	**Specification**
1	Processor	2 * Intel Xeon Processor E5-2640v3 or higher, 8Core, 2.6 GHz
2	Chipset	Intel Chipset/ OEM Chipset
3	DIMM Support	24 DIMM Slots with support for 16GB/32GB DDR4 ECC Memory DIMMs, supporting minimum 1866 MT/s upgradable to minimum 768GB
4	Memory	Should be populated with minimum 32GB RAM using DDR4 Memory modules
5	Memory protection	Advanced ECC with multi-bit error protection supporting technologies of memory mirroring
6	Drive Bays	2x2.5" Hot-plug SAS or better
7	RAID Controller	Integrated hardware RAID Controllers that support RAID 0, 1
8	Hard Disk	2x300 GB, SAS, 15K RPM, 2.5" or higher
9	NIC	4 x 10Gbps Converged Network physical ports
10	Remote management	▪ Should be IPMI compliant ▪ Should be able to provide full out of band remote management capabilities, browser support, troubleshoot and remediate the Server from any location ▪ Should be able to power on & off the Server remotely ▪ Should be capable of remotely deploying, updating, monitor and maintaining servers with or without a systems management software agent installed and provide virtual KVM functionality ▪ Should be capable of remotely doing firmware, BIOS updates and roll back, independent of the OS installed ▪ Should be capable of providing power monitoring & power control at server hardware level for power savings ▪ Must have the ability to map the remote media to the server and ability to transfer files from the user's desktop/laptop folders to the remote server with only the network connectivity
11	Server Management S/w	Server management software should be from the same OEM brand as that of the server
12	OS Compatibility	Server should support operating systems such as Microsoft Windows Server (2012/2012R2), Red Hat Enterprise Linux 6.x
		Microsoft Hyper-V, VMware ESX 5.x & above, Citrix XenServer
13	Ports	USB ports: one external. One internal for boot device, security key, or mass storage device
14	Warranty	3 Yrs 24 x 7 on-site Comprehensive Warranty should be provided by OEM

e. **Anti-Virus/Security Server**

Anti-Virus/Security Server - 1 No		
Sl. No	**Component**	**Specification**
1	Processor	2 * Intel Xeon Processor E5-2620v3 or higher, 6Core, 2.4 GHz
2	Chipset	Intel Chipset/ OEM Chipset
3	DIMM Support	24 DIMM Slots with support for 16GB/32GB DDR4 ECC Memory DIMMs, supporting minimum 1866 MT/s upgradable to minimum 768GB

4	Memory	Should be populated with minimum 32GB RAM using DDR4 Memory modules
5	Memory protection	Advanced ECC with multi-bit error protection supporting technologies of memory mirroring
6	Drive Bays	2x2.5" Hot-plug SAS or better
7	RAID Controller	Integrated hardware RAID Controllers that support RAID 0, 1
8	Hard Disk	2x300 GB, SAS, 15K RPM, 2.5" or higher
9	NIC	4 x 10Gbps Converged Network physical ports
10	Remote management	▪ Should be IPMI compliant ▪ Should be able to provide full out of band remote management capabilities, browser support, troubleshoot and remediate the Server from any location ▪ Should be able to power on & off the Server remotely ▪ Should be capable of remotely deploying, updating, monitor and maintaining servers with or without a systems management software agent installed and provide virtual KVM functionality ▪ Should be capable of remotely doing firmware, BIOS updates and roll back, independent of the OS installed ▪ Should be capable of providing power monitoring & power control at server hardware level for power savings ▪ Must have the ability to map the remote media to the server and ability to transfer files from the user's desktop/laptop folders to the remote server with only the network connectivity
11	Server Management Software	Server management software should be from the same OEM brand as that of the server
12	OS Compatibility	Server should support operating systems such as Microsoft Windows Server (2012/2012R2), Red Hat Enterprise Linux 6.x
		Microsoft Hyper-V, VMware ESX 5.x & above, Citrix XenServer
13	Ports	USB ports: one external. One internal for boot device, security key, or mass storage device
14	Warranty	3 Yrs 24 x 7 on-site Comprehensive Warranty should be provided by OEM

f. Server for application software at the Higher Education Council for NIC

Item	Description of Requirement
Chassis	2 U Rack Mountable
CPU	Two Intel® Xeon ® E5-2600 Processor /AMD equivalent product family processor with 2.5MB per core Cache ; Proposed servers should have Minimum 2.0 Ghz and four Cores per CPU.
Motherboard	Intel® C600 Chipset
Memory	32 GB DDR3 Registered (RDIMM) memory operating at 1333MHz, scalable to 256 GB.
Memory Protection	Advanced ECC (multi-bit error protection), Mirroring mode, Lockstep mode
Bays	Minimum 16 Hot Plug 2.5" hard disk bays / 8 Hot Plug 3.5" hard Disk Bays + CDROM/DVD Bay
Hard disk drive	3 X 146/300 GB SAS Hot plug 2.5" HDDs
Controller	SAS Raid Controller with RAID 0/1/1+0/5/5+0 with 256/512MB battery backed write cache (onboard or in a PCI Express slot).

Networking features	Dual Port Multifunction Gigabit Server Adapters (four ports total, Embedded or Slot based) with TCP/IP Offload Engine, including support for Accelerated iSCSI
Ports	USB 2.0 support With 5 total ports: (2) ports up front; (2) ports in back; (1) port internal
Bus Slots	Min. Seven PCI-Express slots (1 x16 PCIe Slot & 6 x8 PCIe Slots)
Optical drive (Internal / External)	DVD/CD-RW combo drive
Power Supply	Redundant Power Supplies
Fans	Redundant Fans
Compliance	The quoted system must conform to the following norms: FCC Class A, RoHS, CSA
Security	Hardware-based system security feature that can securely store information, such as passwords and encryption keys, which can be used to authenticate the platform. It can also be used to store platform measurements that help ensure that the platform remains trustworthy.
OS Support	Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Oracle Enterprise Linux (OEL), Vmware, Citrix XenServer
Warranty	3 year warranty. Pre failure warranty on CPU, Memory and Hard disks
Remote Manageability Software	System remote management software should support browser based Graphical Remote Console
Server	The Server Management Software should be of the same brand as of the server supplier.

g. SAN Storage:

Sl. No	**Description**
1	**Controller: NAS :** The NAS should be a distributed file system, with a minimum of 1 x dual controller nodes in an active-active mode. The front end connectivity to the client network should be on 4 x 10Gbps across the controller pair. The backend connectivity to the SAN storage should be on FC/10 Gbps, however, these ports should be additional in both NAS & SAN. The controller pair should be provided with a minimum of 48GB of system memory for Read/Write caching. The controller pair should not be more than 2U form factor. The NAS should support option to scale the controllers to a minimum of 4 controller pairs without changing the model, for future growth requirements. All NAS controllers in the NAS cluster should load-balance I/O, even as new appliances are added to the cluster. Incoming connections should be automatically balanced across all the physical ports in the client network and across all the controllers in the cluster.
2	**SAN:** The backend SAN storage should be provided with dual controllers in Active-Active mode. Each controller should be with Single/Dual CPU 4-cores or above. The controller pair should not be more than 2U form factor. The controller pair should be configured with a minimum of 4 x 8Gbps FC and 2 x 10Gbps SFP+ ports for either host connectivity or replication with necessary cables. The backend disk shelf connectivity should be preferably 4-lane, 6Gps SAS. The controller pair should have a minimum of 32GB of system memory. The SAN controllers should be able to scale to a minimum of 4 pairs, with addition of controllers. There should not be change in the model.
3	**RAID :** The storage sub-system should support redundancy levels offered by RAID0, RAID 10, RAID 5 and RAID 6 & DM.
4	**Capacity : NAS :** Proposed storage system should be configured with 56TB usable capacity on RAID6 (8D+2P) with 1TB NL-SAS drives. The storage should support SAS 6Gbps 15/10K, NL-SAS 7.2K & SSD's SLC/MLC with auto tiering. Need to add 1 Hot spare for every 20 drives & should be global.
5	**Capacity: SAN :** Proposed storage system should be configured with 5TB usable capacity on RAID10

	with SSD drives. 1 Hot spare to be additional for every 20 drives
6	**Design:** The system must be specifically designed to provide enterprise NAS functionality. The NAS OS should be of hardened UNIX/LINUX flavors & the same should be supported by the OEM. The storage should also support connectivity of the servers for block access, without replacing the controllers. The NAS controllers are preferred to be in gateway mode. However, the management interface for both NAS & SAN should be unified, with a single pane of glass management. The NAS gateway & the backend Block storage should be from the same manufacturer/OEM.
7	**Scalability:** The proposed system should be scalable to at least 175+ drives without replacing the controllers. Future augmentation with high capacity drives should be possible with the proposed solution without affecting the existing configuration and performance.
8	**Client Network Access:**The NAS system should have a minimum of 2 x 10Gb ports per controller with Base-T dedicated for serving data to clients. The Connectivity to the SAN should be over 8Gbps FC & there should be a minimum of 2 ports per controller.
9	**Throughput** : Sequential read/write throughput of the system should be at least 4GBpswith RAID 6 redundancy. Throughput should be linearly scalable to 10GBps.
10	The Storage should support Synchronous & Asynchronous Replication of data for SAN & asynchronous replication for NAS. The license for file replication to be provided for the entire capacity.
11	The storage should support tiering with additional license. Tiering should not be dependent on SSD's. The storage should support tiering between spinning drives, between SSD's & between Spinning & SSD's.
12	The storage should be able to add all the disk types to a single pool. The storage should support migration of data from one RAID to another, without any user intervention & performance de-gradation.
13	Should be configured with Thin-provisioning & file level De-Dupe & Compression. Any license required for these functionality, should be provide for the whole capacity of the storage.
14	The storage should be configured with Re-Direct on Write Snapshots. The policy of NAS snapshots should be set at NAS volume level.
15	**Availability**: Any maintenance activity on the storage controller, OS up-gradation, file system expansion should be performed online without causing any downtime. Architecture should have no single point failure - data should remain accessible even in the event of any single device failure without requiring any intervention from a system administrator. Performance offered by the system after a single failure (of any component) should not be less than 50% of the original performance. Redundancy to meet this requirement should be part of the design.
16	**External Tape backup**: Storage system should support network backups via NDMP v4 or above. Full, incremental and differential backups should be supported. Two-way or Three-way NDMP backup modes should be supported.
17	**Software:** The storage should be provided with fully functional management software, which can also generate reports on the usage patterns, capacity utilization etc & should provide a minimum of 30 days historical report stored at the onsite management server. Any additional components required for this should be part of the BOM proposed. All software licenses procured should be transferred, while replacing the existing storage, without any additional cost.
18	All accessories required for integration (e.g. connectors, adapters, media converters, and transceivers) and other hardware and software elements including licensing required for realizing the proposed system has to be offered as turnkey solution.
19	**Power Supply:** The offered storage solution should be provisioned with hot swappable redundant power supply units in N+N Redundancy.
20	**Cooling:** The offered storage solution should be provisioned with hot swappable cooling fans in N+N

	Redundancy.
21	**Protocols Supported:** Should support SMB3.0, NFS V3/4, FC, iSCSI, for use with different applications and avoid any protocol related buying in future. Any hardware/software required for this functionality shall be supplied and external appliance should have high availability architecture for data and management.
22	**Licensing:** All the relevant licenses on the storage system must be provided for the offered capacity supported by the system from day one.
23	**Authentication:** Should support authentication with LDAP/AD
24	**Management**: Configuration, management and performance monitoring of the entire system should be possible through a single management GUI. Any additional license needed to provide this functionality should be included. Easy to use GUI based and web enabled administration interface for configuration, storage management. The storage management GUI should allow managing more than one single system from the GUI and even remote systems. Performance monitoring tool or software should be provided and the same will need to be licensed for the full capacity and maximum servers supported by the array. The management software should also provide user readable reporting feature, without the need to send the files to the OEM for report generation. The report should provide details like Port throughputs, bandwidth, back-end throughputs etc.
25	**Client OS support:** Should support heterogeneous clients connecting to the system. Clients include Microsoft Windows, Red Hat Linux, SUSE Linux and Ubuntu Linux
26	**Warranty**:24 x 7 on-site Comprehensive Warranty for Hardware & Software components for 5 years should be provided by OEM 24X7 with maximum 4 hour response.
27	**Remote Diagnostics/ Maintenance:** The proposed system should support Web based, Email facility for remote service & also support dial-in / dial-out to report errors and warnings.

h. SAN Switch:

Each Switch should be modular supporting FCoE and Native FC Modules in the same switch, and built with redundant RPS Support.
Each Switch should be able to support at least 36 ports of 1/10Gig FCOE using SFP+ ports and 12 ports of 2/4/8 Gbps of native FC ports in the same switch.
Each Switch should be Configured with redundant power supply & cooling Fans
The switch should be modular in nature
Each switch should be 1U in rack space
Each Switch should be inserted with 20 No's of 1000 Base T Transceiver in the SFP+ Ports for user connectivity.
Each Switch should be inserted with 4 No's of SFP+ SR Transceiver.
Each Switch should be inserted with 6 Nos of 8 Gbps FC Transceiver.
Each Switch should be supported with 4 No's of 40QSFP Gig ports.
Each Switch should be considered with RJ 45 20 No's of 10 Mtrs patchcord, and 6 No's of LC –LC MM Fiber patchcord, and 2 No's of 40Gig 1QSFP DAC cable of 1 Mtr length.
MAC addresses: 128K
IPv4 routes: 16K
Should be able to support BGP, OSPF, IS-IS, Multicast (IGMP v1, v2 and V3), availability (MSTP, RSTP, VRRP, STP), VLAN, DCB, Fiber channel, FCoE Features and SDN.
Switch fabric capacity: 1.28 Tbps (full-duplex)
600 Gbps (half-duplex)

Forwarding capacity: 960 Mpps
Link aggregation: 8 links per group, 128 groups per stack
Queues per port: 4 queues
Layer 2 VLANs: 4K
MSTP : 64 instances
Line-rate Layer 2 switching: all protocols, including IPv4 and IPv6
Line-rate Layer 3 routing: IPv4 and IPv6
802.1AB LLDP
802.1ag Connectivity fault Management
802.1p L2 Prioritization
802.3ad Link Aggregation with LACP
802.3ae 10 Gigabit Ethernet (10GBASE-X)
802.3ba 40 Gigabit Ethernet (40GBase-SR4, 40GBase-CR4) on optical ports
802.3x Flow Control
802.3z Gigabit Ethernet (1000BASE-X)
802.1Qbb PFC
802.1Qaz ETS
ANSI/TIA-1057 LLDP-MED
MTU 12K bytes
802.1AB LLDP
802.1ag Connectivity fault Management
802.1p L2 Prioritization
802.3ad Link Aggregation with LACP
802.3ae 10 Gigabit Ethernet (10GBASE-X)
802.3ba 40 Gigabit Ethernet (40GBase-SR4, 40GBase-CR4) on optical ports

i. Network Bandwidth Optimization Tool:-

	WAN/Network Optimizer
	Introduction
1	The Technical Specifications is designed to define the Wan Optimization Solution at hub and remote/branch locations for Application optimization and accelerated application access.
2	Purpose built platform to reduce the impact of network congestion, latency and packet loss that dramatically slows end user response times
	Design Parameters - Remote/Branch Locations
4	Should be dedicated appliance based solution (not router integrated module) with purpose built hardware for high performance.
5	Branch appliance should support 4 Mbps of optimized bandwidth and 500 optimized TCP flows
6	Solution must support single instance store technology to store content on disk. Storage support should be 500GB
7	Network Interface: 2 numbers of Inline Gigabit Ports and 2 dedicated management ports for centralized management and monitoring. Scalability: The Appliance must be able to scale to support 10 Mbps of optimized bandwidth and 1000 TCP flows by without changing the physical appliance to a larger appliance
	Design Parameters - Hub Location

