Annexure 1- Technical Specifications

1. SSL Device

S no	SSL Offload-Minimum Requirement Description
1	Device should support day 1 Layer 7 throughput of atleast 10 Gbps
2	System must support minimum of 150 K Layer 7 CPS
4	System should have Minimum 8000 SSL TPS (SSL handshake per second) for 2048 bit SSL
5	system must support bulk encryption of 4 Gbps
6	System must have Minimum 2 x10G SFP+ Ports (fully populated) and options for min. 2 SFP+ for 10G connectivity
7	System must support High availability
8	The appliance should support Self generates CSR (Certificate Signing Request), self-signed Certificate and private key for specified host.
9	The appliance should have integrated hardware SSL termination/ acceleration i.e. end to end ssl support to act as a SSL Server and/or as SSL Client
10	Supports cyptographic standards like AES, 3DES, DES, RSA etc and variable key lengths (512|1024|2048|4096)
11	System should support different protocol parsers such as HTTP, SSL, DNS, FTP,TFTP, SIP, SMTP, SPDY, RTSP, RADIUS,
12	System should support SSHv2/SNMPv3
13	System should support TLS 1.0, TLS 1.1, TLS 1.2, SSL3
14	System should support Hashing Algorithms like MD5, SHA-1, SHA256, SHA384
15	System must fully support IPv6
16	System must support NAT46
17	Comprehensive onsite hardware warranty for 3 years with Next business Day (NBD) resolution.
18	The solution should have dual AC power supply fully populated (within box) from day one
19	System must support at least 30 Application Delivery partitioning / Virtual context, dedicated configuration file, routes for each customer's traffic, where in resources can be either dedicated to each partition or can leverage common pool of resources i.e. CPU and Memory, concurrent connection for each context should be configurable

2. Web Application Firewall

Sr. No.	WAF - Minimum Requirement Description
1	The Web application firewall should address Open Web Application Security Project (OWASP) Top Ten security vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), Broken Authentication and Session Management
2	The solution should prevent the following attacks (but not limited to):
	a) Brute force /DDOS
	b) Access to predictable resource locations
	c) Unauthorized navigation
	d) Web server reconnaissance
	e) HTTP request format and limitation violations (size, unknown method, etc.)
	f) Use of revoked or expired client certificate
	g) File upload violations.
3	Should support positive and negative security model.
4	Should have the ability of caching, compression of web content and SSL acceleration.
5	Should meet all applicable PCI DSS requirements pertaining to system components in the cardholder data environment, should also monitor traffic carrying personal information.
6	Should have the ability to inspect web application output and respond (allow, block, mask and/or alert) based on the active policy or rules, and log actions taken.
7	Should inspect both web page content, such as Hypertext Markup Language (HTML), Dynamic HTML (DHTML), and Cascading Style Sheets (CSS), and the underlying protocols that deliver content, such as Hypertext Transport Protocol (HTTP) and Hypertext Transport Protocol over SSL (HTTPS). (In addition to SSL, HTTPS includes Hypertext Transport Protocol over TLS.)
8	WAF should support dynamic source IP blocking and should be able to block attacks based on IP source.
9	The solution must be able to perform validation on all types of input, including URLs, forms, cookies, query strings, hidden fields, and parameters, HTTP methods, XML elements and SOAP actions.
10	Inspect any web socket protocol (proprietary or standardized) or data construct (proprietary or standardized) that is used to transmit data to or from a web application, when such protocols or data are not otherwise inspected at another point in the message flow.
11	WAF should support inline bridge or proxy mode of deployment.
12	WAF should have an option to configure in Reverse proxy mode as well.
13	Actions taken by WAF to prevent malicious activity should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address.
14	Transactions with content matching known attack signatures and heuristics based should be blocked.
15	The WAF database should include a preconfigured comprehensive and accurate list of attack signatures and geo-location data update service.
16	The Web application firewall should allow signatures to be modified or added by the administrator.
17	The Web application firewall should support automatic updates (if required) to the signature database, ensuring complete protection against the latest application threats.
18	WAF support the following normalization methods:

19	a) URL-decoding (e.g. %XX)
	b) Null byte string termination
	c) Self-referencing paths (i.e. use of /. / and encoded equivalents)
	d) Path back-references (i.e. use of /.../ and encoded equivalents)
	e) Mixed case
	f) Excessive use of whitespace
	g) Comment removal (e.g. convert DELETE/**/FROM to DELETE FROM)
	h) Conversion of (Windows-supported) backslash characters into forward slash characters.
	i) Conversion of IIS-specific Unicode encoding (%uXXYY)
	j) Decode HTML entities (e.g. c, ", ª)
	k) Escaped characters (e.g. \t, \001, \xAA, \uAABB).
20	WAF should support different policies for different application sections.
21	The Web application firewall should automatically learn the Web application structure and elements.
22	The Web application firewall learning mode should be able to recognize application changes as and when they are conducted.
23	The WAF should have the ability to perform behavioral learning to examine traffic and highlight anomalies and provide recommendations that can be turned into actions such as apply, change and apply, ignore etc. The WAF should allows the administrator to define the rules and patterns to apply to a specific page in a Web Application
24	The Web application firewall should support line speed throughput and sub-millisecond latency so as not to impact Web application performance.
25	For SSL-enabled Web applications, the certificates and private/public key pairs for the Web servers being protected need to be up loadable to the Web application firewall.
26	The Web Application Firewall should have "anti-automation" protection which can block the automated attacks that use hacking tools, scripts, frame work etc.
27	The Web application firewall should have an out-of band management port.
28	The Web application firewall should support web based or a centralized management and reporting for multiple appliances.
29	Bidder should be able to deploy the Web application firewall and remove the Web application firewall from the network with minimal impact on the existing Web applications or the network architecture.
30	The Web application firewall should be able to generate custom or pre-defined graphical reports on demand or scheduled.
31	The Web application firewall should provide a high level dashboard of system status and Web activity.
32	Should be able to generate comprehensive event reports with filters:
	a. Date or time ranges
	b. IP address ranges
	c. Types of incidents
	d. Geo Location of attack source
	d. Other (please specify).
33	The following report formats are deemed of relevance: HTML, PDF, XML, etc.
34	The appliance based solution should support Inline, Reverse Proxy mode of deployment.
35	Unique transaction ID should be assigned to every HTTP transaction (a transaction being a request and response pair), and included with every log message.
36	Web application firewall should provide notifications through Email, Syslog, SNMP Trap etc.

37	WAF should be able to log full session data once a suspicious transaction is detected.
38	Should be simple to relax automatically-built policies.
39	The solution should provide the admin to manually accept false positives.
40	Should be able to recognize trusted hosts.
41	The WAF in passive mode should be able to provide impact of rule changes as if they were actively enforced.
42	Should support High availability for WAF sharing the same policy.
43	The solution should support virtual environments.
44	The solution should have the capability of load balancing between the applications in an active – active environment.
45	The Web application Firewall should support authentication with LDAP and radius server.
46	The Solution should allow commands like PING, trace route, telnet from WAF for troubleshooting network related issues.
47	The Solution should have option to configure NTP server details.
48	Support should include 3 years onsite warranty with 24 x 7 support with Next business Day (NBD) resolution.
49	The solution should have network routing feature.
50	In case of RMA Process, Define the no of days to deliver the solution.
51	Should support both IPv4 and IPv6
52	The solution must support the web application vulnerability assessment tools (Web application scanners in Leaders of Latest Gartner Magic Quadrant Application Security Testing) to virtually patch web application vulnerabilities.
53	The solution must be able to support 2 Gbps of WAF (HTTPS) throughput
54	The solution must be a Leader or Challenger in the Gartner Magic Quadrant of Web Application Firewalls 2016/2017
55	System must have minimum(fully populated) 2 x10G SFP/SFP+ Ports and option of min. 2 SFP/SFP+ for 10G connectivity (field upgradable on same hardware)
56	The solution should have dual AC power supply fully populated (within box) from day one.

