SCOPE & TECHNICAL SPECIFICATION

1. The scope of the project includes supply and deployment of the web content filter solution at BHEL PSSR Chennai, the installation includes all the necessary initial setup and deployment to all the users.

2. The vendor shall install latest patches/firmware required for the device.

3. The vendor shall integrate Active directory with the appliance enabling single sign- on for AD users in LAN.

4. The vendor shall configure all the Network parameters.

5. The vendor shall create all the rules/policies and assign them to the corresponding active directory group.

6. The vendor shall design the backup policy and document the procedure for the same.

7. The vendor shall demonstrate all the features specified in the technical specification of the document.

8. The vendor shall provide the documentation and procedure for initial setup, Installation and configuration of the Content filter solution.

9. The vendor shall give a one day training on the product to BHEL Technical team in BHEL's premises.

10. Stable version upgrades and patches shall be incorporated in to the solution whenever the OEM releases new version upgrades and patches.

11. Installation and complete configuration support shall be extended by the vendor, whenever any updates/upgrades for the software/firmware takes place without downtime.

12. Support level escalation matrix shall be provided.

13. The vendor shall make quarterly visits to BHEL PSSR Chennai to audit the health status of the solution and must submit a report on the same.

14. Telephonic support shall be extended by vendor whenever required. In the event of problem not being solved, the vendor shall provide onsite support and resolve the issue.

15. The vendor shall provide a portal support details/login of OEM for creating support case.

Technical Specifications for Mail Security Gateway Appliance			
Sr No	**Specifications**	**Products**	**Remarks**
Mail Gateway Features			
1	Solution should be appliance based.		
2	Solution must offer a layered approach to scanning email, using both connection management and mail scanning techniques to filter email.		
3	The solution should be supplied with 1000 users license. The solution should be scalable upto 1500 concurrent users on a single appliance.		
4	Solution must offer at a minimum 3 layers of antivirus protection.		
5	Solution must offer real-time protection that will block new spam and viruses in real-time without waiting for new definitions to be downloaded to the appliance.		
6	Solution must cache definitions for known viruses locally.		
7	Solution should enable users to whitelist senders and mark messages as spam and not spam directly from Microsoft Outlook and Lotus Notes clients.		
8	Solution should be able to store quarantine email on the appliance itself and also have the capability to send quarantined email off-box to an administrator email address for management.		
9	Solution should offer users the ability to whitelist/blacklist senders as well as manage their own spam scores.		
10	Solution should be able to perform federated searches across logs between distributed appliances.		
11	In a clustered environment, solution should offer and maintain redundant storage on separate appliances for user quarantine email.		

12	Solution should offer a g lob al (managed and controlled by the administrator) and per user Bayesian Analysis		
13	Solution should have the ability for administrators to block emails via header/subject/body using regular expressions and exact word matches.		
14	Solution should be able to block attachments by file type and file extension.		
15	Solution should have the capability to force a SMTP over TLS connection when sending email to or receiving email from a specific domain.		
16	Solution should have the ability to utilize a database of IP address and domain p airs to help b lock spam and allow good email through, similar to Registered Email Sender List (RESL).		
17	Solution should be able to block bounce messages/NDR's from forged return ad dresses that did not originate from the network		
18	Solution should have the ability to enforce email policy based on character set of message parts.		
19	Solution should be able to perform a reverse DNS lookup on the send er IP address, determine the Top Level Domain (TLD) and block emails originating from IP addresses assigned to providers in common spamming countries.		
20	Solution should be enable administrators to create custom rules based on results of reverse DNS lookup of sender IP address.		

21	Solution should be able to enforce email policy by checking the nameserver of a domain referenced in an embedded URI and validating against a list of nameservers known to b e used exclusively by spammers.		
22	Solution should be able to enforce email policy by inspecting the content of free Web sites such as GeoCities and Blogspot linked to URIs in spam emails.		
23	Solution should allow the administrator the enforce email policy based on URIs embedded in email parts, without the use of complex regular expression.		
24	Solution must be able to prevent spammers from sending large amounts of email to the appliance over a short time period from any single IP address.		
25	Solution should be able to use SNMP for monitoring and alerts and utilize an API for making configuration changes without having to log into the appliance.		
26	Solution must offer at least 4 roles of administration to the appliance.		
27	Solution should leverage collaborative efforts of white hat community security researchers in the collection and usage of antispam and antivirus protection.		
28	No user intervention should be required to install spam, virus, and security definitions.		
29	Appliance based solution should not charge per user license fees.		

30	Solution should be able to provide hybrid email security; cloud pre-filtering of inbound email traffic to stop spam and malware with delivery of filtered email to an on-site secure email g ateway.		
31	Solution should be able to provide email continuity through spooling in the cloud and delivery to an alternative email server if needed.		
32	Solution should be able to do outbound email encryption through policy on the unit or user specified with a Microsoft Outlook add-in.		
33	Solution should be able to provide internal email antivirus protection with the Microsoft Exchange Anti- Virus Agent add-in for example.		
34	Solution should be able to receive email from IPv6 networks, apply content policies, and deliver to either IPv4 or IPv6 networks.		
35	Solution must be able to prevent compromised internal systems from sending emails to a large number of recipients from a single user account over a short period of time.		
36	Solutions should be able to centrally manage policies and do administration.		
37	Solution should be offered in virtual form factors that run on popular hypervisors for virtualized environments.		
38	Solution should be able prevent leakage of sensitive data by detecting sensitive data in outbound emails and either blocking or encrypting it.		