8	should be dedicated appliance based solution with purpose built hardware for high performance.
9	Branch appliance should support 300 Mbps of optimized bandwidth and 40,000 optimized TCP flows
10	solution must support single instance store technology to store content on disk. Storage support should be 2TB
11	Network Interface: 2 numbers of Inline Gigabit Ports and 2 dedicated management ports for centralized management and monitoring.
12	Scalability: The Appliance must be able to scale to support 1000 Mbps of optimized bandwidth and 100,000 TCP flows without changing the physical appliance to a larger appliance
	General Features
13	Should support TCP optimization for efficient data transfer across WAN, higher bandwidth utilization, faster recovery after any packet loss. TCP optimization must include Windows Scaling, Slow start with congestion avoidance, Fast Convergence & Selective acknowledgements to ensure efficient throughput in Long FAT Networks
14	Should support standard compression mechanism and stream based differencing to avoid transmission of content that has been previously received in the local data store.
15	The solution should be able to support & recognize repetitive byte patterns, and be able to replace the repetitive data with reference records and other metadata.
16	Network de-duplication to avoid the repeated content across the WAN and to ensure efficient utilization WAN bandwidth. content should be stored on disk at both ends of the network and when similar content is seen again, messages are sent to the peer device to replay the content locally rather than re-transmitting the data across the WAN
17	content aware de-duplication: solution should able to distinguish protocol used to transfer the contents for efficient disk utilization and better performance.
18	Single instance store: Solution should support single universal dictionary for maintaining larger histories without requiring per peer data store. Architecture of the solution must ensure that single copy of any content is maintained irrespective of the peer is being sent to.
19	Application acceleration blueprints: Solution should provide Layer 7 application intelligence to mitigate not only the chattiness of legacy protocols but also to improve the performance of protocols like HTTP or iSCSI when they are used over a WAN. Should support real time payload identification for de-duplication.
20	HTTP acceleration : Solution must support HTTP application blueprint address the protocol chattiness issues that affect the HTTP performance
21	Should support "Pre-Cache Acceleration" (PCA) which helps speed up the rendering of Web pages by eliminating repetitive trips over the WAN connection to validate the freshness of content. client's browser must query the remote server with an HTTP 304 request for the "freshness value" of the object
22	HTTPs acceleration: Support for HTTPS application acceleration blueprint to address protocol chattiness and performance issues. Solution must able to intercept the HTTPS traffic for content de-duplication and protocol optimization.
23	HTTPS acceleration blueprint should to break the end to end security trust model, certificates must be only loaded on datacenter/Hub location device and not on the remote location devices.
24	Acceleration device must support PFX and PKCS#12 certificate format.
25	MAPI acceleration: The solution should natively address protocol chattiness issues for the MAPI protocol used by Exchange servers and Outlook clients using application specific blueprints
26	CIFS acceleration: The WAN optimization solution must address protocol chattiness issues for the CIFS protocol
27	The CIFS Blueprint should support multiple techniques including read-ahead, write-behind and directory optimizations in order to improve the throughput

27	ICA acceleration: support for ICA blueprints to address protocol chattiness and performance issues. Solution must be able to intercept ICA traffic for content de-duplication and protocol optimization without any server side configuration changes.
28	The solution should be able to define classes of application traffic and apply Quality-of-Service policies to each class
29	The solution should support traffic shaping and provision to allocate Guaranteed Bandwidth to each class of applications
30	The solution should be able to allocate a maximum bandwidth usage cap to each class of traffic. The solution must allow usage to burst above the maximum bandwidth usage cap if no other traffic classes attempt to utilize the available bandwidth
	Deployment
31	Should support various deployment modes including inline mode, out-of-line mode & out-of-path for seamless integration with other network devices
32	Out-of-line mode operation must support WCCPv2 for traffic redirection. WCCP forwarding & return methods must include Generic routing encapsulation (GRE) and layer2 switching
33	Must have built-in blackhole detection support - should not impact traffic flow if optimization appliance is not in service.
34	Out-of-line mode operation should also support VRRP and policy based routing (PBR) to redirect traffic to Wan optimization appliances.
35	should support correct addressing mode of operation for out-of-path deployment
36	Solution should be deployed transparently into the existing/proposed WAN environment and should not modify any network characteristics like IP addresses, headers or port numbers etc.
37	Should support correct addressing with server side transparency (CAST) mode of operation. Correct Addressing with Server-Side Transparency should provide Correct Addressing mode on the WAN and Transparent Addressing on the LAN
38	The solution must support auto-discovery of remote peer devices and dynamically detect the presence of any other WAN optimization devices. Peers are automatically removed from the discovered list if a connection cannot be made within 24 hours
39	OEM must have local TAC support in INDIA and must have executed at least 2 similar wan optimization projects in INDIA with minimum of 200 remote locations.
40	OEM must have presence in INDIA from last 5 years.
	Management
41	Solution should provide centralized management tool for centralized configuration; monitoring provisioning and reporting. Instead managing individual devices.
42	Should allow centralized software management of WAN appliances across an entire network
43	Each appliance must have an integrated performance dashboard displaying traffic types, acceleration levels per traffic type, usage of the WAN link, and traffic statistics over time
44	A performance data export feature using Net Flow must be supported to send data to existing network management tools.
45	The solution must support RADIUS.
46	The solution must support SSH for access to the management Command Line Interface.
47	The appliance software must also have the option to run on Windows Server 2008 which is commonly found deployed in remote offices
48	Should support remote notification capabilities, including SNMP , SMTP notification, and syslog notifications.

j. Network Management & Monitoring System/Tool:

Basic Requirements
i. The proposed solution should be based on industry best practices and the OEM should have technical support center in India with at least 250 support staff.
ii. The Service Management solution namely Service desk (incident and problem mgmt) and Asset Management should be built on the same platform/code and leverage the same common, shared configuration database with a unified architecture. The same platforms should be used across all modules, requiring no complex integrations to leverage the combined benefits offered by the integrated platform.
iii. The service automation solution should be a unified solution supporting provisioning, configuration management and compliance assurance across servers, networks and applications and should support end to end full stack and dynamic server, network and application provisioning.
i. The solution should possess capabilities that deliver self-learning capabilities to virtually eliminate the ongoing costs of manual threshold, rule, and script maintenance.
ii. The solution should be able to generate dynamic performance baselines and continuously update and refine these normal operational bands by automatically adapting the changes in enterprise infrastructure. The solution should have the capability to minimize manual threshold management, by performing automated dynamic threshold management.
iii. The solution should have predictive analytics and intelligence in-built into it so as to detect any anomaly before it could potentially hit the threshold thereby giving enough lead time to users to resolve the issues before the threshold is breached.
i. The solution should have Service Management Process Model in built based on ITIL v3 best practices.
ii. Should manage complete lifecycle starting with the initiation of the procurement through to retiring and (if applicable) harvesting unused software.
iii. Should be integrated with Service Desk for maintenance and support of assets
i. Should support all major OS and virtualization platforms
ii. Should Support comprehensive and configuration-level roll-back for changes
iii. Automated provisioning for physical, virtual, and cloud-based environments
iv. Policy-based, Cross-Platform patch support across Windows, Linux, and Unix
v. Support compliance Policies for regulatory and security standards with integrated exception documentation
vi. Support Granular and environment-aware configuration policies and deployment
vii. Automated packaging, promotion, and deployment of applications
viii. Should support cross-platform and reusable packaging with built-in rollback support
ix. Should maintain complete configuration for all managed servers at completely granular level ensuring any minor change is also tracked and reported on
x. Should support Configuration-level Control of Tasks, Objects, and Policies
xi. Should have ability to monitor the parameters in real time and confirm compliance to security policies
xii. Closed loop change Management workflows that monitor and track these compliance changes
xiii. Should have audit capabilities that compare the server status to policies defined in real time
i. The solution should be able to support configuration management across the network infrastructure, including routers, switches, firewalls, load balancers, wireless access points, and other network devices.
ii. The solution should be able to instantly provide the who, what, where, and when of planned, unplanned, and unauthorized network changes
iii. The solution should be able to audit and enforce configuration standards, such as those around security, performance, and routing which would help in proactively assessing the impact of change and also quickly recover from problematic changes
iv. The solution should be able to dynamically create scripts to allow for changes to be pushed into the device without having to reboot the device (i.e., non-disruptive rollback)

v. The solution should be able to provide the mechanism to push access control lists (ACLs) into a device without exposing the device to potential security vulnerabilities"
vi. Should support Standard Authentication Methods, Role Based Access Control (RBAC), Realms and Groups, Sensitive Data Masking, Telnet SSH proxy
vii. The solution should support an extensible, automated import feature to collect device information from third party discovery engines and other sources.
The solution should be able to dynamically create scripts to allow for changes to be pushed into the device without having to reboot the device (i.e., non-disruptive rollback)
The solution should be able to provide the mechanism to push access control lists (ACLs) into a device without exposing the device to potential security vulnerabilities"
Should support Standard Authentication Methods, Role Based Access Control (RBAC), Realms and Groups, Sensitive Data Masking, Telnet SSH proxy
The solution should support an extensible, automated import feature to collect device information from third party discovery engines and other sources.
Should support Configuration-level Control of Tasks, Objects, and Policies
Should have ability to monitor the parameters in real time and confirm compliance to security policies
Closed loop change Management workflows that monitor and track these compliance changes
Software license usage metering and License compliance management
Provide detailed compliance measurement using a flexible, rule-based license engine with wizard-based license rules creation
Automate linkages between assets and software license, leases, warranty, and support contracts to optimize entitlements and ensure compliance
Track TCO, including costs attributable to maintenance, incidents, changes, and depreciation
The solution should come with a built-in Software library that has pre-populated list of 1000s of software along with details of their digital signatures and software categorization
Provide Service Blueprints Policy-based cloud service placement
Should provide Smartmerge to auto generate change scripts for Network provisioning
Should provide SmartACL management to push access control lists (ACLs) into a device w/o exposing the device to security vulnerabilities

k. SSL VPN:

i. SSL VPN should be a hardware based purpose built appliance with minimum 4 triple speed
10/100/1000 Mbps interface ports.
ii. Should support 1000 concurrent users and scalable up to 3000 users on same hardware
iii. Should provide fast and easy access to all applications including Web-based, client/server, server-based architecture
iv. Should support external wan optimization feature functions including TCP optimization, data deduplication, single instance store and application optimization blueprints for HTTP, HTTPS, CIFS, MAPI protocols for optimized application access through SSL VPN.
v. Should support standard compression mechanism and stream based differencing to avoid transmission of content that has been previously received in the local data store.
vi. Should support Active-Active High availability with stateful session failover (SSF)
vii. Should support following Authentication methods:
a) Username and Password, Active Directory, LDAP
b) Client side digital certificates
c) RSA Secure ID
viii. Should support at least 45 Virtual portals and support for delegated administrative management

per virtual portal.
ix. SSL VPN solution must provide machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access to corporate resources.
x. SSL VPN solution should provide provision for auto collect, auto approve functions for automated collection and approval of hardware ID's without any manual intervention
xi. Appliance must support workflow functionality that should allow security administrators to approve end user hardware machine before users can access the published resources
xii. SSL VPN solution offers encrypted and authenticated access to internal applications from internet. Multi factor authentication is additional layer of security that ensure only authorized user can access the resources, Static passwords can be compromised having said that attacker or intruder can bypass SSL security control and gain unauthorized access to internal applications. it is highly recommended form security stand point proposed SSL solution
i. SSL VPN should be a hardware based purpose built appliance with minimum 4 triple speed

l. Server Load Balancer:

S. no.	Feature /Specification
1.	**Architecture**
a.	Able to synchronize configurations at boot time and run time, connection-states to provide stateful-failover of applications.
b.	Able to be deployed in both Active-Standby and Active-Active setups.
c.	Able to detect system failure, SSL card failure, process health check, cpu overheated or shutdown/reboot, and perform failover to ensure high availability, by using either network and serial-connection based heartbeat.
d.	Able to be deployed in a single arm (single subnet) network topology environment.
e.	Supports RPC-XML scripting messages from third party applications or devices to modify configuration of the load balancer.
f.	Supports both CLI via SSH and web-based GUI configuration and administration.
g.	Extensible policies (e-Policy) scripts to implement business logic on network without any changes in application code to support complex application integration.
2.	**Delivery**
a.	Able to load balance ANY IP based application.
b.	Able to support both TCP and stateless UDP (User Datagram Protocol) applications.
c.	Able to should support server load balancing algorithms such as round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, snmp, SIP session ID, hash header etc.
d.	Able to maintain server persistency based on source ip and destination ip, http header, url, cookie and SSL ID.
e.	Able to support application based monitoring, such as HTTP/HTTPS,FTP (passive/active), POP3, IMAP, DNS, SMTP, telnet, RADIUS,LDAP, RTSP, RDP
f.	Able to support external customized / script based health check to perform extended health-checks on the servers and other devices.
g.	Able to support single arm, reverse and transparent proxy mode deployment scenarios and should support nested layer7 and l4 policies..
h.	Able to support different cookie persistence methods such as, insert, rewrite and hashing.
i.	Able to read into HTTP header and make traffic-management decision based on HTTP host, URI, method, version, cookie and browser type etc.