3. Anti – Virus Solution

Sr. No.	Anti-Virus -Minimum Requirement Description
1	Anti-virus software engine should be installed on all workstations at the requisite facilities
2	The anti-virus software shall be kept current by obtaining the latest updates at regular intervals.
3	All servers and desktops should automatically update the virus definitions from centralized server on daily basis.
4	The solution should be detect and prevent ransomware and its spread
5	The antivirus solution should protect against all kinds of viruses, Trojan horses and worms including: boot sector, master boot sector, memory resident, file multipartite, macro, stealth and polymorphic
6	The antivirus solution should provide scanning capabilities such as:
	On access scanning
	Real time scanning
	On-demand scanning
	Scheduled scanning
	Heuristic scanning
	Compressed file scanning
	Firewall
7	The anti-virus should provide protection for critical system by blocking blacklisted applications.
8	The anti-virus solution should prevent malicious applications from inserting code into trusted applications.
9	Anti-virus should scan email traffic for leading email clients.
10	To address the threats and nuisances posed by Trojans, the solution should be able to do the following:
	Terminating all known virus processes and threads in memory
	Repairing the registry
	Deleting any drop files created by viruses
	Removing any Microsoft Windows services created by viruses
	Restoring all files damaged by viruses
	Includes Cleanup for Spyware, Adware etc
11	The solution would be managed centrally using a web-based console that allows system monitoring, software updates, client configuration, and event reporting. The central site administrator should have the ability to manage the software at all levels of the network and have the ability to remotely deploy product updates and modifications to all users.
12	The solution should be capable of automatic (dynamic) deployment to client workstations, as well as, removal of any existing Antivirus software.
13	The central site management system must be capable of providing a daily report of found viruses, including locations and a report of incomplete or failed nodes updates for each location. These reports must be accessible by the network administrator at the Central Server.
14	The solution should provide an automatic alert to the system administrator on multiple virus detections.

Sr. No.	Anti-Virus -Minimum Requirement Description
15	The solution should provide quarantine management in order to prevent spreading. A management interface must be provided to allow the administrator to review, sort and analyze quarantined items.
16	The solution should provide Role based administration.
17	Virtual Desktop Support : Solution should support Virtual Desktop for Vmware
18	Shall offer customizable & standard notifications via - SMTP, SNMP, Pager, NT Event Log
19	The solution must be in Leader's quadrant of the latest Gartner Magic Quadrant report 2016/17 on End Point Protection
	Server Security
20	Server Security solution should have anti-malware, firewall,HIPS, Integrity monitoring within the Same Agent.
21	Firewall should have the capability to define different rules to different network interfaces.
22	Firewall rules should filter traffic based on source and destination IP address, port, MAC address, etc. and should detect reconnaissance activities such as port scans.
23	Solution should have the ability to lock down a computer (prevent all communication) except with management server.
24	Firewall should integrate with Hypervisors like Vmware ESXi without the need to install agents on the guest VMs
25	Solution should have Security Profiles allows Firewall rules to be configured for groups of systems, or individual systems.
26	Solution should be capable of blocking and detecting of IPv6 attacks.
27	Solution should offer protection for virtual or physical, or a combination of both the environment
28	Product should support CVE cross referencing when applicable
29	Solution should also support restoration of quarantined files.
30	Solution should support integration with Hypervisor components such as vshield endpointAPI (EPSEC) and provide Agentless AntiMalware protection for guest VMs
	Other
31	Comprehensive onsite warranty for 3 years with Next business Day (NBD) resolution.

4. Backup Solution

Sr. No.	Backup - Minimum Requirement Description
1	Backup software must be present as Leaders in Gartner's Magic Quadrant for 2016/17.
2	Backup software must support GUI with centralized management / Single interface for management of all backup activities.
3	The offered software must support Advanced sharing of different media across the environment (disk, tape and optical)
4	The offered software must support multiple level of backups including full, incremental, differential and synthetic full.
5	The offered software must support following application and database backup with native integration (without third party agents integration)for 64-bit Active Directory, SQL, Exchange, Share-Point, Oracle, MySQL, PostGreSQL etc.
6	The offered software must provide Enterprise-wide search and data classification for flat files integrated with the base product.
7	The software must be able to perform inline block-level de-duplication of data across backup and archive.
8	The software must provide Global de-duplication
9	The software must be able to Compress and Encrypt data at the Client-side and this feature should be available even during de-duplication.
10	The offered software must have various Encryption algorithms including 128 bit Blowfish, 128 bit AES, 256 BIT AES and Serpent and encryption granularity and should not demand for additional license, any such license if needed should be quoted for the total backup capacity license.
11	The offered software must support complete integration of Server Backup, Desktop/Laptop Backup, Virtual Machine Backup, Snapshot Management, Archive and Replication Solution with a Single Console to manage all the solutions
12	The offered software solution must support hardware integrated snapshot backup, with application aware, including virtualization and granular recovery option for leading storage vendors Dell, IBM, HP, EMC, HDS, Fujitsu, NetApp etc.
13	The offered software must support sharing of media between media servers to reduce tape count.
14	Backup solution must support multi tenancy feature for creation of distinct data zones.
15	The offered software must be able to auto discover guest VMs and dynamically configure them for data backup.
16	The software solution must provide full support for Global Filter lists.
17	The offered software solution must support IPV4 and IPV6 addressing system.
18	The offered software solution must have capability to do trend analysis for capacity planning of backup environment.
19	The offered software must support heterogeneous media server agent failover.
20	All license to be quoted on capacity basis.
21	Bidder has to offer perpetual software license to meet following requirement of Railtel Data Center;
	ü **Application, database and Non-database files of 30 TB**
	o Application and database backup for Oracle, MS SQL, MySQL, DB2, Sybase, PostGreSQL, Share Point, SAP etc.
	o Backup features should include OS image (BMR), NDMP backup, VMWare host, Deduplication

Sr. No.	Backup - Minimum Requirement Description
	o Should support table level restoration
	o Should have support to replicate backed up data to secondary location
	o Non-database file include PDF, XLS, JPEG, MP4 and other similar flat files
	o Historical data to be archived based on user defined policy of age, file size, primary storage quota
	o Stub / shortcut of the archived files should be created on primary storage for user to get direct access
	o **Capacity license for Backup to be quoted**
	ü **Hadoop Backup for 40 TB**
	o Should support Hadoop backup with Hadoop Journal Integration
	o Should support Disk to Disk to Tape Backup
	o **Capacity license for Hadoop to be quoted**
22	Three year premium level 24x7 Annual Technical Support (ATS) for software license
23	The solution should have dual AC power supply fully populated (within box) from day one