j.	Able to support a mixed combination of IPv6 and IPv4 virtual addresses and nodes.
k.	Able to support IPv6-IPv4 and IPv4-IPv6 translations.
3.	**Optimization**
a.	Able to provide integrated SSL termination / acceleration, and SSL re-encryption to the servers.
b.	Able to aggregate multiple connections to a single server side connection – connection multiplexing.
c.	Able to provide real time Dynamic Web Content Compression to reduce server load and selective compression for Text, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT, and XLS Mime types.
d.	Able to provide support for customized cache rules including max object size, TTL objects, refresh time interval etc.
e.	Able to support TCP optimization options including windows scaling, timestamp & Selective Acknowledgement for enhanced TCP transmission speed.
4.	**Security & management**
a.	Able to support Do mitigation through connection reverse proxy.
b.	Able to support packet filtering based on layer 3 to layer 7 information.
c.	Able to support Rate shaping & QoS Support so that all applications work optimally without impacting user experience
d.	Role based access control for granular authentication and authorization. Administrator should able to define multiple roles namely Admin, Security-admin, Network-Engineer, Network Monitor, Network Manager on the appliance
e.	The appliance should have SSH CLI, Direct Console, SNMP, and Single Console per Cluster with inbuilt reporting.
5.	**General**
a.	Shallberack-mountableintostandard19"-wide rack.
b.	Should be appliance based solution with high performance purpose built hardware.
c.	Shall be able to support the following load balancing algorithms that can be simple to set up and configure: round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, snmp, SIP session ID, hash header etc.
d.	Shall be able to support 'sticky' connections to servers based on the following switching mechanisms: URL/content switching policies URL hashing, Cookie-based, SSL ID based
e.	Should provide full ipv6 support and solution should be IPv6 gold-certified. OEM should be listed vendor for ipv6 phase-2 certification.
f.	OEM Shall have TAC Centre in India with 24x7 availability through toll free line
g.	OEM must have direct presence in India with at least 10 Nos. of Technical Manpower direct support in India for the offered technology.
6.	**Physical Specification**
a.	ShouldhaveOptimizeThroughputofminimum5 Gbps from day one available
b.	Should support4Millionconcurrentconnection
c.	4*10/100/1000 copper interface with 8 GB RAM
d.	Future support for 2*10G SFP+ interfaces and throughput scalability up to 10 Gbps on same hardware
e.	Should support hardware based SSL Acceleration with SSL throughput of 3Gbps

f.	Should have at least 12,000 SSL TPS (transaction per seconds) and scalable to 25,000 on same device
g.	Should support integrated hardware/software based compression module?
h.	Should have Redundant Power Supply

m. Link Load Balancer:

Hardware
Should be appliance based solution with purpose built hardware and dual power supply.
Intel based Quad core CPU with 8 GB RAM to support multiple features and load balancing functions.
The appliance should have minimum 4 triple speed gigabit 10/100/1000 copper ports.
The appliance should have 3 Gbps of system throughput and scalable to 4 gbps on same appliance.
Should provide 2M concurrent connections and scalable to 4M.
Load balancing Features
Support for multiple internet links in Active-Active load balancing and active-standby failover mode.
Should support Outbound load balancing algorithms like round robin, Weighted round robin, shortest response, target proximity / dynamic detection.
Should support inbound load balancing algorithms like round robin, Weighted round robin, target proximity /dynamic detection.
Should support Static NAT, Port based NAT and advanced NAT for transparent use of multiple WAN / Internet links.
IPV6 support with IPv6 to IP4 and IPv4 to IPv6 translation and full IPv6 support.
In case of link failure, device should detect it in less than 30 seconds and divert the traffic to other available links.
Shall provide individual link health check based on physical port, ICMP Protocols, user defined l4 ports and destination path health checks.
Should provide mechanism to bind multiple health checks, support for Application specific VIP health check and next gateway health checks.
Should support persistency features i.e. RTS (return to sender) and ip flow persistence.
High Availability and Cluster
Should provide comprehensive and reliable support for high availability based on Per VIP based Active-active & active standby unit redundancy mode.
Statefull session failover with Connection mirroring support
Appliance should not have any limitations for connection mirroring
Should support USB based FFO link and/or Ethernet link to synchronize configuration at boot time of HA
Support for multiple communication links for real time configuration synchronizations including HA group, gateway health check, decision rules, SSF sessions etc.. and heartbeat information
Must have support for secondary communication link for backup purpose
should support floating IP address and group for sate full failover support. Appliance must have support 256 floating ip address for a floating group
should support built in failover decision conditions including unit failover, group failover and reboot
should also have option to define customized rules for gateway health check – the administrator should able to define a rule to inspect the status of the link between the unit and a gateway
Configuration synchronization at boot time and during run time to keep consistence configuration on both units.
Should support global load balancing algorithms like global round robin (grr), VIP based weighted global round robin, global connection overflow, global least connections, IP overflow, Proximity etc.,
Security and Application Performance
Should provide performance optimization using TCP connection multiplexing, TCP buffering and IEEE 802.3ad

link aggregation.
should support TCP optimization options including windows slicing, timestamp & Selective Acknowledgement for enhanced TCP transmission speed.
TCP optimization option configuration must be defined on per virtual service basis not globally.
Optional software based compression for HTTP based application, SSL acceleration and high speed HTTP processing on same appliance.
Should support QOS for traffic prioritization, CBQ , borrow and un-borrow bandwidth from queues.
Should provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols.
Should support rate shaping for setting user defined rate limits on critical application.
Should support integrated firewall module to protect the device itself from network based DOS and DDOS attacks.
Appliance should have security features like reverse proxy firewall, Syn-flood and dos attack protection features from the day of installation.
Centralized Management
Must provide single window centralized management for Application load balancer and link load balancer.
Must be appliance/software based centralized management solution in HA mode
Management appliance should have 4GB memory and 4*10/100/1000 copper ports
Visibility to quickly identify and isolate performance problems in the application, device or network problems
Real time monitoring, over 30 different types of Layers 2-7 system status and traffic graphs with simultaneous views of multiple graphs for each managed device
Perform software upgrades, rollback and patches on one or more devices. Reuse configuration templates between similar devices or device groups
Should provide role based administration with different privilege levels with audit logs for troubleshooting and compliance
The appliance should provide detailed logs and graphs for real time and time based statistics
Load balancer appliance must support multiple configuration files with 2 bootable partitions for better availability and easy upgrade / fallback.
The system should support led warning and system log alert for failure of any of the power and CPU issues

n. Desktop thin Client with 23 inch monitor:

Description	
Operating System	Windows Embedded Standard 7
Processor	Dual-core Intel® Celeron® N2807 1.6 GHz processor
Memory	Standard: 16GB Flash, 4GB RAM DDR3-1333MHz
Graphics	Integrated with APU
Power	Worldwide auto-sensing 100–240 VAC, 50/60Hz 65W, 19V DC. Energy Star V.5.2. Phase V external and EuP-compliant power supply
Power consumption (short idle)	Under 6 watts
Security, physical	Built-in Kensington security slot (cable sold separately)
Certifications (Based on US ratings)	Citrix Ready, VMware Ready
EAP-TLS; EAP-LEAP; EAP-PEAP, EAP-MSCHAPv2, EAP-GTC	Yes
WEP	Yes
WPA Personal; WPA2 Personal; WPA Enterprise; WPA2 Enterprise	Yes

DVI-I	Yes
DVI-D	Yes
Enhanced USB keyboard with Windows Keys (104 keys) and PS/2 mouse port included in the U.S. and sold separately outside the U.S.	Yes
PS/2 or USB optical mouse are also available and sold separately (availability varies by region)	Yes
SB 2.0 ports	Three (one front, two rear)
Super Speed USB 3.0 port (backwards-compatible with USB 2.0)	One (front)
Optional serial port (mutually exclusive with DVI-I port)	AO
10/100/1000 Base-T Ethernet (RJ45)	Yes
Optional single and dual band 802.11 a/b/g/n/ac integrated wireless with external dual antenna	AO
Optional SFP Module supports either Base-T or Fiber network connectivity (mutually exclusive with the default RJ45 configuration)	AO
VESA monitor support with Display Data Control (DDC) for automatic setting of resolution and refresh rate	Yes
Single: DVI-I: 1920x1200@32bpp	Yes
Single: DVI-D: 1920x1200@32bpp	Yes
Dual: 1920x1200@32bpp	Yes
Internal mono speaker	Yes
Composite audio jack: 1/8-inch mini, 16-bit stereo	Yes
Height x Width x Depth without stand:	187mm x 29mm x 117mm (7.37 in x 1.15 in x 4.61in)
Dimensions (H x W x D) with stand:	197.5mm x 69mm x 117mm (7.78inx1.15 in x 4.61 in)
Shipping weight	2.34 kg. (5.2 lbs.)
Vertical feet	Yes
VESA mounting bracket	Optional
Vertical position, only; power button up: 50° to 104°F (10° to 40°C)	Yes
Storage: 14° to 140°F (-10° to 60°C)	Yes
Condensing: 20% to 80%	Yes
Non-condensing: 10% to 95%	Yes
Three-year limited hardware warranty	Yes

o. Desktop -2

General	**Descriptions**
Chassis	Small Form Factor
Processors	Intel Core I5-4590
Chipset	Intel® H81 Chipset

Operating System Options1	Windows 7 Professional, English, 32bit (includes Windows 8.1 Pro 64bit License and Media)
Graphics	Integrated Intel® HD Graphics 4600 (with select CPUs)
Memory	4GB
Networking	Integrated Realtek® RTL8151GD Ethernet LAN 10/100/1000
I/O Ports	2 external USB 3.0 ports /6 external USB 2.0 ports
Hard Drives4 Options	1TB
Expansion Slots	1 half height PCIe x16 /1 half height PCIe x1
Monitor	23 inch Screen Monitor with LED Back Light

1

Router at all Branches:

Sl. No.	**Detailed Technical Specifications**
1.0	**General requirements**
1.	Device should have a modular architecture
2.	Minimal performance degradation when running advanced services such as stateful firewall, NAT and IPSec.
3.	Device should support Routing, IPSEC, Firewall, IPS for IPv4 and IPv6 from day-1
	Hardware and interface requirements
4.	Device should have atleast4 x 10/100/1000, 4 SFP'sWAN and LAN ports and 4 free slots for future expansion. Should have 2 nos of v.35/E1 ports across different card/module.
5.	Device should support modular LAN and WAN connectivity options including Gigabit Ethernet T1/E1, serial V.35, E3, 10G.
6.	Should have internal redundant power supply from day 1.
7.	Should have minimum 1GB RAM and 1GB Flash
	Performance requirements
8.	The Device should support IPS performance of 600 Mbps with 2000+ Concurrent signatures. Device should support both IPv4 & v6 signatures & protection The functionality can also be met using external device. Hardware should be ready from day-1.
9.	The Device should have Firewall performance of 4 Gbps.
10.	The Device should support minimum 24,000 Connections per second
11.	The Device should support minimum 2,50,000 Concurrent Sessions
	Quality of Service (QoS) requirements
12.	Devices should support Class-based queuing with prioritization
13.	It should be possible to configure maximum bandwidth and guaranteed bandwidth
14.	Devices should support Queuing based on VLAN, DLCI, interface, bundles, or filters
15.	Devices should support Marking, policing, and shaping
16.	Devices should support congestion management features like WRED
	Routing protocol support
17.	The Device should support IPv4 and IPv6 routing
18.	The Device should support VRRP
19.	The Device should support Static Routes
20.	The Device should support RIPv1 & RIPv2
21.	The Device should have OSPFv2 and IS-IS routing features

Sl. No.	Detailed Technical Specifications
22.	The Device should support Policy Based Routing
23.	The Device should support Routing over IPSec Tunnels
24.	The Device should support ECMP
25.	**Multicast Features**
26.	Multicast Listener Discovery (MLD)
27.	IGMP v1/v2/v3
28.	PIM-SM
29.	Source Specific Multicast (SSM)
30.	**MPLS Features**
31.	Layer 2 VPN
32.	Layer 3 VPN
33.	LDP
34.	RSVP
	Security features
35.	Devices should support AAA using RADIUS or TACACS
36.	Devices should support Packet Filters
37.	Devices should support Network attack detection
38.	Devices should support DoS and DDoS protections
39.	Devices should support MD5 and SHA-1 authentication
40.	Devices should support Prevent replay attack
41.	Devices should have role based access mechanisms.
	Management and Troubleshooting
42.	Device should have Console, Telnet and Web for management
43.	Devices should support Software upgrades through Web
44.	Devices should support SNMPv2 and SNMPv3
45.	Extensive debugs on all protocols
46.	Real-time traffic-interface/sub interface statistics.
47.	Real-Time Performance Monitor—service-level agreement verification probes/alerts
	Certifications
48.	Safety certifications UL 60950-1
49.	EMC certifications FCC Class B
50.	Device shall be minimum EAL 3/ NDPP Certified.

p. General Specifications of the Networking Components

1.1.1 Firewall for Datacenter

Feature Specs
Hardware & Interface Requirements
Appliance should support at least 12 x 1-GbE SFP, 8 x 1 GbE, 1GbE Management, 1 Console
Appliance should support at least 4 x 10-GbE SFP+
Should have a dedicated 1 GbE management Interface
Appliance should have minimum 64 GB of RAM
Appliance should support 80 GB or above SSD Flash
Hardware architecture should consist of at least 60 core CPU or above
Firewall should support Dual Redundant Hot Swappable fan and power supply.
Capacity Requirements

should support a sustained Firewall throughput of the firewall system without packet drop of at least 40 Gbps and above
Should support a sustained Gateway Antivirus throughput of the firewall system without packet drop of at least 10 Gbps and above
Should support a sustained Intrusion prevention throughput of the firewall system without packet drop of at least 24 Gbps and above
Should support a sustained Application Inspection throughput of the firewall system without packet drop of at least 24 Gbps and above
Should support at least 3 Million firewall connections
should support at least 2,80,000 new TCP connections per second
should support a sustained 3DES/AES IPSEC VPN throughput of the firewall system without packet drop of at least 18 Gbps and above
Licensing and Certification
The OEM should be in the leader quadrant of UTM Gartner report for last three years
The OEM should be recommended by NSS Labs for last three years.
The device should be IPv6 Ready
The device should be appliance based firewall, with ICSA labs (International Computer Security Association) Firewall
The device should be appliance based firewall, Antivirus certification and preferably VPNC (Virtual Network Consortium) featured.
HA appliance should not carry any additional licensing and should share all license from primary appliance including hardware warranty
Bandwidth Management & Application control
Bandwidth Control/ Restriction per IP Address group & per Policy should be available.
Traffic management: Option to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy.
Should have application control feature for 4400 or more applications
Should block P2P applications, block Anonymous proxies etc.
VPN
Should support at least 25,000 IPSec Site-to-Site VPN tunnels and 2 or more no of IPSec Client Remote access VPN
Solution should support IPSEC & SSL VPN
Solution Should support VPN Encryption DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1,
IPS
IPS shall be able to detect incidents that originate from inside the network perimeter as well as from outside the network perimeter and shall be able to take action on the basis of configured policies.
Appliance should have support for DOS & DDOS scanning attacks and attack protection.
Should not have any point of failure devices like hard drives inbuilt on the appliance rather should support flash.
Should have all security functionality inbuilt and activated on single appliance.
Should do real time scanning rather than proxy based scanning of all the traffic passing through the appliance.
Signatures should have a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (eg. For severity level: high, medium, low)
Should be able to generate graphical reports on top attacks, source for attack etc.
Should have the option to schedule reports for automatic generation & email it to admin.
The OEM should have regular update of its attack signature database and the same should be configurable

to update the signatures automatically without manual intervention.
The new attack signatures and new major software releases should be available in OEM website for free download.
Should not buffer traffic before scanning for IPS.
Should be integrated solution with appliance based firewall on a single chassis with multi-core processor.
AV
Antivirus should provide real-time detection of viruses and malicious code at the gateway for SMTP, POP3, HTTP, FTP etc internet traffic.
The proposed solution should be licensed per unit as against per user.
The device should be featured with Gateway Antivirus and DPI SSl Scanning
Antivirus gateway should have option to configure to respond to virus detection in several ways
Automatic Frequent updates of virus pattern files should be available from the vendor without manual intervention
Should not buffer traffic before scanning for virus
Should have facility to block files based file extensions.
Should be an unlimited user based appliance.
Should have capacity to scan unlimited file size without buffering them.
There should not be any file size limitation to be scanned at GAV level.
Web Content Filtering
Web content filtering solution should work independently without the need to integrate with proxy server, there should not any proxy inbuilt into the UTM.
Should have facility to block the URL's based on categories.
The proposed solution should be licensed per unit as against per user.
URL database should have at least 15 million sites and 54 + categories.
URL database should be updates regularly by the OEM automatically.
Should be able to block different categories / sites based on users/groups.
Should have facility to configurable policy options to block web sites based on banned words.
Appliance should be able to re rate website into custom URL category.
The solution should support facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc.
Should have configurable policy options to define the URL exempt list.
The solution should be able to block spyware/adware etc.
The solution should have options to block java applets, active X as well as cookies.
The Solution should have RBL database of known spam sources to validate / check whether the mail is a spam or not
Solution should have the abilities to block the application not based on port and protocols.
Should support policy based on FQDN, Mac address, along with IP address.
Logging and reporting
Should have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc.
Logging and reporting solution should be supported.
The solution should generate the reports for the firewall, gateway level AV, IPS web filtering requested.
The solution shall have readymade templates to generate reports like complete reports or attack reports, bandwidth report etc.
The solution should help to analyze/understand attacks over various protocols like HTTP , FTP , SMTP etc.
The solution should help to analyze/understand the live application usage in the network.

Should have options to generate reports in terms of which are the frequent attacks as well as top sources and destination for attacks.
Should have options to generate reports in different formats
The solution should have configurable options to send the reports as a mail to the designated email address
Should have configurable parameters to send alert emails based on event type.
Should have configurable parameters to set alerts
The solution should have configurable options to schedule the report generation.

Core Router:

	Detailed Technical Specifications
	General features:
1.	The router should be chassis based with minimum 3 payload slots with distributed architecture through the segregation of control plane and data plane
	Architecture
2.	Should have internal redundant power supplies
3.	Should have redundant CP/ Routing Engine, in case of failure of primary CPU there should be no drop in the transit traffic.
4.	Minimum back-plane capacity of 70-Gbps & forwarding performance of 55 Million packets per sec of 64 bytes packet. The performance is considered with IPv4 & IPv6
5.	The Router Should support variety of interfaces I/O cards such as 1 Gig, 10 Gig, STM1, STM4, STM16, DS3/E3, E1/T1, ATM Interfaces, Circuit emulation (SAToP, CESoPSN) . All of the I/O slots should be universal and should support all of the above stated interfaces.
6.	Should have Minimum 8 X 10/100/1000 TX Ethernet and 8 X SFP based Ports, and 2 X 10 Gig SR ports from day one. The Optics for the interface should be provided.
	Ipv4 Feature support
7.	The Router should support the below IPv4 protocols and feature ISIS; LDP; BGP; MP-BGP; Support for RIP Version 2 , OSPF , Support for BGP confederations & Route Reflectors Resource Reservation Protocol (RSVP) & Label distribution protocol(LDP) MPLS , L3VPN, L2VPN VPLS The router should support DCI with EVPN supporting RFC 4364 RFC 4761 Should support security features like IPSEC, Firewall and Network attach detection from day-1
8.	**IPv6 Features:** IPv6 ping IPv6 trace route, RIPng OSPF v3 , IS-IS , VRRPv6 , MLD , IPv6 ACL
9.	Should support 6PE, 6VPE and NAT64.
10.	Should support IPSEC for encrypting traffic on WAN interface.
11.	Should support virtual switch or bridge domain for local switching
12.	Should support at-least 500K IPv4 routing entries per system and 500k IPv6 routing entries per system
13.	Should support minimum 1000 VRF’s
14.	Should support 4 logical Systems
15.	Should support 1 K VPLS instances
16.	**High Availability support:**Non Stop Routing, Graceful Restart, MPLS FRR, Should support 802.1ag , Y.1731, Multi chassis Link aggregation (MC-LAG), BFD for IPV4 and IPV6, VRRP .
17.	ISSU ,in service software upgrade
18.	Non Stop bridging and Non-stop-Routing
19.	Should support HQOS, Classification based on source and port, priority queue for critical traffic. Should support policing and shaping of traffic.
20.	Network Management:
21.	SNMP: Support for SNMP version 2 & upgradable to version 3 shall be provided.
22.	Console or Out-of –band Management: The Router shall have console management access
23.	The Router shall support Network Time Protocol (NTP) as per RFC 1305 or SNTP (simple NTP) as per as per RFC 2030
	Certifications
24.	Router should be EAL3/ NDPP and NEBS certified
25.	Safety certifications UL 60950-1
26.	EMC certifications FCC Class A

Firewall Scanning Station

Specifications
General
Integrated Security Appliance which is capable of supporting Firewall, VPN, IPS, Web filtering etc
The device should be IPv6 ready, and should support multi-core architecture.
Should not have 2nd gen proxy inbuilt on to the appliance to avoid latency
Dual WAN/ISP Support : Should support automatic ISP failover as well as ISP load sharing and load balancing for outbound traffic
Product Support should be (24 x 7)
Vendor & OEM should support the appliance with all necessary upgrade for at least 3 years from the date of purchase installation
Hardware and Interface Requirements
The product should have minimum of (5) 10/100/1000 copper gigabit
Minimum 1 GB RAM
Should have 1 USB Interface
Firewall Performance Requirement
Firewall inspection throughput at least 750 Mbps or higher
VPN throughput at least 300 Mbps or higher
The Firewall should support at least 50,000 concurrent sessions and at least 1800 new sessions per second.
The Firewall should have at least 300 Mbps of IPS throughput or higher.
Should have minimum 100 Mbps or higher of Anti-Malware inspection throughput.
Should support full DPI throughput of 100 Mbps or higher.
OEM to declare IMIX internet mix protocol performance for appliance and should not be less than 200 Mbps or higher.
Licensing and Certification
The OEM should be in the leader quadrant of UTM Gartner report for last three years
The OEM should be recommended by NSS Labs for last three years.
The device should be IPv6 Ready
The device should be appliance based firewall, with ICSA labs (International Computer Security Association) Firewall
The device should be appliance based firewall, Anti-virus certification and preferably VPNC (Virtual Network Consortium) featured.
Device should support HA active/passive with single set of license for all security services and hardware warranty
Bandwidth Management & Application control
Bandwidth Control/ Restriction per IP Address group & per Policy should be available.
Traffic management: Option to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy.
Should have application control feature for 4400 or more applications
Should block P2P applications, block Anonymous proxies etc.
VPN
Should support at least 10 IPSec Site-to-Site VPN tunnels and 1 or more no of IPSec Client Remote access VPN

Solution should support IPSEC & SSL VPN
Solution Should support VPN Encryption DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1,
IPS
IPS shall be able to detect incidents that originate from inside the network perimeter as well as from outside the network perimeter and shall be able to take action on the basis of configured policies.
Appliance should have support for DOS & DDOS scanning attacks and attack protection.
Should not have any point of failure devices like hard drives inbuilt on the appliance rather should support flash.
Should have all security functionality inbuilt and activated on single appliance.
Should do real time scanning rather than proxy based scanning of all the traffic passing through the appliance.
Signatures should have a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (eg. For severity level: high, medium, low)
Should be able to generate graphical reports on top attacks, source for attack etc.
Should have the option to schedule reports for automatic generation & email it to admin.
The OEM should have regular update of its attack signature database and the same should be configurable to update the signatures automatically without manual intervention.
The new attack signatures and new major software releases should be available in OEM website for free download.
Should not buffer traffic before scanning for IPS.
Should be integrated solution with appliance based firewall on a single chassis with multi-core processor.
AV
Antivirus should provide real-time detection of viruses and malicious code at the gateway for SMTP, POP3, HTTP, FTP etc internet traffic.
The proposed solution should be licensed per unit as against per user.
The device should be featured with Gateway Antivirus and DPI SSl Scanning
Antivirus gateway should have option to configure to respond to virus detection in several ways
Automatic Frequent updates of virus pattern files should be available from the vendor without manual intervention
Should not buffer traffic before scanning for virus
Should have facility to block files based file extensions.
Should be an unlimited user based appliance.
Should have capacity to scan unlimited file size without buffering them.
There should not be any file size limitation to be scanned at GAV level.
Web Content Filtering
Web content filtering solution should work independently without the need to integrate with proxy server, there should not any proxy inbuilt into the UTM.
Should have facility to block the URL's based on categories.
The proposed solution should be licensed per unit as against per user.
URL database should have at least 15 million sites and 54 + categories.
URL database should be updates regularly by the OEM automatically.
Should be able to block different categories / sites based on users/groups.
Should have facility to configurable policy options to block web sites based on banned words.

Appliance should be able to re rate website into custom URL category.
The solution should support facility to generate reports on virus dedected over different protocols, top sources for viruses, destination for viruses, top viruses etc.
Should have configurable policy options to define the URL exempt list.
The solution should be able to block spyware/adware etc.
The solution should have options to block java applets, active X as well as cookies.
The Solution should have RBL database of known spam sources to validate / check wheather the mail is a spam or not
Solution should have the abilities to block the application not based on port and protocols.
Should support policy based on FQDN, Mac address, along with IP address.
Logging and reporting
Should have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc.
Logging and reporting solution should be supported.
The solution should generate the reports for the firewall, gateway level AV, IPS web filtering requested.
The solution shall have readymade templates to generate reports like complete reports or attack reports, bandwidth report etc.
The solution should help to analyze/understand attacks over various protocols like HTTP , FTP , SMTP etc.
The solution should help to analyze/understand the live application usage in the network.
Should have options to generate reports in terms of which are the frequent attacks as well as top sources and destination for attacks.
Should have options to generate reports in different formats
The solution should have configurable options to send the reports as a mail to the designated email address
Should have configurable parameters to send alert emails based on event type.
Should have configurable parameters to set alert
The solution should have configurable options to schedule the report generation.
Router, Firewall & Switch with a provision of LAN/WAN ports configuration for Evaluation Centre Specifications
General
Integrated Security Appliance which is capable of supporting Firewall, VPN, IPS, Web filtering etc
The device should be IPv6 ready, and should support multi-core architecture.
Should not have 2nd gen proxy inbuilt on to the appliance to avoid latency
Should support OSPF, RIP V1 and V2 routing protocol.
Should support NAT without degrading the performance of the firewall.
Should have Layer 2 bridge or transparent mode
The firewall should be able to support dynamic load balancing for outbound data passing through the firewall, if external firewall load balances are required same is to be mentioned.
Dual WAN/ISP Support : Should support automatic ISP failover as well as ISP load sharing and load balancing for outbound traffic
Should be an ASIC's based or quad core or higher processor based solution for faster processing.
Product Support should be (24 x 7)

Vendor & OEM should support the appliance with all necessary upgrade for at least 3 years from the date of purchase installation
Hardware and Interface Requirements
The product should have minimum of (8) 10/100/1000 copper gigabit
Appliances should have dedicated management interface
Minimum 2 GB RAM
Should have 1 console Port
Should have 1 USB Interface
Appliance should be 1U and rack mountable
Firewall Performance Requirement
Firewall inspection throughput at least 1.5 Gbps or higher
VPN throughput at least 1 Gbps or higher
The Firewall should support at least 200,000 concurrent sessions and at least 10,000 new sessions per second.
The Firewall should have at least 700 Mbps of IPS throughput or higher
Should have minimum 400 Mbps or higher of Anti-Malware inspection throughput
Should support full DPI throughput/ Fully Protected throughput of 300 Mbps or higher
Licensing and Certification
The devices should not have license restriction on number of users
The OEM should be in the leader quadrant of UTM Gartner report for last three years
The OEM should be recommended by NSS Labs for last three years.
The device should be IPv6 Ready
The device should be appliance based firewall, with ICSA labs (International Computer Security Association) Firewall
The device should be appliance based firewall, Anti-virus certification and preferably VPNC (Virtual Network Consortium) featured.
Device should support HA active/passive with single set of license for all security services and hardware warranty
Bandwidth Management & Application control
Bandwidth Control/ Restriction per IP Address group & per Policy should be available.
Traffic management: Option to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy.
Should have application control feature for 4400 or more applications
Should block P2P applications, block Anonymous proxies etc.
VPN
Should support at least 75 IPSec Site-to-Site VPN tunnels and 10 or more no of IPSec Client Remote access VPN
Solution should support IPSEC & SSL VPN
Solution Should support VPN Encryption DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1,
IPS
IPS shall be able to detect incidents that originate from inside the network perimeter as well as from outside the network perimeter and shall be able to take action on the basis of configured policies.
Appliance should have support for DOS & DDOS scanning attacks and attack protection.

Should not have any point of failure devices like hard drives inbuilt on the appliance rather should support flash.
Should have all security functionality inbuilt and activated on single appliance.
Should do real time scanning rather than proxy based scanning of all the traffic passing through the appliance.
Signatures should have a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (eg. For severity level: high, medium, low)
Should be able to generate graphical reports on top attacks, source for attack etc.
Should have the option to schedule reports for automatic generation & email it to admin.
The OEM should have regular update of its attack signature database and the same should be configurable to update the signatures automatically without manual intervention.
The new attack signatures and new major software releases should be available in OEM website for free download.
Should not buffer traffic before scanning for IPS.
Should be integrated solution with appliance based firewall on a single chassis with multi-core processor.
AV
Antivirus should provide real-time detection of viruses and malicious code at the gateway for SMTP, POP3, HTTP, FTP etc internet traffic.
The proposed solution should be licensed per unit as against per user.
The device should be featured with Gateway Antivirus and DPI SSl Scanning
Antivirus gateway should have option to configure to respond to virus detection in several ways
Automatic Frequent updates of virus pattern files should be available from the vendor without manual intervention
Should not buffer traffic before scanning for virus
Should have facility to block files based file extensions.
Should be an unlimited user based appliance.
Should have capacity to scan unlimited file size without buffering them.
There should not be any file size limitation to be scanned at GAV level.
Web Content Filtering
Web content filtering solution should work independently without the need to integrate with proxy server, there should not any proxy inbuilt into the UTM.
Should have facility to block the URL's based on categories.
The proposed solution should be licensed per unit as against per user.
URL database should have at least 15 million sites and 54 + categories.
URL database should be updates regularly by the OEM automatically.
Should be able to block different categories / sites based on users/groups.
Should have facility to configurable policy options to block web sites based on banned words.
Appliance should be able to re rate website into custom URL category.
The solution should support facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc.
Should have configurable policy options to define the URL exempt list.
The solution should be able to block spywares/adware etc.
The solution should have options to block java applets, active X as well as cookies.