5. Tape Library

Sr No.	Tape Library- Minimum Requirement Description
1	The tape library should include a bar-code reader to enable managing the inventory of tape cartridges.
2	Supply should include atleast 275 new LTO7 Data cartridges and 5 Head cleaning cartridges with Barcode labels
3	Library offered with minimum 275 Cartridge slots scalable up to 890 slots in a single library.
4	The tape library should have capability for hot plugging and hot swapping of tape drives, controller cards, power supply, cooling fans, other electronics, etc.
5	The tape library should have mixed media support and should be proposed along with necessary software/licenses
6	The tape library should have capability for automatic calibration of robotic arm.
7	Tape Library should be offered with minimum 4 LTO7 8Gbps Drive scalable to 24 drives in a same Tape library. Tenderer shall offer the Library with the suffiecient Rack Modules & Redundant power supply to scale up the Tape Drives without adding any further Modules at the time of increasing the Drives in the Library.
8	Support should include 3 years onsite warranty with 24 x 7 support with Next business Day (NBD) resolution.
9	Proposed Tape library should be supplied along with required rack mounting kit which should fit into standard 42U rack or should be 45U library frame size. Supply should include all the required cables/PDUs/equipment's necessary for making the system operational.
10	The tape library should have capability to backup data from multiple hosts running HP-UX, IBM AIX, MS Windows, Linux, SUN Solaris, etc.
11	Should provision native web-based remote management tool for remote administration.
12	Offered LTO7 Drives should be Full Height drives with DUAL FC ports for redundancy.
13	Offered drive should have native speed of at least 300 MB/sec and a compressed speed of at least 750 MB/sec for 2.5:1 compression.
14	Tape Library should support for partitioning so that each drive can be configured in a separate partition, and should be provided with initial capability upto 16 partitions
15	Tape Library should provide ENCRYPTION with built-in encryption key management. No external servers.
16	The Tape Library should be SMI-S/ (SNMP& SMTP) complaint.
17	Offered Tape library should have latest technology which enables least power consumption with peak operations
18	The Tenderer should provision adequate number of native full-duplex Fibre Channel ports on the tape library so as to stream data for full-utilization of all the tape drives and also ensuring the backup requirement indicated above.
19	The solution should have dual AC power supply fully populated (within box) from day one

6. DNS Security

Sr No.	DNS Security - Minimum Requirement Description
1	The Proposed Appliance should be able to handle 200K QPS for Non Authoritative and 20K QPS for Authoritative from Day One and should be scalable through software license upgrade to 400K QPS and 60K QPS respectively
2	The DNS shall support traffic steering like Load Balancing.
3	The offered solution shall be fully redundant with no single point of failure
4	IPv6 & Dual stack Compliant including all NAT requirements & DNSSEC
5	The GUI should provide both built-in functionality and mechanisms to integrate with external monitoring and alerting systems.
6	The system can be easily reverted to an earlier version of the software and data in the event that an upgrade has problems
7	The product must have a dedicated Management Port
8	System should must SSHv2 and SSL based administration
9	Support should include 3 years onsite warranty with 24 x 7 support with Next business Day (NBD) resolution.
10	The solution should have dual AC power supply fully populated (within box) from day one
11	Appliance hardware and software should be from the same OEM and should support role based access control
	DNS Functional Requirements
12	Each node must use a hardened operating system
13	The product support the ability to specify a custom list of root nameservers
14	The DNS component must support both types of query mechanism: Recursive and Iterative
15	The product should support Anycast for DNS with BGP and OSPF
16	Should support DNSv6 and DNS64
17	Should support NXDOMAIN redirection
18	Solution Should support DNSSEC
19	The DNS must support security features such as configuration of ACL (Access Control Lists)
20	The product must support the ability to control DNS logging
21	The solution must provide DNS statistics such as Successes, Failures, NXDomain responses, etc
22	The product should support the ability view DNS syslog messages.
23	The product should support a recent version of BIND 9
24	The DNS solutions should supports failover deployment and synchronize the configuration files and zone files to ensure that any update to the configuration will be populated between these servers.
25	DNS architecture should enable the DNS query load to be distributed across many locations for dynamic application delivery(User application requests and application services are distributed based on business policies, data center conditions, network conditions, and application performance)
26	Optimised memory management for caching server as per traffic load
27	Specific portions of the cache can be discarded without restarting the server

28	The DNS must provide appropriate automated failover and disaster recovery mechanisms
29	DNS resolution should continue even if the network is under attack
	DNS Security
30	Secure methods are used for data updates between the devices in the system.
31	The product must use a standard encrypted protocol between the GUI client
32	The system/solution should integrate with existing user data stores to authenticate administrators with standard protocols RADIUS, TACACS+ , LDAP
33	Should be able to secure the system Cache poisoning attacks.
34	Should be able to secure the system from DNS DOS/DDoS attacks.- LAND Attack
35	DNS Attack mitigation 1. DNS reflection Attacks 2. DNS Amplifications Attacks. 3. DNS Tunneling Attacks 4. DNS Based exploits 5. TCP/UDP/ICMP Floods 6. DNS Protocol Anamolies
	Resiliency
36	Solution should support of high-availability (HA)/DNS Anycast and port resiliency (NIC Failover) in each appliance / device / system .
37	The seamless recovery mechanisms in case of box, link or management failures, hardware failover and network failover mechanisms.
38	The product should have the ability to quickly revert to previous data and software versions in the event of upgrade issues?
39	The solution should support the configuration Back-up and restore mechanisms.
	Reporting
40	The DNS must have the capability to export logs produced to any 3rd party reporting and analytics used by the operator.
41	The DNS must provide real time reports on system Operation.
42	The DNS must be capable of generating reporting data.
43	The DNS must report statistics associated with hardware usage and capacity
44	DNS Replies Trend
45	DNS Cache Hit Rate Trend
46	DNS Statistics should include request per – § Application § Virtual server § Domain name § Query type § Client IP address
	DNS reports such as
47	DNS solution should generate atleast the following reports: a. DNS Cache hit b. Memory utilization trend c. Traffic rate trend d. DNS query rate by query type e. DNS query rate by server

	f. DNS ServFail error count
	g. DNS Top attacks types
	h. DNS top attack source
	i. CPU utilization trend
	j. DNS Query trend by domain name
	k. DNS query trend by source IP
	l. DNS traffic trend by malicious domain
	m. DNS protocol malformed/malicious traffic
	Logging, Alerting, Troubleshooting
48	The product should support sending logs via Syslog to external server
49	The product must allow configuration of severity of messages sent to each remote Syslog
50	The product must allow configuration of TCP or UDP for the Syslog transport mechanism
51	The product should support standard MIB/MIB-2 variables
52	The product automatically rotate log files
53	The solution must have option to configure DNS query and response logging for troubleshooting
	DNS Firewall
	DNS solution shall meet following firewall functionality:
	DNS DDoS mitigation
	DNS Protocol inspection and validation
	DNS record type ACL
	Block access to Malicious IPs
	High performance DNS cache
	Should support DNSSEC
	DNS DDoS threshold alerting
	DNS logging and reporting
54	Hardened DNS

7. EMS Solution

Sr. No.	EMS - Minimum Requirement Description
1	EMS architecture should be object oriented, open and extensible set of common services. These common services should offer a rich and comprehensive set of robust management functions such as event management, communications and administrative functions. The whole solution should work in an integrative fashion so that integrity issues and compatibility issues do not arise
2	Ability to integrate with various EMS tools to provide a consolidated dashboard
3	Should be modular and should not be framework dependent so that required modules can be added in future to meet the growing / changing needs
4	Ability to manage wired and wireless LANs from multiple vendors to cope up with the technology changes in the industry
5	Ability to support 3rd party integration and have open API/interfaces for integration
6	Ability to have an object repository based on open standard RDBMS
7	Ability to manage servers having OS such as AIX, HP-UX, Solaris, flavours of Linux, flavours of Windows, etc
8	Ability to manage popular databases such as Oracle, DB2, Sybase, MS-SQL, etc
9	Ability to deliver comprehensive, tightly integrated management capabilities, including performance and availability of database servers, application servers, web servers, other servers, desktop, network, storage, security, etc
10	Ability to correlate events across the spectrum of infrastructure components and should support events from components including Network, hardware, multiple-platform servers, database, etc
11	Ability to measure and manage service levels
12	Ability to support bandwidth throttling for the optimum use of network bandwidth for managing infrastructure
13	Ability to provide web based management consoles for managing the infrastructure and should use secured protocols for management of servers, desktops, etc
14	Ability to support multiple levels of administrative delegation. It should be able to define multiple levels of administrative domains so that each administrator is assigned certain resources for which they are responsible. It should provide for database scoping to protect management database data from unauthorized access
15	Communication between managed server and the target managed system across the network should be secured, reliable and using widely accepted standards such as SNMP, TCP/IP and UDP
16	Ability of quickly identifying the impact of infrastructure failures, identify the root cause of the problem and manage IT infrastructure. It should prevent flooding of non-relevant console messages
17	Ability to provide management of all systems using intelligent single agent technology
18	Should have a very lightweight agent component that consumes very less system resources like memory, disk space, etc.
19	The agent component should be supported on leading OS like HP-UX, AIX, Solaris, Linux, flavours of Windows, etc.
20	Ability to provide configuration utility, which would allow for centralized management of configuration of remote agents on managed objects if required
21	Ability to provide an event console for the entire environment for event monitoring. Events should be colour coded on the GUI based on severity