The Solution should have RBL database of known spam sources to validate / check whether the mail is a spam or not
Solution should have the abilities to block the application not based on port and protocols.
Should support policy based on FQDN, Mac address, along with IP address.
Logging and reporting
Should have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc.
Logging and reporting solution should be supported.
The solution should generate the reports for the firewall, gateway level AV, IPS web filtering requested.
The solution shall have readymade templates to generate reports like complete reports or attack reports, bandwidth report etc.
The solution should help to analyze/understand attacks over various protocols like HTTP , FTP , SMTP etc.
The solution should help to analyze/understand the live application usage in the network.
Should have options to generate reports in terms of which are the frequent attacks as well as top sources and destination for attacks.
Should have options to generate reports in different formats
The solution should have configurable options to send the reports as a mail to the designated email address
Should have configurable parameters to send alert emails based on event type.
Should have configurable parameters to set alerts
The solution should have configurable options to schedule the report generation.

q. Core switch- 48 Port- 1G

General	**Descriptions**
Device Type:	Full managed L3 stackable switch with 48 ports
Ports Qty:	48x RJ45 10/100/1000 Mb auto-sensing ports, 2x SFP+ ports, 2x GbE combo media ports, 1x hot swap expansion module bay, 1x 200W PSU included
Stacking Ports	2 rear stacking ports (21Gbps) supporting up to 84Gbps (full-duplex)
Memory	
RAM:	Minimum 1GB SDRAM
Flash Memory:	Minimum 256 MB flash
Packet Buffer	Minimum 32 MB
Performance	
Switching Capacity	Minimum 260Gbps
Switching Throughput	Minimum 193Mpps
MAC Address Table Size	16000 MAC addresses
802.1Q Vlans	4K 802.1Q vlans user configurable
Networking Features	
Routing Protocol:	Static routing, RIP V1/V2, Ospf V1/V2/V3, CIDR, IDRP, VRRP,BGP
	PIM Dense Mode (PIM-DM), Sparse Mode (PIM-SM), and Source-Specific Mode (PIM-SSM) for IPv4 and IPv6 multicast applications

Communication Mode:	Half-duplex, full-duplex
Switching Protocol:	Ethernet
Status Indicators:	Link activity, port transmission speed, port duplex mode, power, link OK, system, temprature LED, Diagnostic LED,rest button
Vlans	Should support Port, Voice, QinQ, Protocol, GVRP
DHCP and BOOTP relay	Should support DHCP (udp helper), BootP, DHCP Relay, DHCP Snooping
Redundancy Protocols	Should support STP, RSTP, MSTP, STP Root Guard, BPDU Guard, MLAG
Qos	Flow based Qos service, port based qos service, ACL Qos,MAC based cos assignment, rate limiting and metering
Security Features	
	Should support 802.1x and Guest vlans
	Should support MAC based port security by number of MAC
	Should support Packet filtering at L2/L4 with flow based classification based on source MAC address, destination MAC address, source IP (IPv4/IPv6) address, destination IP (IPv4/IPv6) address, port, protocol, and VLAN. Malicious Code Detection
	Should support Standard, Extended acl's
Management Function	
OpenFlow	Should support Open Flow 1.x
Configuration	Should support CLI, WEB based, and SNMP v1/v2/v3 based managements
	Should support Sflow or equivalent technologies
	Should support management vlans and Port namings to each interfaces
	Should support Link Layer Discovery protocols
	Should support multiple configuration and system files
	Should support management function like Ping, Telnet, Tracert for both IPv4 and IPv6
Miscellaneous	
Authentication Method:	Secure Shell (SSH), RADIUS, TACACS+
Power	
Power Device:	Power supply AC
Voltage Required:	AC 110/240 V (50/60 Hz)
Certifications	Energy Efficient Ethernet (EEE), FCC Class B , FCC Class A, IPv6 USGv6 Certification, IPv6 UNH Certification

r. Core switch- 48 Port-10G

Switch should be equipped with 48 port 1gig /10gig SFP+ Ports with 4 Numbers of 40Gig ports.
Ports support 1Gb and 10Gb transceivers for SFP/SFP+ and 100Mb, 1Gb and 10GBASE-T for RJ-45 environments and 40Gb transceivers for QSFP environment
Up to 64 10GbE ports of copper or fiber with module options in a 1RU form factor
Loaded with -10Gb SR Mode modules
Total Switching Capacity : 1.28Tbps
Switch should be able to support latency not more than 800ns and third party report should be submitted to validate the same.

Switch should be able to support Scripting through Perl and Python
Enhanced mirroring capabilities including 1:4 local mirroring, Remote Port Mirroring (RPM) and Encapsulated Remote Port Mirroring (ERPM). Rate shaping combined with flow based mirroring enables the user to analyze fine grained flows
Should be able to enforce standard configurations by automatically configuring network switches.
Should be able to support Smart Scripting through Perl and Python.
Should increase network flexibility by automatically provisioning VLANs when VMs are migrated and switch should be able to support at least VMware 4.0, 4.1 and Citrix XenServer 5.6.
Maintain network connectivity and security policies in virtual environments.
Switch through Programmatic Management should be able to support XML
Should be able to support SDN through the support of OPENFLOW 1.0 or higher protocol.
Performance
MAC addresses: 128K
IPv4 routes: 16K
IPv6 routes: 7K (shared CAM space with IPv4)
Switch fabric capacity: 1.20 Tbps (full-duplex)
600 Gbps (half-duplex)
Forwarding capacity: 960 Mpps
Flow-based port mirroring
Link aggregation: 8 links per group, 128 groups per stack
Queues per port: 4 queues
Layer 2 VLANs: 4K
MSTP : 64 instances
Line-rate Layer 2 switching: all protocols, including IPv4 and IPv6
Line-rate Layer 3 routing: IPv4 and IPv6
IPv4 host table size 8K
IPv6 host table size 4K
IPv4 Multicast table size 4K
LAG load balancing: based on Layer 2, IPv4 or IPv6 headers
Latency sub 700ns
Packet buffer memory: 9MB
CPU memory: 2GB
IEEE Compliance
802.1AB LLDP
802.1ag Connectivity fault Management
802.1D Bridging, STP
802.1p L2 Prioritization
802.1Q VLAN Tagging, Double VLAN Tagging, GVRP
802.1s MSTP
802.1w RSTP
802.1X Network Access Control
802.3ab Gigabit Ethernet (1000BASE-T)

802.3ac Frame Extensions for VLAN Tagging
802.3ad Link Aggregation with LACP
802.3ae 10 Gigabit Ethernet (10GBASE-X)
802.3ba 40 Gigabit Ethernet (40GBase-SR4, 40GBase-CR4)
on optical ports
802.3u Fast Ethernet (100BASE-TX) on mgmt ports
802.3x Flow Control
802.3z Gigabit Ethernet (1000BASE-X)
ANSI/TIA-1057 LLDP-MED
RFC and I-D Compliance
2385 MD5
RFC 2545 BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
2439 Route Flap Damping
2796 Route Reflection
2842 Capabilities
2858 Multiprotocol Extensions
2918 Route Refresh
3065 Confederations
4360 Extended Communities
4893 4-byte ASN
5396 4-byte ASN representations
Redundant Power Supply - Internal Hot-Swap

s. 24-Port Switch- For Evaluation and Scanning Station

General	Descriptions
Device Type:	Full managed stackable switch with 24 ports
Ports Qty:	24 10/100/1000BASE-T auto-sensing Gigabit Ethernet switching ports; 2 SFP+ ports for fiber media support; 2 HDMI Stacking Ports
Stacking	2 rear stacking ports (21Gbps) supporting up to 84Gbps (full-duplex)
Memory	
RAM:	minimum 1GB SDRAM
Flash Memory:	minimum 256 MB flash
Packet Buffer	Minimum 32 MB
Performance	
Switching Capacity	Minimum 170 Gbps
Switching Throughput	Minimum 128 million pps
MAC Address Table Size	8000 MAC addresses
802.1Q Vlans	4K 802.1Q vlans user configurable
Networking Features	
Routing Protocol:	Static routing support for 256 IPv4 routes
Communication Mode:	Half-duplex, full-duplex

Switching Protocol:	Ethernet
Status Indicators:	Link activity, port transmission speed, port duplex mode, power, link OK, system, temperature LED, Diagnostic LED, rest button
Vlans	Should support Port, Voice, QinQ, Protocol, GVRP
DHCP and BOOTP relay	Should support DHCP (udp helper)
Redundancy Protocols	Should support STP, RSTP, MSTP, STP Root Guard, BPDU Guard, MLAG
Qos	Flow based Qos service, port based qos service, ACL Qos,MAC based cos assignment, rate limiting and metering, 8 priority queues per port
Security Features	
	Should support 802.1x and Guest vlans
	Should support MAC based port security by number of MAC
	Should support Packet filtering at L2/L4 with flow based classification based on source MAC address, destination MAC address, source IP (IPv4/IPv6) address, destination IP (IPv4/IPv6) address, port, protocol, and VLAN. Malicious Code Detection
	Should support Standard, Extended acl's
Management Function	
Configuration	Should support CLI, WEB based, and SNMP v1/v2/v3 based managements
	Should support Sflow or equivalent technologies
	Should support management vlans and Port namings to each interfaces
	Should support Link Layer Discovery protocols
	Should support multiple configuration and system files
	Should support management function like Ping, Telnet, Tracert for both IPv4 and IPv6
Miscellaneous	
Authentication Method:	Secure Shell (SSH), RADIUS, TACACS+
Power	
Power Device:	Power supply AC
Voltage Required:	AC 110/240 V (50/60 Hz)

t. Switch 48 Port- For Evaluation and Scanning Station

General	**Descriptions**
Device Type:	Full managed stackable switch with 48 ports
Ports Qty:	48x RJ45 10/100/1000 Mb autosensing ports, 2x SFP+ ports, 2x stacking ports, 1 integrated 1000W PSU
Stacking	2 rear stacking ports (21Gbps) supporting up to 84Gbps (full-duplex)
Memory	
RAM:	minimum 1GB SDRAM
Flash Memory:	minimum 256 MB flash
Packet Buffer	Minimum 4 MB

Performance	
Switching Capacity	Minimum 220Gbps
Forwarding rate:	Minimum 164Mpps
MAC Address Table Size	8000 MAC addresses
802.1Q Vlans	4K 802.1Q vlans user configurable
Networking Features	
Routing Protocol:	Static routing support for 256 IPv4 routes
Communication Mode:	Half-duplex, full-duplex
Switching Protocol:	Ethernet
Status Indicators:	Link activity, port transmission speed, port duplex mode, power, link OK, system, temprature LED, Diagnostic LED,rest button
Vlans	Should support Port, Voice, QinQ, Protocol, GVRP
DHCP and BOOTP relay	Should support DHCP (udp helper)
Redundancy Protocols	Should support STP, RSTP, MSTP, STP Root Guard, BPDU Guard, MLAG
Qos	Flow based Qos service, port based qos service, ACL Qos,MAC based cos assignment, rate limiting and metering, 8 priority queues per port
Security Features	
	Should support 802.1x and Guest vlans
	Should support MAC based port security by number of MAC
	Should support Packet filtering at L2/L4 with flow based classification based on source MAC address, destination MAC address, source IP (IPv4/IPv6) address, destination IP (IPv4/IPv6) address, port, protocol, and VLAN. Malicious Code Detection
	Should support Standard, Extended acl's
Management Function	
Configuration	Should support CLI, WEB based, and SNMP v1/v2/v3 based managements
	Should support Sflow or equivalent technologies
	Should support management vlans and Port namings to each interfaces
	Should support Link Layer Discovery protocols
	Should support multiple configuration and system files
	Should support management function like Ping, Telnet, Tracert for both IPv4 and IPv6
Miscellaneous	
Authentication Method:	Secure Shell (SSH), RADIUS, TACACS+
Power	
Power Device:	Power supply AC
Voltage Required:	AC 110/240 V (50/60 Hz)

	DDOS Protection Device
Sl. No	Specifications
1	Solution should be deployment in form of dedicated hardware platform delivers a latency rate of less than 50 microseconds
2	Should be able to deploy in layer 2 transparent mode so that minimum change is required in the network.
3	should be easy to deploy and start protecting from day 1 against the DDoS prevention against targeted attacks, worm outbreaks, DDoS and Botnet attacks, source tracking, and Inbound and Outbound attacks.
4	Should have a dedicated management interface
5	Shouldhave multiple Gigabit/10-Gig interface for connectivity to network.
6	Should support redundant power supply
7	Performance & Scalability
8	Should support scalable performance
9	Should have capability to inspect minimum 1 Million concurrent session & should be scalable
10	Should be based on behavior-based detection Engine
11	High Availability
12	Should support high-availability by clustering two or more devices in A/A or A/P deployment scenario
13	Should support Segregation and virtualization of the DDoS appliance allows separate security policies on each segment for multi-tenant environments.
14	Feature Requirement
15	Should be able to protect from malicious traffic with VLAN tags
16	Should have user friendly console for management
17	Should be fully IPv6 compliant
18	Should support dynamic and self-learning mechanism
19	Should be able to stop both volumetric and low and slow DDoS attacks.
20	Should have capability to identify various application stacks in the network to prevent stealth attack
21	Should support black and white-list of IP/subnet/Countries.
22	Should be able to protect against DDOS in both direction
23	Should support management interface with different user access levels
24	Should support monitoring of multiple subnets & networks
25	Reporting and Logging
26	Should support reporting in various readable formats like PDF /word format
27	Should support SNMP & Syslog
	Content Caching Device
1	Should work in multiple mode Transparent Inline Proxy, Routed Inline Proxy, Explicit Proxy, WCCP Target

2	Caches resource heavy viral video content, e.g. YouTube, MSN, Metacafeetc
3	Bandwidth Reduction and Application Acceleration
4	Detects same video ID when content comes from different CDN hosts
5	Detect advertisements automatically played before actual videos
6	Web content filtering to prevent access to unwanted or malicious content
7	Caches HTTP objects whilst observing HTTP/1.0 and 1.1 standards
8	Caches Microsoft, Apple and common AV signature updates
9	Caches video formats and understands popular DDNs to maximize performance benefits
10	Seek forward/backward in video
11	Should provide Web filtering consists of 79 content categories in 8 groups, which can be filtered or blocked based on the user credentials
12	Should have Multiple TB of Hard Disk in redundant mode
13	Should Have redundant Power Supply
14	Should support Reporting & Logging