Sr. No.	EMS - Minimum Requirement Description
22	Ability to provide an event correlation engine, which should be rules based and work in conjunction with event management
23	Ability to act on events either in an automatic mode or operator initiated response mode
24	Ability to capture all events that are being generated across the complete IT infrastructure, correlate them and automate initiation of suitable corrective action as defined
25	Ability to generate web based real-time reporting and historical reporting of elements in the infrastructure, providing the ability to format and present data in a graphical and tabular display
26	Ability of integrating events to automatically create trouble tickets in helpdesk system for in-time problem resolution. It should provide filters that enable specified user groups to receive event notifications via various methods such as e-mail, pop-up messages, banners, SMS, etc
27	Ability to provide display of infrastructure as per various groups such as location wise, device type wise, servers type etc to provide more meaningful type of display to the operator depending on their roles
28	Ability to diagnose performance problems using recent and historical data and help in taking corrective measures before user service quality goes down
	Database Monitoring Requirement
29	Ability to proactively monitor various critical RDBMS parameters such as database tables, tablespaces, logs, file store space, system resource utilization, locking system,etc. using agents on the servers to be monitored
30	Ability to integrate with EMS and support monitoring of various RDBMS like Oracle, MS-SQL, DB2, Sybase, etc
31	Ability to configure the database monitoring agents to monitor based on thresholds. When thresholds are exceeded, the agents should be able to send alerts to event console of EMS
32	Facility for Database Administrators such that they should be able to set thresholds for key performance indicators based upon their observations of declining performance. The database management function should be able to enforce sophisticated policies that monitor and correlate multiple events
33	Ability to monitor various database parameters depending on the database being monitored yet offer a similar interface for viewing the agents and setting thresholds
34	Ability to monitor all server databases as well as configuration information and store it in the object repository
35	Ability to monitor the status of database server processes. In conjunction with EMS, it should be able to restart critical processes when they shut down
36	Ability to monitor short-term and long-term CPU utilization to ensure database server does not place unacceptable loads on the host. To avoid unnecessary warning when CPU utilization momentarily exceeds thresholds, the function should send an alert only when the database server is placing a sustained load on the machine.
37	Ability to monitor the caching system to assess the effectiveness of the cache size
38	Ability to continuously monitor the number of available locks to avoid a situation where the locking system blocks transactions.
39	Ability to automate day-to-day DBA tasks while enabling control across multiple environments
40	Ability to deliver a complete set of tools for performance analysis of database
41	Inclusion of SQL statements within the Solution should be a standard “easy-to-use” function.
42	The solution must monitor for Blocking (exceeding duration) and Deadlocks

Sr. No.	EMS - Minimum Requirement Description
43	The solution must be able to report & check for last recent Full database backup and last recent Transaction Log backup
44	The solution may support monitoring of Replication, DB Mirroring and Log shipping if applicable
45	The solution should support auto-discovery of database instances.
	Virtualization Monitoring Requirement
46	The solution should provide support for leading virtualization platforms.
47	The solution should support monitoring of virtualized environment through management interface like vsphere or through hypervisor
48	The solution should provide capability to monitor events generated by the hypervisor to generate alarms and alerting functionality
49	The solution should provide capability to create monitoring template and auto configure any newly detected virtual machine.
50	The solution should provide a configurable interface to view performance metrics related to virtualization infrastructure
51	The solution should provide capability to monitor the availability to Web API's of application.
52	The proposed solution should be integrated with centralised monitoring tool to enable aggregation of alarms and alerts.
53	The proposed solution should allow reporting through unified reporting console along with other infrastructure devices being monitored.
	SLA Monitoring Specifications
54	Ability to provide full-fledged service level monitoring and reporting capability using which administrator should be able to define metrics to be measured, measure on such metrics and do comprehensive service monitoring and web-based reporting based on service availability, downtime and response
55	Ability to integrate with other modules of EMS to provide service level reporting and be able to generate service level reports based on customized business process views if required.
56	Ability to generate and publish service level reports. Should allow users to access or generate reports via web as per their roles & responsibilities.
57	Ability to define service incidents, identifying periods in which data is invalid for specific data collections. Ability to ignore collected data which is not to be included in the report generation
58	Alerts should be available when SLA is violated along with the root cause of the problem.
59	Facility to send potential breaches of SLAs to the event management console of EMS (e.g. sending notifications based on availability measurements of web servers, etc.)
60	Ability to present results relative to previously defined service goals and as deviation reports, which includes only results that exceed previously defined service goals
61	Ability to monitor and report on availability, utilization and also provide reports on historical utilization of CPU, memory of monitored servers running EMS agents
62	Facility of a Report Configuration tool, which can be used to tailor reports to view data collected within intervals of interest only such as business hours, days or weeks. The user should be able to filter reports to show the level of details to suit job function or interest.
63	Ability to automatically generate service reports and should have capability to upload the reports automatically to a remote web server
64	Facility for Users such that they should be able to monitor service level incidents to indicate what factors affect non-compliance. It should also highlight periods when the external factors such as power outages are responsible for non-compliance with SLA

Sr. No.	EMS - Minimum Requirement Description
65	Should be scalable and support data collectors distributed across locations, should be able to gather and measure statistics from the IT infrastructure. Distributed data collection and measurement architecture should be available that makes the offering a scalable solution regardless of size
	Helpdesk Management
66	The proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident manually via web and console interface.
67	The proposed helpdesk solution must be able to provide flexibility of incident assignment based on the workload, category, location etc.
68	Each escalation policy must allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no programming.
69	The escalation policy would allow flexibility of associating with different criteria like device/asset/system, category of incident, priority level, organization and contact.
70	The proposed helpdesk solution must provide web-based knowledge database to store useful history incident resolution
71	Ability to provide flexible logging of incidents / queries manually via GUI and web interface. Should provide various ways to create incidents / queries and not limited to email
72	The web interface console of the incident / query tracking system should allow viewing, updating and closing of tickets
73	Facility to link calls/ incidents / queries in case the same is reported more than once
74	Ability of the web interface console to offer tips to the users.
75	Ability to define multiple levels / tiers of categorization on the type of incidents / queries being logged
76	Facility for classification to differentiate the criticality of the incident / query via the priority levels, severity levels and impact levels
77	Ability to provide audit logs and reports to track the updating of each ticket
78	Ability to allow easy definition of multiple escalation levels and notification to different personnel for escalation policy.
79	The escalation policy should allow flexibility of associating with different criteria like device / asset / system, category of incident, priority level etc
80	Ability to have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues
81	Ability to store detail asset information on hardware and software inventory
82	Ability to support tracking of SLA for call requests within the help desk through service types
83	Ability to provide status of registered queries to end-users over email and other means
84	Ability of assigning query requests to technical staff manually as well as automatically based on predefined rules and should support notification and escalation over email, web, etc.
85	Ability to provide integration with desktop management suite of products.
86	The proposed helpdesk solution must have a strong Business Objects based reporting module built in it.
87	The proposed helpdesk solution must have an updateable knowledge base for technical analysis and further help endusers to search solutions for previously solved issues.
88	The proposed helpdesk solution must support request management, problem management, configuration management and change order management.

Sr. No.	EMS - Minimum Requirement Description
89	The proposed helpdesk solution must have an integrated CMDB for better configuration management & change management process. CMDB should have be able to scale as per the requirements of the project for creation of CI families, CI Classes and CI Relationship Types out of the box. Both helpdesk &
90	CMDB should have same login window for seamless access.
91	The proposed helpdesk solution must have a top management dashboard for viewing the helpdesk KPI in graph & chart formats.
	Server Management
92	Ability to monitor various OS parameters such as processors, memory, files, processes, file systems, etc., using agents on the servers to be monitored.
93	Ability to configure the OS monitoring agents to monitor based on user-defined thresholds for warning / critical states and escalate events to event console of EMS
94	Ability to integrate with EMS and support OS monitoring for various platforms - various flavours of Unix, Linux, Windows, etc
95	Ability to monitor various OS parameters depending on the OS being monitored yet offer a similar interface for viewing the agents and setting thresholds
96	Ability to provide performance scoping and trending to provide real time as well as historical reporting
97	Ability to provide performance configuration to enable agent configuration to be done from a central point of control using intuitive GUIs that provide a common look and feel across various platforms. Performance profiles could be defined in this GUI and using drag-and-drop techniques, delivered to the various specified machines in the enterprise running performance agents. These agents could then dynamically reconfigure them to use the profiles they receive
98	Historical performance agent would be responsible for long term data collection and data management. It should collect historical performance data for a wide range of resources on supported platforms such as Windows, Linux, Unix, etc. The collected data should be available for the purpose of detailed trend analysis and capacity planning if required
99	Ability to support management of following parameters
100	**Processors** - Each processor in the system should be monitored for CPU utilization. It should compare current utilization against user-specified warning and critical thresholds
101	**File Systems -** Each file system should be monitored for the amount of file system space used
102	**Files -** File attributes such as overall file size, time-stamp change and file growth between intervals should be monitored
103	**Log Files -** Logs should be monitored to detect faults in the OS, the communication subsystem, and in applications. System agents should also analyze log files residing on the host for specified string patterns
104	**System Processes -** System agents should provide real-time collection of data from all system processes. Using this it should help identify whether or not an important process has stopped unexpectedly. It should provide an ability to automatically restart critical processes
105	**Memory -** System agents should monitor memory utilization and available swap space and should raise an alarm in event of threshold violation
106	**Event Log -** User-defined events in the security, system and application event logs should be monitored. E.g. an event-log watcher can be configured to identify the occurrence of failed logon attempts, indicating that someone may be attempting to violate a sensitive system

Sr. No.	EMS - Minimum Requirement Description
107	System agents for Windows should provide functionality to monitor logical volumes, mounts, distributed file systems, quotas, directories, services, jobs, sessions and network interfaces
108	System agents for Unix and Linux should provide functionality to monitor swap space, load averages, network interfaces, inter-process communication, physical disks, message queues, semaphores, shared memory segments and other kernel parameters
109	The event generated as a part of server management should go to a common enterprise event console where a set of automated tasks can be defined based on the policy
	Asset Management
110	Ability to have reporting capabilities; provide predefined reports and ability to create customized reports on data in the inventory database. Report results could be displayed as lists or graphs
111	Ability to provide facility to recognize custom applications on desktops
112	Facility for the administrator to register a new application to the detectable application list using certain identification criteria. Should enable the new application to be detected automatically next time the inventory is scanned
113	Ability to support configuration management functionality using which standardization of configuration can be achieved of all the desktops
114	Software metering should be supported to audit and control software usage. Should support offline and online metering.
115	Ability to support dynamic grouping of enabling assets to be grouped dynamically based on some pre-defined criteria e.g. a group should be able to display how many and which computers has a specific application installed. As and when a new computer gets the new application installed it should dynamically add to the group
116	Ability to use the query tool to identify specific instances of concern like policy violation (presence of prohibited programs / games and old versions,etc.), inventory changes (memory change, etc) and accordingly it could perform several actions as reply. These actions could be (a) sending a mail, (b) writing to files, sound an alarm (c) message to scroll on monitor screen if the administrator, etc
117	Facility to track changes by maintaining history of an asset
118	Ability to have web based console
119	Facility to support event policies such that predefined actions can be triggered , such as sending an email notification, when key events occur such as software license violations, etc
120	Ability to provide inventory of hardware and software applications on end-user desktops including information on processor, memory, OS, mouse, keyboard, etc. through agents installed on them
121	Ability to send queries to an engine (to pump the inventory information to the console) to be executed at predefined days and time
	Network Management System
122	The Proposed Network Fault Management consoles must provide web based topology map view from a single central console. The system should provide Auto Discovery & inventory of heterogeneous physical SNMP enabled network devices like Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.
123	Network Fault Management should support Graphical User Interface (GUI).
124	The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time to keep the topology as up to date as possible. This discovery should run at a low overhead, incrementally discovering devices and interfaces.

Sr. No.	EMS - Minimum Requirement Description
125	The NMS should provide very powerful event correlation engine and thus must filter, correlate & process, the events that are created daily from network devices. It should assist in root cause determination and help prevent flooding of non-relevant console messages.
126	Ability to integrate with EMS and be able to provide monitoring of the available network.
127	Should be based on SNMP and TCP/IP standard and permit network layer level management. Should utilize management standards like SNMP, RMON, etc. to monitor and manage the network. Standard network protocols like TCP/IP should be fully supported
128	Ability to monitor network devices of various vendors and should be easily accessible through a common interface
129	Ability to provide traffic / percentage utilization, error statistics, etc. through various reports based on the environment monitored
130	Ability to provide various maps of topology with drill down capability to quickly arrive at a root cause of a problem
	Other
131	Network Monitoring of altleast 50 devices
132	Database Monitoring of atleast 10 database
133	Atleast 250 servers
134	Service Management having 5 concurrent users
135	Monitoring of 10 application

8. UTM Solution

Sr. No.	UTM - Minimum Requirement Description
1	The UTM should be Hardware based and enterprise class (complete control from GUI as well as CLI)
2	UTM appliance should have at least 04 x 10/100/1000 GE RJ45 ports and 2 x 1GE SFP+ ports with fully populated (SFP+ transceivers) from day one
3	UTM appliance must have separate SYNC and management ports other than the above mentioned ports
4	Firewall should provide at least 8 Gbps of real world/ production envoirnment throughput
5	IPS throughput should be atleast 1 Gbps or better for real world/production throughput
6	UTM appliance should have at least 8 GB RAM
7	UTM appliance should have a on device storage of min 100GB to be able to hold multiple OS images, logs, backups etc
8	Firewall should support 120,000 new sessions per second
9	Firewall should support 5 Million concurrent sessions
10	The UTM appliance should be Rack Mountable, not exceeding 1U.
11	The Firewall solution should support NAT64, DNS64 & DHCPv6
12	Firewall should operate in Route mode and transparent mode
13	The appliance should support Link aggregation (IEEE 802.3ad) technology to group multiple physical links into a single logical link of higher bandwidth and link fail over capability
14	The proposed system should have integrated Traffic Shaping functionality.
15	Support at least 10 firewall domains/instants/context
16	Certified by ICSA 4.1x OR EAL4 OR NDPP
17	Internationally accepted marked/Certified like RoHS, UL/CUL, FCC,CE,..etc.
18	The system should inherit all the standard RFC's.
19	Firewall should be either IPv6 Ready Logo certified or equivalent
20	Should facilitate to apply policy like IPS, Content filtering, Traffic shaping & policy based routing decision
21	User authentication facilitated by services like LDAP and RADIUS.
22	Management over GUI using HTTPS or equivalent secure mechanism, SSH and console access.
23	Management access control using Profile/Role based for granular control.
24	Configuration backup and restore on to/from a remote system via GUI/CLI over HTTP/SSH/TFTP or equivalent.
25	Support configurable option for E-mail or SMS alerts (Via SMS gateway) incase of any event trigger.
26	Firmware/OS/software updates via Web UI / TFTP or equivalent and should support version roll back functionality.
27	All SNMP versions support (v1, v2c and v3).
28	Support IEEE 802.1q (VLAN Tagging) and VLANs on all interfaces with at least 1024 VLANs
29	Dynamic Routing (RIPv2, OSPF, OSPFv3, BGP4, RIPng), Static Route, Policy Based Routing, Multicast Routing
30	Support DHCP server, DHCP client, DHCP relay, DNS clientand NTP client
31	Support NAT (SNAT and DNAT) with following modes Static, Dynamic, PAT and IPv6 to IPv4 (vice versa).