Data Loss Prevention Tool (DLP)
Must provide next generation data threat prevention and information discovery functions to protect structured, semi-structured, unstructured mission critical data in the enterprise
Network Data Loss Prevention
For software based Solution, Supplier has to provide appropriate hardware keeping overall design and functional requirement under consideration and must not affect overall application performance. The proposed Solution must support 500 users & scalable to 1000 users.
Solution should not require any third party proxy server (such as ICAP servers) to provide Enforcement of Information Security.
Solution should cover both Active and passive FTP including fully correlating transferred file data with control information. Solution Should have the ability to monitor popular IM protocols (AIM, Yahoo, MSN, IRC etc.) and properly classify tunneled IM traffic (HTTP)
Solution should be able to interface with an institution’s employee or staff directories (e.g., Active Directory, LDAP)
Content Detection
Solution must have Identity and Role Based policy capabilities that integrate with AD/LDAP/HR database.
Solution should enforce “Automatic Access Control” on Data and Information
Solution must be able to apply different policies to different employee groups
Solution should have ability to filter out network traffic for inspection based on protocol, IP range, or email sender/recipient email
Solution should provide encryption capabilities to protect data at risk
Solution should have a comprehensive Information Classification methodology that would be readily deployable and does not dependent on fingerprint technology
Solution should have Resources Qualification and experience in Information Classification
Solution should have ability to create and manage policies that can be deployed across all components (Network and Endpoints)
DLP Policy Creation
Solution MUST use automated policy mechanism

The network DLP Solution should have capability to test the policy on an offline data before making it live, it helps to avoid false positives.
Solution should have built-in Automated Policy Synthesis mechanism
Solution should be able to monitor and prevent Advanced Persistent Threats (APT)
Solution should have Built-in Ontologies on International PII and PCI-DSS capabilities and has the ability to add or customized new Ontologies to cater to specific Government or Defense requirements
The Solution should provide ability to configure policies to detect on fingerprints and files from share/repository/date created etc.
Solution should have Ability to detect and protect confidential unstructured data based on the data categorization that has been learnt
Solution should have ability to Detect based on fully customizable regular expressions
Solution should have Ability to detect and protect new or unseen documents, which content is similar to the data categorization which has been taught via data categorization Solution should have Ability to detect scanned documents, which contains sensitive data in text form
Solution should have Ability to detect screen captures or picture formats, which contain sensitive data in text form.
Solution should have Ability to learn to categorize data via providing a set of sample documents to improve accuracy of detection
Solution should have Ability to configure and send multiple automated responses based on severity, match count, policy, etc
Solution should have Ability to release quarantined email from notification received.
Reporting and Notification
On-screen/ pop-up/ e-mail notification delivered to users during a rule/ policy violation and escalation workflow to ICT Security team or immediate manager.
User's ability to conduct self-remediation (such as on-screen/pop-up/e-mail notification prompting user to confirm whether to continue or cancel confidential data transfer). Ability to capture justification for DLP rule/policy violation as part of logs capturing all relevant incident details on a single screen/ page to allow quick user decision-making and immediate action.
Per-user ability to customize the layout and data of the incident snapshot
Incident Management and administration
Ability for an incident to be correlated to other incidents by subject, sender, recipient, filename, file owner, user name, and policy.
Solution should have ability to support real-time incident analysis
DLP Reporting
Solution should have a list of pre-defined template reports
Solution should Support report customization
DLP Management
Solution should have Integration with external directory for incident workflow assignment
Support for role-based access and delegated administration
Integration with Active Directory or other directory
Host DLP
Control use of all the USB devices
Track what data is saved to USB storage devices
Track what data is copied from USB storage
The proposed Solution architecture, Design and deployment, Warranty for a period of 5 (Five) Years should be certified by OEM Professional Services with relevant documents.

Advanced Persistent Threat Prevention Solution:

2 S. No	3 Specification
4 1	5 The solution must be Hardware based on premise solution with dedicated appliance based Sensors and Analysis appliances. The sensors must intercept traffic and forward to Analysis appliance for APT and Zero-day detection.
6 2	7 The APT analysis appliance should support 128 GB RAM, 128 GB HDD, 4 no of Gigabit interfaces. It must support dual 6-core processor for high performance. The APT sensor appliance most support dual power supplies and 12x 1 Gig, 8x 1 Gig SFP.
8 3	9 The APT sensor must deliver at least 2 Gbps performance with 64B HTTP packet and 1 Gbps of performance with vulnerability, anti-malware, anti-virus, anti-bot, application visibility and control. The performance must be measured using Data Center Environment with all Traffic enabled (not just internet traffic). The OEM must furnish details of the testing methodology.
10 4	11 The APT sensor must support at least 250,000 concurrent sessions. The session count must be active TCP connections. The concurrent sessions must not drop while enabling all requested features.
12 5	13 The APT sensor must support deployment in Tap mode, Transparent mode and Inline (Layer 3) mode. The sensor should support deployment capability in all modes simultaneously.
14 6	15 The APT sensors should have dedicated inbuilt hardware resources for access and management at all times, and must be available irrespective of load.The solution must report on the CPU usage for management activities and CPU usage for other activities.
16 7	17 The APT sensors must not have Application specific chips like ASICs that doesn't allow future firmware and feature expansions on the same hardware. Solution must be based on parallel processing architecture and must not use proprietry ASIC chips.
18 8	19 The APT sensor must support Full tunnel, split tunnel and application specific tunnel for client to site VPNs to identify zero-day malware for outside users. Solution must allow custom policies to control VPN traffic based on users, applications. It must allow different policies for different users groups for threat (Viruses, vulnerabilities, zero-day malware) within VPN traffic.
20 9	21 The APT sensor should support optionally Active/Active and Active/Passive HA (not required from day one.) and must support synchronization of the following for HA. -All sessions -Decryption Certificates -All VPN Security Associations -All vulnerability and AV sessions -All threat and application signatures -FIB Tables
22 10	23 The proposed solution must support different Custom vulnerability and Application policies for different users and groups.
24 11	25 The APT sensor should support Session based (not packet based) differentiated services code point (DSCP) classification. This should help in end-to-end priority policing and C2S & S2C direction enforcement.
26 12	27 The APT solution must identify unknown malware and zero-day exploits across any port, protocol and application. It must not be limited to just Web, Email or Files only. The solution must not require MTA deployment for malicious file scanning through emails.
28 1	29 The solution must be unified to analyze malicious files across any application/port or protocol.

3	There must not be multiple individual appliances for Web, Email or File scanning.
30 14	31 The solution must be scalable and a single sandbox appliance should handle multiple networks and segments through sensors.
32 15	33 The solution should support enhanced File type support: .exe, .dll, .scr, .ocx, .sys, .drv, Adobe (.pdf), Microsoft Office Documents (.doc, .docx., .xls, .xlsx, .ppt, and .pptx), Non-Microsoft document types (.rtf), Java (.jar and class files), Adobe Flash .swf
34 16	35 The Solution should support (zip/gzip), packed and encrypted (SSL) content and analysis of commonly embedded objects such as Javascript, flash, images, etc. within these file types.
36 17	37 The solution must support inspection against files within SSL and SSH encryption. The solution must not use any third party (Different OEM) for decryption.
38 18	39 The Solution must support both inbound and outbound SSL and SSH decryption.
40 19	41 The Solution must decrypt, identify and block malicious data upload and download in applications over SSL.
42 20	43 The Solution must decrypt and identify SSH traffic and Tunneling applications. It should have the capability allow SSH traffic but drop tunneled applications.
44 21	45 The solution should support protection against anti-VM evasion techniques that include sleep calls, enumerating for processes and debuggers, simulating user environments (key clicks, mouse clicks, mouse movement, etc.), detection of malware attempting to determine what port the VM process is connected to, determining if the VM is running in a single processer versus a multi-core processors, etc.
46 22	47 The solution should allow automated signature creation within 5 mins of Zero-day/Unknown malware detection.
48 23	49 The APT analysis appliance must automatically create signatures in the Sensor appliances without manual intervention. The Signature must be based on content/payload, not just hash and URL.
50 24	51 The solution must support submission of up to 1,000 samples per day and up to 10,000 report queries per day.
52 25	53 The solution should provide detailed analysis of every malicious file sent across multiple operating system environments, including both host-based and network-based activity
54 26	55 The APT sensor must allow policy rule creation for application identification, user identification, host profile, threat prevention, content filtering, file blocking, QOS and scheduling in a single rule and not at multiple locations
56 27	57 The proposed solution shall be able to create application signatures for Homegrown and custom applications without any additional cost.
58 28	59 The APT sensor must support different actions in the policy such as deny, drop, reset client, reset server, reset both client and server.
60 29	61 The solution must provide complete Session data associated with the delivery of the malicious file, including source, destination, application, User-IDTM, URL, etc.
62 30	63 The proposed solution shall support DNS-based signatures to detect specific DNS lookups for hostnames that have been associated with malware. The solution must identify hosts interacting with malicious domains, not just unknown domains.
64 31	65 The solution should provide access to the original malware sample for reverse engineering and full PCAPs of dynamic analysis sessions.
66 32	67 The solution must support minimum four level of decompression/decoding for any combination of decoding: ZIP, gzip, base64,chunked, uuencode.
68 33	69 The solution must provide the ability to block files with multi-level-encoding with 5 or more level of compression e.g office file in 5 levels of zip.

70 34	71 The proposed solution shall support packet captures based on: -Applications -Unknown Applications -any threat -data-filters
72 35	73 The solution must support an open API for integration with best-in-class SEIM tools and leading endpoint agents.
74 36	75 The API must enable to programmatically send file analysis jobs to Sandbox environment and query for report data through a simple XML API interface.
76 37	77 The solution must allow configurations for file types and file size that needs to be analyzed in Sandbox environment. The other file types must not hit the sand box appliance at all.
78 38	79 The Proposed solution should support authentication for terminal services like Citrix and Microsoft.
80 39	81 Solution should detect probable exploit kit activity targeted at a host on the network. Exploit kits should be identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature.
82 40	83 The proposed solution must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance
84 41	85 Solution should correlate and detect hosts that have received malware detected by inbuilt APT solution, and have also exhibited command-and-control (C2) network behavior corresponding to the detected malware.
86 42	87 Solution should detect probable exploit kit activity targeted at a host on the network. Exploit kits should be identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature.
88 43	89 Solution should correlate and detect likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc.
90 44	91 The solution must provide detailed Change monitor or baseline deviations applications, source and destinations. The change monitor dashboard must compare changes in applications, source and destinations in terms of percentage increase/decrease for last 15 mins/ 30 mins/ one hour/ one day against historical time period of 24 hours/ 7 days/ one month etc.
92 45	93 The APT sensor should support Session based (not packet based) differentiated services code point (DSCP) classification.
94 46	95 The solution must provide a Single View on Known Threats, Unknown/Zero-day Threats (identified through static and dynamic analysis), Hosts/Users visiting malicious URLs, Hosts/Users resolving malicious domains, applications involved in Zero-day/Unknown attacks, applications using non-standard ports, and detailed view on security policies allowing applications on non-standard ports.
96 47	97 The solution must provide detailed Change monitor or baseline deviations applications, source and destinations. The change monitor dashboard must compare changes in applications, source and destinations in terms of percentage increase/decrease for last 15 mins/ 30 mins/ one hour/ one day against historical time period of 24 hours/ 7 days/ one month etc.
98 48	99 The solution must provide detailed view on User Activity (along with source and destination IP) with granular view on Data transferred (bytes/sessions), threats associated with a user, Content and URLs accessed by User. This information must be available in Graphical as well as tabular format.

1004 **9**	**101 The APT solution must be from a different OEM than the Endpoint security OEM like AV, HIPS etc.**

IVRS System (Hardware + Software):

Specifications
Solution should provide an embedded IVR functionality with following features:
Should be scalable to support 10 PRI Lines
Automated Attendant
Multi Language Support
Database Query, Execute, Timer functions
Prompt, Play, Record, Speak functions
Dial, Answer, Call Reject, Hang Up
Get Digits, Route, Wait for Key functions
Integration with other databases or web services
Embedded Speech Recognition and Text to Speech
Exclusion Management
Callback scheduling
Asynchronous Play
Voice Media Simulator
Self service portal to manage IVR prompts.
Self service portal for prompts recordings.
Self service portal for Voice message/SMS
Outbound IVR for Voice Broadcasting (Notifications, alerts, advisory)
Agent Screen pop ups
File I/O Functions
Reuse of Project Names
Voice XML 2.0 compliant, Voice XML 2.1 compliant
Transaction Recording(Optional)
Supports Third Party Verification Processes(Optional)
Ability to Extend Application via Application Programming Interface
Application Interface
GUI client application
Centralized resource management
Redundancy options
Off-Line development of the IVR script
Transfer to ACD service, agent, external, Voicemail etc.,
IVR should allow to create prompt text such as greetings, closings and attention retainers
Should run on COTS servers
Note: The vendor should provide all the necessary hardware, software, customization, integration, support and maintenance. Redundancy and high availability

Advanced Persistent Threat Prevention Solution:

S. No	Specification
1	The solution must be Hardware based on premise solution with dedicated appliance based Sensors and Analysis appliances. The sensors must intercept traffic and forward to Analysis appliance for APT and Zero-day detection.
2	The APT analysis appliance should support 128 GB RAM, 128 GB HDD, 4 no of Gigabit interfaces. It must support dual 6-core processor for high performance. The APT sensor appliance most support dual power supplies and 12x 1 Gig, 8x 1 Gig SFP.
3	The APT sensor must deliver at least 2 Gbps performance with 64B HTTP packet and 1 Gbps of performance with vulnerability, anti-malware, anti-virus, anti-bot, application visibility and control. The performance must be measured using Data Center Environment with all Traffic enabled (not just internet traffic). The OEM must furnish details of the testing methodology.
4	The APT sensor must support at least 250,000 concurrent sessions. The session count must be active TCP connections. The concurrent sessions must not drop while enabling all requested features.
5	The APT sensor must support deployment in Tap mode, Transparent mode and Inline (Layer 3) mode. The sensor should support deployment capability in all modes simultaneously.
6	The APT sensors should have dedicated inbuilt hardware resources for access and management at all times, and must be available irrespective of load.The solution must report on the CPU usage for management activities and CPU usage for other activities.
7	The APT sensors must not have Application specific chips like ASICs that doesn't allow future firmware and feature expansions on the same hardware. Solution must be based on parallel processing architecture and must not use proprietry ASIC chips.
8	The APT sensor must support Full tunnel, split tunnel and application specific tunnel for client to site VPNs to identify zero-day malware for outside users. Solution must allow custom policies to control VPN traffic based on users, applications. It must allow different policies for different users groups for threat (Viruses, vulnerabilities, zero-day malware) within VPN traffic.
9	The APT sensor should support optionally Active/Active and Active/Passive HA (not required from day one.) and must support synchronization of the following for HA. -All sessions -Decryption Certificates -All VPN Security Associations -All vulnerability and AV sessions -All threat and application signatures -FIB Tables
10	The proposed solution must support different Custom vulnerability and Application policies for different users and groups.
11	The APT sensor should support Session based (not packet based) differentiated services code point (DSCP) classification. This should help in end-to-end priority policing and C2S & S2C direction enforcement.
12	The APT solution must identify unknown malware and zero-day exploits across any port, protocol and application. It must not be limited to just Web, Email or Files only. The solution must not require MTA deployment for malicious file scanning through emails.
13	The solution must be unified to analyze malicious files across any application/port or protocol. There must not be multiple individual appliances for Web, Email or File scanning.
14	The solution must be scalable and a single sandbox appliance should handle multiple networks and