	Intrusion Prevention System
32	The IPS capability should have NSS, ICSA or other equivalent Certification
33	IPS throughput should be atleast 1 Gbps or better for real world/production throughput
34	The IPS detection methodologies should consist of:
35	a) Signature based detection using real time updated database
36	b) Anomaly based detection that is based on thresholds
37	The IPS should be able to inspect SSL sessions by decrypting the traffic
38	The IPS system should have at least 7,000 signatures with support for custom IPS signatures
39	IPS Signatures should be updated in different ways: manually, via pull or push technology. Administrator should schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available
40	IPS signatures should have a configurable actions like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending an alert and logging the incident
41	Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)
42	Solution should be able to detect & Prevent the Bot communication with C&C
	Web Content Filtering & Application Control Features:
43	Support web content filtering up to layer 7 traffic like HTTP, HTTPS, FTP, DNS, SMTP, IMAP, POP3 etc., with Application identification like IM, torrent etc., Allow/Deny traffic based on Src / Dst IP / Networks, Web URLs, Regular expressions, Web plug-ins such as ActiveX , Java Applet & Cookies, Regular file extensions, Spy wares and Ad wares
44	URL database should have at least 200 million+ sites and 50 + categories.
45	Manually defined web filtering based on URL, web content and MIME header
46	Support for geographical based filtering like country level TLD etc.
47	The appliance should have 3000 or more application signatures database
48	Should have the intelligence to identify & control of popular IM & P2P applications like KaZaa, Bit Torrent, Skype, You Tube, Facebook, LinkedIn etc.
	User Authentication
49	The proposed solution shall be able to support various form of user Authentication methods simultaneously , including:
	a) Local Database entries
	b) LDAP server entries
	c) RADIUS server entries
	d) Native Windows AD (Single sign on capability)
50	Firewall should support the system authentication with RADIUS and local authentication. Both should work simultaneously.
	High Availability
51	System should have built-in high availability (HA) features without extra cost/license or hardware component from day one
52	Should support state full session maintenance in the event of a fail-over to a standby unit.
53	High Availability feature must be supported for either NAT/Route or Transparent mode
54	High Availability Configurations should support Active/Active, Active/ Passive & Clustering
	Management, Logging and Reporting

55	The management solution must offer console capability for managing the logs, policy, reporting and various features of the UTM.
56	Logging and Reporting up to layer 7 traffic details (firewall policy level, denied traffic details etc.)
57	Should provide log report in Web/GUI /dashboard based format with detailed information categorized by IP/Application/Port/Protocol etc., able to forward logsto syslog server and sending schedule reports and send via email.
	Anti-virus, Anti-bot & Advance Persistence Threat Solution
58	Should provide protection against viruses, worms or any other malicious content in traffic like SMTP, SMTPs, POP3, POP3s, IMAP, IMAPs, HTTP, HTTPs, FTP, FTPs etc. and must be configurable/applicable on specific firewall Policy
59	Should be able to scan the file either on the basis of flow or buffering.
60	Should have option to respond to virus detection in several ways like delete/quarantine the file and send notification via e-mail/SMS.
61	The antivirus signature database of proposed solution should comprise of up to date list of signatures of virus, malwares, spyware etc.
62	Should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.
63	Firewall must include Anti-bot capability using IP reputation DB, terminates botnet communication to C&C servers also.
	Support and Warranty
66	Comprehensive onsite hardware warranty for 3 years with Next business Day (NBD) resolution.
67	Online upgrade the version of firmware/software/patches as and when required.
68	Telephonic support with call logging mechanism should be provided on 24x7x365 basis.
69	Provide confirmation letter for license (if any) subscription for 3 years. License applicable from day one.
70	All the technical specifications mentioned above must be available from day one
	Other Requirements
72	For all requirements listed above, the necessary cables, connectors, external software media, manuals or anyother hardware and software must be provided along
73	The solution must be present as Leaders in Gartner's Magic Quadrant for 2016/2017 and have atleast 90% in the NSS NGFW security effectiveness value.

9. Next-Gen Firewall (NGFW)

Sr. No.	NGFW - Minimum Requirement Description
1	The solution should be Hardware based and enterprise class (complete control from GUI as well as CLI)
2	the solution appliance should have at least 4 GE ports and 4 x 10G SFP+ ports with fully populated (SFP+ transceivers) from day one
3	The solution appliance must have separate SYNC and management ports other than the above mentioned ports
4	Firewall should provide at least 20 Gbps of real world/ production envoirnment throughput
6	The solution appliance should have at least 16 GB RAM
7	The solution appliance should have a on device storage of min 200GB to be able to hold multiple OS images, logs, backups etc
8	Firewall should support 180,000 new sessions per second
9	Firewall should support 10 Million concurrent sessions
10	Rack Mountable not exceeding 2U with redundant/dual AC power supply fully populated (within box) from day one
11	The Firewall solution should support NAT64, DNS64 & DHCPv6
12	Firewall should operate in Route mode and transparent mode
13	The appliance should support Link aggregation (IEEE 802.3ad) technology to group multiple physical links into a single logical link of higher bandwidth and link fail over capability
14	The proposed system should have integrated Traffic Shaping functionality.
15	Support at least 10 firewall domains/instants/virtual context
16	Certified by ICSA 4.1x OR EAL4 OR NDPP
17	Internationally accepted marked/Certified like RoHS, UL/CUL, FCC,CE,..etc.
18	The system should inherit all the standard RFC's.
19	Firewall should be either IPv6 Ready Logo certified or equivalent
20	Should facilitate to apply policy like Traffic shaping & policy based routing decision
21	User authentication facilitated by services like LDAP and RADIUS.
22	Management over GUI using HTTPS or equivalent secure mechanism, SSH and console access.
23	Management access control using Profile/Role based for granular control.
24	Configuration backup and restore on to/from a remote system via GUI/CLI over HTTP/SSH/TFTP or equivalent.
25	Support configurable option for E-mail or SMS alerts (Via SMS gateway) incase of any event trigger.
26	Firmware/OS/software updates via Web UI / TFTP or equivalent and should support version roll back functionality.
27	All SNMP versions support (v1, v2c and v3).
28	Support IEEE 802.1q (VLAN Tagging) and VLANs on all interfaces with at least 1024 VLANs
29	Dynamic Routing (RIPv2, OSPF, OSPFv3, BGP4, RIPng), Static Route, Policy Based Routing, Multicast Routing
30	Support DHCP server, DHCP client, DHCP relay, DNS client and NTP client