	segments through sensors.
15	The solution should support enhanced File type support: .exe, .dll, .scr, .ocx, .sys, .drv, Adobe (.pdf), Microsoft Office Documents (.doc, .docx., .xls, .xlsx, .ppt, and .pptx), Non-Microsoft document types (.rtf), Java (.jar and class files), Adobe Flash .swf
16	The Solution should support (zip/gzip), packed and encrypted (SSL) content and analysis of commonly embedded objects such as Javascript, flash, images, etc. within these file types.
17	The solution must support inspection against files within SSL and SSH encryption. The solution must not use any third party (Different OEM) for decryption.
18	The Solution must support both inbound and outbound SSL and SSH decryption.
19	The Solution must decrypt, identify and block malicious data upload and download in applications over SSL.
20	The Solution must decrypt and identify SSH traffic and Tunneling applications. It should have the capability allow SSH traffic but drop tunneled applications.
21	The solution should support protection against anti-VM evasion techniques that include sleep calls, enumerating for processes and debuggers, simulating user environments (key clicks, mouse clicks, mouse movement, etc.), detection of malware attempting to determine what port the VM process is connected to, determining if the VM is running in a single processer versus a multi-core processors, etc.
22	The solution should allow automated signature creation within 5 mins of Zero-day/Unknown malware detection.
23	The APT analysis appliance must automatically create signatures in the Sensor appliances without manual intervention. The Signature must be based on content/payload, not just hash and URL.
24	The solution must support submission of up to 1,000 samples per day and up to 10,000 report queries per day.
25	The solution should provide detailed analysis of every malicious file sent across multiple operating system environments, including both host-based and network-based activity
26	The APT sensor must allow policy rule creation for application identification, user identification, host profile, threat prevention, content filtering, file blocking, QOS and scheduling in a single rule and not at multiple locations
27	The proposed solution shall be able to create application signatures for Homegrown and custom applications without any additional cost.
28	The APT sensor must support different actions in the policy such as deny, drop, reset client, reset server, reset both client and server.
29	The solution must provide complete Session data associated with the delivery of the malicious file, including source, destination, application, User-IDTM, URL, etc.
30	The proposed solution shall support DNS-based signatures to detect specific DNS lookups for hostnames that have been associated with malware. The solution must identify hosts interacting with malicious domains, not just unknown domains.
31	The solution should provide access to the original malware sample for reverse engineering and full PCAPs of dynamic analysis sessions.
32	The solution must support minimum four level of decompression/decoding for any combination of decoding: ZIP, gzip, base64,chunked, uuencode.
33	The solution must provide the ability to block files with multi-level-encoding with 5 or more level of compression e.g office file in 5 levels of zip.
34	The proposed solution shall support packet captures based on: -Applications -Unknown Applications -any threat

	-data-filters
35	The solution must support an open API for integration with best-in-class SEIM tools and leading endpoint agents.
36	The API must enable to programmatically send file analysis jobs to Sandbox environment and query for report data through a simple XML API interface.
37	The solution must allow configurations for file types and file size that needs to be analyzed in Sandbox environment. The other file types must not hit the sand box appliance at all.
38	The Proposed solution should support authentication for terminal services like Citrix and Microsoft.
39	Solution should detect probable exploit kit activity targeted at a host on the network. Exploit kits should be identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature.
40	The proposed solution must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance
41	Solution should correlate and detect hosts that have received malware detected by inbuilt APT solution, and have also exhibited command-and-control (C2) network behavior corresponding to the detected malware.
42	Solution should detect probable exploit kit activity targeted at a host on the network. Exploit kits should be identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature.
43	Solution should correlate and detect likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc.
44	The solution must provide detailed Change monitor or baseline deviations applications, source and destinations. The change monitor dashboard must compare changes in applications, source and destinations in terms of percentage increase/decrease for last 15 mins/ 30 mins/ one hour/ one day against historical time period of 24 hours/ 7 days/ one month etc.
45	The APT sensor should support Session based (not packet based) differentiated services code point (DSCP) classification.
46	The solution must provide a Single View on Known Threats, Unknown/Zero-day Threats (identified through static and dynamic analysis), Hosts/Users visiting malicious URLs, Hosts/Users resolving malicious domains, applications involved in Zero-day/Unknown attacks, applications using non-standard ports, and detailed view on security policies allowing applications on non-standard ports.
47	The solution must provide detailed Change monitor or baseline deviations applications, source and destinations. The change monitor dashboard must compare changes in applications, source and destinations in terms of percentage increase/decrease for last 15 mins/ 30 mins/ one hour/ one day against historical time period of 24 hours/ 7 days/ one month etc.
48	The solution must provide detailed view on User Activity (along with source and destination IP) with granular view on Data transferred (bytes/sessions), threats associated with a user, Content and URLs accessed by User. This information must be available in Graphical as well as tabular format.
49	The APT solution must be from a different OEM than the Endpoint security OEM like AV, HIPS etc.

u. KVM Switch

Minimum technical specification
One number of 8 port IP based KVM switch for centralized monitoring of servers along with 8 cables, converter and connectors for server connectivity. 18.5” TFT-LCD collapsible flat panel monitor console kit with keyboard and mouse including cables (1U).

1 Local, 2 Remote with necessary user licenses 10/100/1000 Mbps PS2/USB

v. 10 inch Tablet PC with Battery Backup

Description	Minimum Specification
CPU	1.3 GHz Quad Core or above
RAM	2 GB DDR3
INTERNAL STORAGE & EXTENDED CAPABILITY	16GB & Feasibility to extend up to 32 GB micro SD
SCREEN	Minimum 10.x" with resolution 1280*800 IPS display, 16:9 aspect ratio.
Touch Panel	10 point Multi Touch
CAMERA	• Front 2.0 Mega pixels & Back 5.0 Mega pixels with HD 2048 x 1536 pixels • 720p @30fps • Geo tagging function/ reference function.
NETWORK Features · Wi-FI · SIM slot · Bluetooth · Voice Call	 Yes (802.11b/g/n) Yes Yes-Ver.4.0 Yes
OS	Android4.4 Kitcat or with latest version
Language	English & Multi Language
Applications	Adobe-reader, Photo-JPG, BMP, Video/Audio Player
Connectors	USB, Micro-SD, SIM, Speaker
User Manual	Yes
Charger	Yes
Data Cable	Yes
Certification	BIS & RoHS
Battery	5500mAh with 8 hours backup on video mode
Warranty	3 yrs onsite comprehensive

w. Thermal Printer

Thermal Printer	
Memory flash	2 M Flash or higher
Firmware support which can support Barcode	UPC-A, UPC-E, Code 39, Code 128, Jan8 and Jan13 (EAN Codabar, PDF417
Connectivity	USB and Serial
Print methods	Direct thermal
Printing of barcodes, text and graphics.	Barcode, Text, Ability to print logo :
Resolution	203 dpi/8 dots per mm
Print Width	80mm
Print speed	230mm/ Sec or higher
Media Sensors	Paper low sensor
Microsoft Windows Drivers	Microsoft windows drivers i.e Win 7, Windows Vista 32 & 64, x professional, WEPOS, Embeded POS Ready
RS 232 Interface	RS 232 connector/ Interface

USB Interface	USB Interface

x. High End Scanner

Item	Minimum technical specification
Scanner type	A4 flatbed colour image scanner and also should have A4 sheet fed, one pass duplex scanner
Scanning Method	Fixed document and moving carriage (for flatbed), Fixed carriage and moving document (for ADF)
Optical Sensor	4-line colour CCD
Optical Resolution	1200 dpi x 1200 dpi
Scan Speed (Colour) Time (300dpi)	Less than or equal to 8 sec
Scan Speed	30 ppm or more in Duplex mode
Multi Feed Detection	Ultrasonic Sensor
System Interface	USB 2.0
Media types supported	Ability to scan Paper of thickness upto 80GSM and more and paper size A4/Letter/Legal along with photograph pasted on the paper.
Scan file format	PDF, searchable PDF, JPG, BMP and more
Compatible Operating System	Windows XP/Vista/7, Mac
Power Consumption	Less than 15 watt in standby mode.
ADF Capacity	100 sheets or more
Daily Duty cycle	More than 2500 pages
Energy Star Qualified	YES

y. 80 Column Dot Matrix Printers:

Item	Description of requirement
Print Method	Serial Impact Dot Matrix
Print Direction	Bi-directional logic seeking
Print Head - Type	24-Wire
Print Width	80 - Column
Print Head Life	200 Million Characters
Print Speed	
Character Pitch (cpi)	15 12 10
High Speed Draft (cps)	>=300 >=360
Draft (cps)	>=250 >=300 >=375
Letter Quality (cps)	>=80 >=100 >=125
Draft - ISCII (cps)	250
LQ - ISCII (cps)	41
Resident Printer Fonts	
Draft	Draft, High Speed Draft
Letter Quality	Roman, Sans Serif, Courier, Prestige, Script, Script - C, Orator, OCR-B, Orator - S
Letter Quality Scalable Fonts	Roman & Sans Serif (8 - 40 Points)
Resident Barcode Font	Code 3 of 9
Paper Handling	

Paper Path-Standard	Top, Rear and Bottom
Continuous-Tractor Feed- Standard	Convertible Push & Pull
Paper Size	
Continuous From Width	4 - 16"
Paper Thickness (max) - Tractor feed	0.3mm
Paper Thickness (max) - Friction feed	0.3mm
Copy Capability	1+3 with Carbon
Consumables - Ribbon	
Type	Ribbon Cassette
Color	Standard Black
Buffer (Kilo Bytes)	100 KB
Acoustics - Noise Level	55 Db (A)
Interface	
Standard	IEEE-P1284A Parallel & USB (Auto interface switching)
Electrical Specifications	
Operating Voltage	150-270 V AC
Mains Frequency	47 - 63 Hz
Power (Standby)	12W
Environmental - Operating Conditions	
Temperature	5 to 45 C
Relative Humidity	10% to 80%

z. Multi Functional Unit

Item	**Minimum Technical Specification**
Print Speed	60 PPM (Letter) or more, 55 PPM (A4) or more
Application	Network-ready, high volume, high performance, two-sided printing,copying, scanning, digital sending, and analog faxing
Paper Input	800 or more-sheet capacity:
	100-sheet multipurpose tray 1 and two 500-sheet input trays 2 and 3
	(Optional: 2,000 or more sheets capacity via two additional 500- sheet input trays 4
Paper Output	**500-sheet output bin**
Copying/Scanning	Via 50-sheet reversing automatic document feeder or colour flatbed Scanner
Faxing	Standard
Duplex Scan Speed	**65 sides per minute (A4)**
Scanning Type	**DADF / RADF**
Digital sending	Send to e-mail or network folder; advanced digital sending with optional software
Automatic Two-Side Printing	Standard
Memory/Storage Memory Enhancement technology (MEt); 40 GB hard disk	256 MB DDR RAM (fixed), expandable to 512 MB via one open DDR DIMM slot;
Connectivity	Fast Ethernet-10/100Base-TX Ethernet embedded print server; Hi- Speed USB 2.0 port; (10/100/1000)
	EIO slot; Foreign Interface port; analog fax port

aa. 1 KVA Line Interactive UPS

Description
Input Characteristics
Voltage Range (VAC): 150-305
Frequency (Hz): 50 +/- 6%
Input P.F : greater than 0.9
Input Harmonics : should be less than 7 %
Phase: Single Phase, Three-Wire
Waveform: Sinewave
Battery Voltage (VDC): 12V/24
Battery: 12V/7AH
Hot swappable of batteries should be possible in UPS :
Back-up: 30 minutes for Single P4 Pc with 15 " Monitor and 1 Printer
Inverter Output
Capacity (VA/W): 1000/700
Voltage (VAC): 230+/-5% (Battery), 202-253(AC)
Frequency (Hz): 50 +/- 0.2% (BAT)
Switching Time: Typical value 6 ms, including detection time and switching time
Efficiency: 77% Batt Mode
Overload Capacity
Utility Power: Load >= 200% - 3 seconds, Load >= 100% - 5 minutes
Battery Load: + 150%-1 second, Load >= 100%-30 seconds
Other Characteristics
Recharge Time: 8 Hrs for 90% charge
Communication: RS 232 support UPsilon2000 / Power manager
Alarm: Output: overload, Battery under voltage, Utility power abnormal, UPS
Panel Indication: LCD/LED shows UPS operation status
Sound Level: <55 db
Protection: Battery low protection, Overload protection, Short circuit protection, Temperature protection
Relative Humidity: 0-95% without condensation
Environment Temperature: 1-40°C
Built In Automatic Voltage Regulator
Valid test certificate to be be produced from ETDC/CPRI/or any NABL Approved Labs
ISO Certification – 9001, 14001, 18001
vendors should be empanelled in centre for e governance, Govt of Karnataka
similar capacity should have been supplied to any one customer at least 400nos in last two years and satisfactory performance should be produced

bb. 136 Col. DMP

Item	Description of requirement
Print Method	Serial Impact Dot Matrix
Print Direction	Bi-directional logic seeking
Print Head - Type	24-Wire

Print Width	136 - Column
Print Head Life	200 Million Characters
Print Speed	
Character Pitch (cpi)	15 12 10
High Speed Draft (cps)	>=300 >=360
Draft (cps)	>=250 >=300 >=375
Letter Quality (cps)	>=80 >=100 >=125
Draft - ISCII (cps)	250
LQ - ISCII (cps)	41
Resident Printer Fonts	
Draft	Draft, High Speed Draft
Letter Quality	Roman, Sans Serif, Courier, Prestige, Script, Script - C, Orator, OCR-B, Orato- S
Letter Quality Scalable Fonts	Roman & Sans Serif (8 - 40 Points)
Resident Barcode Font	Code 3 of 9
Paper Handling	
Paper Path-Standard	Top, Rear and Bottom
Continuous-Tractor Feed-Standard	Convertible Push & Pull
Paper Size	
Continuous From Width	4 - 16"
Cut sheets Width	7.2 - 16.1"
Paper Thickness (max) - Tractor feed	0.3mm
Paper Thickness (max) - Friction feed	0.3mm
Copy Capability	1+3 with Carbon
Consumables - Ribbon	
Type	Ribbon Cassette
Color	Standard Black
Buffer (Kilo Bytes)	100 KB
Acoustics - Noise Level	55 Db (A)
Interface	
Standard	IEEE-P1284A Parallel & USB (Auto interface switching)
Electrical Specifications	
Operating Voltage	150-270 V AC
Mains Frequency	47 - 63 Hz
Power (Standby)	12W
Environmental - Operating Conditions	
Temperature	5 to 45 C
Relative Humidity	10% to 80%

cc. Book Scanner

Specifications
1 Size and Scanning Specifications

Scan Area : A3 + - Up to 560mm x 370mm (open book), 280mm x 370mm (per page)
Optical Resolution : 400ppi optical
Maximum Book Thickness : up to 170mm
Color Tone : 24bit color; 8bit grey; 1bit b/w
File Formats : JPEG, TIFF, RAW, BMP,GIF, PDF, PDF OCR, XML
2 Capture Technology Specifications
36MP Dual CMOS Sensors capture system
Carl Zeiss 50mm Makro Planar Lenses
Easy to upgrade, exchange and maintain
3 Cradle Specifications
V-Shape minimum 80 degree book cradle with soft spine support
Automated pressure controlled book support flaps
Anti slip mats for perfect stability
Anti Glare Glass plate to flatten the pages and optimize curvature free scanning
Glass to be automated movement and pressure controlled
Easy change between modes - no second unit to scan covers or problematic pages or books.
4 Page Turning Specifications
Automated Bionic Finger system with secure page separation and turning
Nearly touch free: not more than 5 mm² point of contact to the book
Double Page control system based on laser light measure tool
Every page to be measured with a light density sensor. Never turn more than one page
5 Light System Specifications
LED cold light with constant illumination
No UV emission
Easy to upgrade, exchange and maintain
6 Computer Specifications
Integrated Computer System with multicore processing, 4TB storage and 24 inch Flat Screen
Monitor
Integrated 64 bit Software for single and batch mode capturing, processing, image
enhancement, on the fly OCR and workflow management
7 Other Specifications
Is a table top system, easy to install, place and reposition
System should work around the book, leaving it in place, not stressing the binding, the pages or
the covers
Easy to use Automated Operations, with minimum operator interference
A modular system, that in current form has a life expectancy of 10 years and parts availability
of 12 years
Can be easily upgraded in time in terms of image quality
Fully customizable to suit project requirements

dd. Back UP Solution

No	Requirements
	Backup Management Software
1	All backup/restore administration must be controlled by a centralized master system

2	The master system must support the following systems: 2008/2008R2 & Linux (x8664) 5.x/6.x
3	Supported client systems include: Windows, Linux, Unix and Mac OS X Platform
4	The software must be based on Graphical User Interface (WebGUI) so that all backup servers can be managed centrally, regardless of location
5	Proposed solution should also support complete BMR backup with incremental snapshots for virtual machine and Physical server running on both Windows and Linux environment and should support restoration on Similar and Dissimilar Hardware including Hypervisor Hyper-V, VMware, Cirtrix Xen
6	Proposed solution should also support latest space saving technologies like de-duplication and compression and universal recovery.
7	Proposed solution should support universal recovery to restore physical machine to virtual or vice-versa.
8	Full backup and restoration capabilities management from remote location.
9	Network bandwidth compression for management of network utilization to reduce loads when backup occurs during production time.
10	Support for leading connectivity protocols :-
	a. SAN iSCSI / FC
	b. NAS
	c. Ethernet Technologies 10/100/1000/10000 BaseT
11	Must be capable of “block level” backups for Bare Metal Recovery of Physical servers
12	Should have specific agents to perform “hot” backups on the following databases and applications such as:
	a) Oracle on Windows/Linux and Unix
	b) Informix on windows/Linux and Unix
	c) Sybase on windows/Linux and Unix
	d) DB2 on windows/Linux and Unix
	e) MS SQL on window
	f) MySQL on Linux and Windows
	g) Postgres SQL on Linux and Windows
	h) Ms Exchange on Windows
	i) Lotus Notes in Windows/Linux and Unix
13	Should meet the following Media Management capabilities
	a. Allow tape library sharing among media servers
	b. Allow individual tape drive sharing among media servers and allow for reconfiguration without rebooting media servers
	c. Tape drive sharing must support both iSCSI and Fiber based connections.
14	The software should be capable of performing of Restart able backup.
15	The software inbuilt reporting tool must has the ability to create customize reports without any additional purchase of another reporting module or 3rd party reporting module
16	The size of index or catalogue file must be less than 100 bytes per files/folder/directories that are being backed up.
17	Ability to integrate with storage NAS snapshot based protection mechanisms by providing control GUI module

18	Ability to support and manage snap shot based backup, and file based backup “ under one roof “ while maintaining granular file level recovery.
19	Must support storage protocols such NDMP (version 3 & above). Please provide interoperability matrix with storage appliance firware/OS release compliance. Specify specific features advantages aligned with the storage vendors
20	Must be able to utilize Direct Access Restore for NDMP technologies to facilitate single file level restore.
21	Should support 5 ways NDMP Backup.
22	Support for server virtualization especially VMWare & Hyper-V
23	Must be integrated with VMware VADP with D2D2T layout. Must be synchronized with VMware VADP for data integrity.
24	Allows full VMware VADP backup by utilizing LAN, SAN and HotAdd advanced transport mechanisms to optimize data transfer of virtual machine backups.
25	Proposed backup solution should come with • Enterprise Edition Backup License on Windows • 1 nos. of MS-SQL Cluster License • 30-40TB NDMP License • 18TB RDA License for De-Dupe Storage • 1 Backup Server with 16GB Memory, 2 * Quad Core Processor, 2 * 300GB 15K HDD, 2 * 10G NICs and Windows Server Standard 2012 OS • De-Dupe Storage – 18TB • Tape Library with Minimum with 3 Drives • 20 Tapes Media • 3 years 24X7 support by OEM

ee. Archiving Solutions

Sl. No.	Technical Specification
1	The solution must be capable of archiving content from multiple sources like messaging including MS Exchange, Domino File Servers , MS Sharepoint, VOIP etc
2	The proposed solution must have integration with Email solution through SMTP archiving without the need of any additional hardware.
3	The solution should have the capability to archive data from multiple electronic repositories to single repository to achieve best single instance across multiple frontend source data.
4	The solution must support a Single unified console to manage archiving from different sources like File server, SharePoint, Mailing solution etc
5	The solution should reduce redundancy of archived content by ensuring single instance storage across different sources like emails, email attachments, SharePoint, file servers etc. The single instance capability should not require any additional software and storage features.
6	The solution must have capability of global single-instance across multiple storage partition which are even dispersed geographically.
7	The solution should support complete ILM of source content by facilitating migration from primary disks to secondary disks to tapes (for long term) while providing seamless access to end-user without any IT intervention
8	The solution should be cluster-aware and must support Windows native clustering
9	The solution should also facilitate a cold standby on which the archiving services can be quickly failed over.
10	The solution should facilitate addition of archiving servers to handle additional archiving finger printing

	workload whereas data repository will still be on old server.
11	The solution should provision a web based discovery mechanism to search relevant data across archives from multiple sources like file server, messaging, SharePoint etc. The discovery mechanism should support a guided, hierarchal review of searched data with capability to filter, marking and legal hold to prevent deletion/expiry.
12	The solution should facilitate a supervision mechanism for emails to ensure compliance of messaging content. The supervision mechanism should facilitate sampling of messages and subsequent review by authorised personnel
13	The solution should support tagging of messages by message security solutions like anti-spam/anti-virus for efficient retention
14	Proposed solution must support outlook on Windows & MAC machines.
15	Archival solution must have support with IMAP compliant devices to access thy emails.
16	Proposed solution should support archiving both at premises and cloud.
17	Proposed solution must have monitoring integration with messaging solution vendor; Microsoft System Centre Operations Manager (SCOM) for easy management.
18	The solution should support Message Journaling as well as Envelope Journaling, capture BCC data and expansion of distribution lists
19	The solution must support "Agentless" archiving of messages. There should be no need to deploy any agent on the messaging server.
20	The solution must support search for mails based on undisclosed recipients criteria
21	The solution should support seamless access using shortcuts from the native email client as well as browser based client. The solution should support all archiving actions like manually archive, search, restore, retrieve, delete from the native email client and browser based client
22	The solution should support archiving based on either any or a combination of the following criteria: - Item Type (message, calendar etc.) - Date - Size - Email Attachment only - User - Organizational Unit
23	Proposed solution must have advance way of archive disk/partition data backup to avoid backup of old partitions which must be possible with or without WORM devices.
24	The solution should also support creation of "filter-rules" to configure more sophisticated archiving policies
25	The solution should not be dependent on journaling for archiving mails from identified user mailboxes. The two solutions should work independent of one another.
26	The solution should be able to selectively mark old archived data as "read-only". E.g. Quarterly archived data should me marked as read-only.
27	The solution shall facilitate migration mails located at end-user desktop/laptop in the form of PST/NSF. The migration should retain the original folder structure
28	The solution should support WORM features of storage boxes i.e. HCAP
29	The solution should support storing local copies of archived content to ensure optimal bandwidth utilization.
30	The solution must support automatic expiration of shortcuts from mailboxes based upon time which may be shorter than the retention period of the mails. E.g.: customers may keep shortcuts for 1 year and archived items for 3 years.

31	The solution must allow the administrators to configure the following in shortcuts: - Include recipient information in the shortcuts. - Include nothing / original message body / custom message body in shortcuts. - Include "X" number of characters in the shortcut. - Include a custom body defined from a configuration file in the shortcut etc.
32	The solution should leave a shortcut at either the time of archiving or later as well.
33	The solution should allow users to view archived items directly without having the need to restore them to the messaging server to avoid delays and impact on messaging solution. No network connections should be established between archiving server and messaging server at the time of retrieving archived items
34	The solution must support indexing and archiving of minimum 500+ commonly used file types.
35	The solution should support archiving of entire email folders and application of selective archiving policies based upon folders.
36	The solution must support dynamic retention period of archived items i.e. retention of archived items can be increased or decreased on fly.
37	The solution should facilitate "future proofing" of content by facilitating an HTML copy for long term retention and search
38	The solution should support "safety copies" of items to be kept on the mail server. The "safety copy" allows the archiving software to wait for the archived item to be backed up or replicated before the original item is removed from the mail server.
39	Archival solution must have option to set or configure disk property read and read-write access
40	Archival solution must have disk configurable option with High & Low watermark. In case, Height watermark reaches, disk should automatically become Read only and other pre-configured disk should get read-write access to store fresh archived items.
41	The solution must have OWA integration in such a fashion that archived item can be browsed directly through archived browser tab instead of browsing through internet explorer (IE). IE can be additional feature.
42	The solution should provide out of the box reporting for the following: • Volume of items archived per archiving server • Mailbox archiving status • Archive quota usage per user • Most frequently accessed archived items • Journal mailbox archiving status and trends • Archive store usage by archive or billing account The solution should facilitate customization of reports, export reports in PDF, XLS, HTML, TIFF formats and schedule generation and emailing of report
43	The archival solution must have offline access of archived emails from day one even when user is not connected to network.
44	The solution should facilitate seamless migration of shortcuts and access to archives to a newer version of messaging solution or a supported messaging solution from a different vendor
45	The archival solution must have an integrated e-discovery solution which allows guided **Discovery, review** and **analysis** of data from the archives and non archived data like desktop, SharePoint, file server, Documented etc. It’s required for future proofing.
46	Proposed Archival solution must have seamless and consistent end user search experience across multiple interface like Desktop/Laptop, mobile, tablets etc.

ff. <u>External Tape Drive</u>

Performance	
Native sustained transfer rate	160 MB/s
2:1 compressed transfer rate	400 MB/s
Native formatted capacity	2500 GB
Compressed formatted capacity	6250 GB
Burst Transfer Rate (MB/sec)	600
SAS (max)	
Data Buffer Size	512 MB
Average file access time	50 sec
Interfaces available	6 Gb/s SAS
Tape Format	
Format	LTO Ultrium 6
Recording density	15.143 Kb/mm
Encoding method	16 Channel 32/33 RLL NPML
Data compression	2.5:1
Physical	Internal w/ bezel
Width (in/mm)	5.87 / 149.1
Height (in/mm)	1.76 / 44.65
Length (in/mm)	8.3 / 211
Weight (lbs/kg)	3.2 / 1.45
Environmental	
Operating Temperature	50° to 104° F / 10° to 40° C @ 6 CFM
Operating Non-condensing humidity	20% to 80%
Altitude	13,000 ft (4,000 m)
Non-operating Temperature	-40° to 149° F/-40° to 66° C
Non-operating Non-condensing humidity	10% to 95%
Power	
Voltage	+5V, +12V
Power consumption	Idle: 3.8 Watts
	Typical: 23.8 Watts
	Peak: 31.5 Watts
Reliability	
MTBF	250,000 hours at 100% duty cycle
MSBS	1,000,000 cycles
Load/Unload Life	100,000 cycles
Non-recoverable Error Rate	1 in 1 × 10^{17} bits (non-media error, clean drive)
Media Compatibility	
LTO-6 (read/write)	
LTO-6 WORM (read/write)	
LTO-5 (read/write)	
LTO-5 WORM (read/write)	
LTO-4 (read only)	
LTO-4 WORM (read only)	
Media Specifications	

Cartridge Dimensions	4” × 4.15” × .85”
(L×W×H)	(102mm × 105.4mm × 21.5mm)
Archive Storage	30 years

Image Sensor Type		Charge coupled device (CCD) image sensor (x 2)
Output Resolution	Monochrome, Grayscale and Color	50 to 600 dpi
Optical Resolution		600 dpi
Output Format		Color: 24-bit; Grayscale: 8-bit; Monochrome: 1-bit
AD Converter		1,024 levels (10-bit)
ADF Capacity		200 sheets
Document	ADF Minimum	A8 (52 mm x 74 mm or 2 in. x 3 in.)

gg. **Scanner (Scanning cum Bar-code reading feature)**

Size	ADF Maximum	A3 Portrait (297 mm x 420 mm or 11.7 in. x 16.5 in.) Double letter (279.4 mm x 431.8 mm or 11 in. x 17 in.)
Interfaces		Ultra SCSI, USB2.0/USB1.1 (Selectable)
Scanning speeds[2]		
Letter/Landscape Mode	**Simplex**	**Duplex**
Monochrome, Grayscale & Color @ 200 dpi	90 ppm	180 ipm
Monochrome, Grayscale & Color @ 300 dpi	80 ppm	160 ipm
Ultrasonic double-feed detection with advanced control		
Loaded with "intelligent" functions for more efficient scanning		
Comes with 2D Barcode for Paper Stream		

Important note:-

Scanning Solution	• The OEM of the scanner shall have to provide required API/SDK to integrate the storage of the scanning output with the central server but not in the local HDD/memory of PC/Desktop where scanner is connected • All the scanners installed in a particular location would be connected in local LAN and linked to the Router/Firewall/Switch of that location/scanning centre for onward storage of scanned images at the central server • The API/SDK of the OEM would be useful to do analysis of the individual scanned pages, creation of meta data of the Answer Booklet(AB) • API/SDK of scanner shall have a provision to read Barcode values printed in the first page and odd pages of the Answer Booklet and record it in a variable to store and process in the later stage • Each AB would be having minimum 35 pages to maximum 55 pages as on today and all pages of one AB should be saved one file in a pdf format • Each AB would be having different bar code values for security purposes to avoid link information from one stakeholder to another involved in the total examination process, therefore the API/SDK of the scanner shall have a provision to capture all bar code values in different variables