31	Support NAT (SNAT and DNAT) with following modes Static, Dynamic, PAT and IPv6 to IPv4 (vice versa).
32	The appliance based security platform should be capable of providing firewall and VPN (both IPSec and SSL) functionality in a single appliance
33	NGFW should support SSL VPN throughput of atleast 3Gbps
34	Firewall should support client based and clientless SSL vpn peers from day one.
35	Should support Nat-T for IPSec VPN
	Intrusion Prevention System
36	The IPS capability should have NSS, ICSA or other equivalent Certification
37	IPS throughput should be atleast 3 Gbps or better for real world/production throughput
38	The IPS detection methodologies should consist of:
39	a) Signature based detection using real time updated database
40	b) Anomaly based detection that is based on thresholds
41	The IPS should be able to inspect SSL sessions by decrypting the traffic
42	The IPS system should have at least 7,000 signatures with support for custom IPS signatures
43	IPS Signatures should be updated in different ways: manually, via pull or push technology. Administrator should schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available
44	IPS signatures should have a configurable actions like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending an alert and logging the incident
45	Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)
	User Authentication
46	The proposed solution shall be able to support various form of user Authentication methods simultaneously , including:
	a) Local Database entries
	b) LDAP server entries
	c) RADIUS server entries
	d) Native Windows AD (Single sign on capability)
47	Firewall should support the system authentication with RADIUS and local authentication. Both should work simultaneously.
	High Availability
48	System should have built-in high availability (HA) features without extra cost/license or hardware component from day one
49	Should support state full session maintenance in the event of a fail-over to a standby unit.
50	High Availability feature must be supported for either NAT/Route or Transparent mode
51	High Availability Configurations should support Active/Active or Active/ Passive & Clustering
	Management, Logging and Reporting

52	The management solution must offer console capability for managing the logs, policy, reporting and various features of the The solution.
53	Logging and Reporting up to layer 7 traffic details (firewall policy level, denied traffic details etc.)
54	Should provide log report in Web/GUI /dashboard based format with detailed information categorized by IP/Application/Port/Protocol etc., able to forward logsto syslog server and sending schedule reports and send via email.
	Support and Warranty
55	Comprehensive onsite hardware warranty for 3 years with Next business Day (NBD) resolution.
56	Online upgrade the version of firmware/software/patches as and when required.
57	Telephonic support with call logging mechanism should be provided on 24x7x365 basis.
58	Provide confirmation letter for license (if any) subscription for 3 years. License applicable from day one.
59	All the technical specifications mentioned above must be available from day one
	Other Requirements
60	For all requirements listed above, the necessary cables, connectors, external software media, manuals or anyother hardware and software must be provided along
61	The solution must be present as Leaders or Challengers in Gartner's Enterprise Firewall Magic Quadrant for 2016/2017.

10. Intrusion Prevention System (IPS)

Sr. No.	IPS - Minimum Requirement Description
1	The IPS capability should have NSS / ICSA or other equivalent Certification
2	The IPS should be a dedicated purpose built hardware, not a part of Router, Firewall module and UTM solution with Real World Throughput 6 Gbps or better
3	The IPS detection methodologies should consist of:
	a) Signature based detection using real time updated database
	b) Anomaly based detection that is based on thresholds
4	The IPS system should have at least 4,500 signatures with support for custom IPS signatures
5	IPS Signatures should be updated in different ways: manually, via pull or push technology. Administrator should schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available All the signatures update subsrciption should be provided from Day1
6	IPS signatures should have a configurable actions like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending an alert and logging the incident
7	Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)
8	Solution should be able to detect & Prevent the Bot communication with C&C
9	The IPS should have deployable capability in the Passive or IDS mode, Inline Protection or Inline Simulation mode.
10	The IPS should be able to detect and block all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability).
11	The IPS should be capable of detecting and blocking zero-day attacks without requiring an update.
12	The IPS should employ full seven-layer protocol analysis of over maximum internet protocols and data file format.
13	The IPS should detect attacks inside IPv6 encapsulated packets
14	IPS device should perform stateful pattern recognition to identify vulnerability-based attacks through the use of multi-packet inspection across all protocols.
15	The proposed IPS must perform protocol decoding and validation for network traffic including: IP, TCP, UDP, and ICMP.
16	IPS should provide anomaly identification for attacks that may cover multiple sessions and connections, using techniques based on identifying changes in normal network traffic patterns.
17	Proposed IPS should identify attacks based on observed deviations in the normal RFC behaviour of a protocol or service.
18	Proposed IPS should have the options of policy configuration, event management, health management and reporting.
19	IPS device should have features to prioritize and send alerts to users after an alert action is taken place
20	The proposed device should support High Availability (Active-Passive). The inspected throughput of the appliance should not degrade in the High Availability mode deployment
	Support and Warranty
21	Comprehensive onsite hardware warranty for 3 years with Next business Day (NBD) resolution.
22	Online upgrade the version of firmware/software/patches as and when required.

23	Telephonic support with call logging mechanism should be provided on 24x7x365 basis.
24	Provide confirmation letter for license (if any) subscription for 3 years. License applicable from day one.
	All the technical specifications mentioned above must be available from day one
	Other Requirements
25	For all requirements listed above, the necessary cables, connectors, external software media, manuals or anyother hardware and software must be provided along
26	OEM should be present in Gartner's LEADER magic quadrant in the report (2016/2017) for IPS OR EAL4+ OR NDPP certified and should have OEM TAC based in INDIA.
27	the solution appliance should have at least 4 x 10G SFP+/XFP ports (fully populated) from day one
28	The solution should have dual AC power supply fully populated (within box) from day one

11. APT Solution

Sr. No.	APT - Minimum Requirement Description
1	The solution should be able to communicate birectionally with the proposed UTM and NGFW solution for automatic blocking/threat update
2	The solution must employ an on premise (not on cloud) analysis engine using virtual execution to detect zero day and unknown threats and must not be signature based.
3	The proposed solution should be able to detect and prevent advanced Malware, Zero-day attack, spear phishing attack, drive by download, watering hole and targeted Advanced Persistent Threat without relying on just Signature database.
4	The proposed solution should perform dynamic real-time analysis of advanced malware on the appliance itself to confirm true zero-day and targeted attacks. No information should be sent to third party systems or cloud infrastructure system for analysis and detection of Malware.
5	The proposed solution should automatically detect and confirm multistage zeroday malware and targeted attacks without prior knowledge of the malware.
6	The proposed solution should utilize a state-full attack analysis to detect the entire infection lifecycle, and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.
7	The proposed solution should analyze advanced malware against a cross-matrix of different operating systems and various versions of pre-defined applications.
8	The solution must support pre-populated Licensed copies of Operating systems and applications/softwares (like Microsoft Office). There should be no requirement for the customer to buy additional licesnse.
9	The system should be able to support file sizes upto 50 mb or more
10	The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents (doc, docx, xls etc), common multimedia contents like JPEG, GIF and ZIP/RAR/7ZIP/TNEF archives, to prevent advanced Malware and Zero-day attacks.
11	The proposed solution should capture and store packet captures of traffic relevant to the analysis of detected threats.
12	The proposed solution should have the ability to display the geo-location of the remote command and control server(s) when possible.
13	The proposed solution should have the ability to report the Source IP, Destination IP, C&C Servers, URL, BOT name, Malware class, executable run, used protocols and infection severity of the attack.
14	The proposed solution should be able to send both summary notifications and detailed per-event notifications utilizing the protocols (SMTP, SNMP, or HTTP POST).
15	The proposed solution should have the ability to be deployed in out-of-band mode (also SPAN/TAP) & inline mode
16	The proposed solution should be capable to block inbound malicious exploits delivered via a web channel and outbound call-back communications when deployed in inline, or out-of-band mode.
17	The proposed solution should have the ability to scan and analyze emails to identify malicious attachments or URLs.
18	The proposed solution should be able to scan servers that support CIFS and NFS protocol for sharing and transferring files.

19	The proposed solution should provide visibility into scan histories of each file scanned that are aborted, completed, or in progress.
20	The solution should provide reports in (but not limited to) PDF/CSV formats.
21	The solution should have anti-evasion capabilities to prevent malwares detection of being run/executed in the vitualized environment.
22	The proposed solution should be able to analyze saved email (.eml) files for malicious attachments.
23	The solution should support for SIEM log integration.
24	The solution should be able to schedule reports and also provide the flexibility to generate on-demand reports like daily/weekly/monthly/ yearly/specific range (day and time) etc.
25	Minimum number of Interfaces - 2x GE & 2 x 10G
26	Number of VM's should be atleast 24
27	It should support Sandbox Analysis for multiple operating systems like WinXP,Win7,Win8,Win10
28	The APT appliance should be able to process minimum of 1000 files/hour or 1,000,000 files/month (either web or mail or both) on the VM sandboxing
29	High Availability & Maximum Scalability
30	Proposed solution must have secured at least 95% security effective-ness in latest NSS Breach Detection System Report
31	The solution should have dual AC power supply fully populated (within box) from day one

12.Web Application Black Box Scanner

Sr.No	Features Description
Vulnerability check	
1	Cross Site Scripting – Product should tests for vulnerabilities of this class
2	Buffer Overflow/Overruns – Product should identify vulnerabilities of this class
3	SQL Injection – Product should tests for vulnerabilities of this class
4	Cookie Poisoning – Product should identify any vulnerabilities of this class
5	Hidden Field Manipulation – Product should identify if hidden field manipulation is possible
6	HTTP Response Splitting – Product should check to determine that proper input handling exists and notify it HTTP Response Splitting is possible
7	Data Sanitization – Product should check for command character escaping and user input encoding
8	User Passwords – Product should check to determine that sensitive data/PII or higher data classification is sent over secure channels only
9	Access Control – Product should check to determine that proper access controls are in place
10	Authentication and Session Management – Product should check to determine that proper authentication is in place and that session integrity is not compromised
11	Privilege Escalation Testing - Product should check to determine if unauthorized users can gain access restricted resources
12	Configuration Management – Product should check to determine that configuration management is secure (i.e., extra verbs not present, config files not writeable, sample sites present, etc.)
13	3rd Party Misconfiguration – Product should check to determine that all 3rd party applications are properly configured to prevent any known vulnerabilities from being exploited
14	Format String Command Execution - Product should check to determine that it is not possible to execute remote commands on the web server through malicious input
15	Cross Site Request Forgery - Product should check to determine if it's possible to perform an action on the vulnerabile site on behalf of the legitimate user.
16	Flash Based Vulnerabilities - Product should check for flash based vulnerabilites such as Cross-Site Flashing, Cross-Site Scripting through Flash, Phishing through Flash
Testing Abilities	
17	JavaScript Parsing – Product should be able to parse JavaScript code
18	JavaScript Execution – Product should be able to execute JavaScript code to determine if any vulnerabilities are present
19	Flash Parsing – Product should parse flash to allow it to extract embedded URL's
20	Flash Execution - Product should be able to play Flash files to discover potential vulnerabilites
21	Web Services – Product should perform web services application scans, includes SOAP version 1.2 coverage
22	Web Services - Product should support web services scan that needs support for MIME attachments, WS encryption, WS signature
23	Error Handling – Product should check to determine if proper error handling is in place and that no errors give explicit information about the application or system
24	Web Forms Tampering – Product should have the ability to tamper with existing form values to test for vulnerabilities

25	Parameter/Cookie Exclusion - Product should be able to exclude certain cookies and parameters from being tested
26	Port Listener Tests - Product should allow highly sophisticated tests that attempt exploit the application ant establish a connection back to the scanning server, giving 100% certainty of a high risk vulnerability
27	Smart Increment/Decrement Number Parameter Testing - Product should attempt to increment and decrement each numeric value to break the logic flaw of the application
28	Smart Out-of-Range Selection Parameters - Product should attempt to use an out-of-range parameter (e.g., long integer instead of an integer) to understand the application handling
29	Adaptive Smart Testing - application understands and alters the existing parameter to uncover new vulnerabilities
30	Multi-phase Testing - Product should allow the user to automatically re-test the application for new areas found during the prior testing phase
31	Pattern Search Testing - Product should allow users to define specific tests from customized regular expressions
32	Product should provide ability to "re-test" a specific or all vulnerabilities
33	Product should provide ability to clear session identifiers before testing login pages
34	Product should provide the ability to parse URL-based session identifiers
35	Product should provide ability to define if login/logout pages should be tested or not
36	Product should provide ability to test JSON protocol parameters in AJAX-based applications
37	Product should provide SQL injection exploit tool to demonstrate how a SQL injection vulnerability in a web application can be exploited to retrieve database information such as usernames, passwords, credit card numbers, etc.
38	Product should able to handle gzip encoded responses
39	Product should Support Web 2.0, JavaScript Frameworks and AJAX frameworks
40	Product should be able to support customizing parameters and redundancy tuning through regular expressions in order to understand custom logic and parameter handling
Explore Options	
41	Product should perform automatic crawling
42	Product should perform manual browsing
43	Product should manually record login
44	Product should provide the ability to handle complex authentication mechanisms and maintain session state
45	Product should perform case-sensitive/insensitive crawling
46	Product should perform multi-phase (recursive) crawling
47	Product should support exploring with an external browser like IE,Mozilla FF & Chrome
48	Product should provide ability to customize the scan by disabling/enabling certain tests or groups of tests
49	Product should provide the ability to include or exclude designated web applications
50	Product should provide default test policies and provide the ability to define custom policies including selection of tests and variants by type, severity or WASC classification
51	Product should provide ability to create user defined tests (add a parameter, modify user input, modify path in request)
52	Product should provide ability to select either depth-first or breath-first crawling
53	Product should support AJAX, JS Frameworks (Dojo,ICEFaces etc.)
54	Product should able to support full dynamic exploration of Flash based applications
55	Product should supports HTTP 1.0 and 1.1 applications
56	Product should disable simultaneous logins on applications that do not allow this
57	Product should automatically is able to determine the correct login sequence required

58	Product should allow for the automatic filling of forms
59	Product should provide ability to export /import form fill values
60	Product should allow the user to specify a particular SessionID that might change in the explore phase of the analysis
61	Product should provide ability to "re-test" without starting a completely new scan
62	Product should provide ability to record/import explore data only
63	Product should support basic, NTLM, Kerberos, Digest and Forms-based authentication
Reporting	
64	Product should reports against all WASC categories
65	Product should provide ability to save reports to HTML/PDF/WORD
66	Product should provide ability to store and report on full requests and responses
67	Product should provide the ability to compare and report on two different scans to enable a delta analysis
68	Product should be able to generate out-of-the-box compliance and industry standards reports
69	Product should include latest update to PCI Data Security Standard (v1.1) compliance report
70	Product should can generate all compliance reports from a single scan
71	Product should report include embedded screen shots of issues
72	Product should report list all successful test variants but only count them as one vulnerability
73	Product should provide ability to divide the report into two different reports -- one for infrastructure problems only (for administrators) and the other for application-specific issues (for developers)
General Requirements	
75	Product should support IPv6
76	Product should provide daily vulnerability updates via download
77	Installation and usage of Product should do not require the need of a database server/instance.
78	The solution should be present as Leaders in the Gartner Magic Quadrant Application Security Testing 2016/2017
79	Comprehensive warranty for 3 years with Next business Day (NBD) resolution.