**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 Web content filter Appliance | | | |
|---|---|---|---|
| **Sr No** | **Specifications** | **Products** | **Remarks** |
| **General** | | | |
| 1 | The proposed solution should be of Appliance based architecture. | | |
| 2 | The solution should be supplied with 300 users license. The solution should be capable of handling<br>300 concurrent users, scalable upto 500 concurrent users on a single appliance. | | |
| 3 | The solution should include supply of URL filter License for the concurrent users for a period of 3 years. | | |
| 4 | Onsite installation of appliance and migration activity is the scope of the bidder. | | |
| 5 | The bidder must ensure complete validity and support of the product from OEM for 3 years from the date of commissioning of the solution. | | |
| 6 | The solution should be IPv6 compliant. | | |
| 7 | The solution should cover updates, upgrades and subscription for a period of 3 years from the date of commissioning of the solution. | | |

| Appliance Specifications | | | |
|---|---|---|---|
| 1 | The appliance should be equipped with sufficient Memory & Flash to handle the load for the number of concurrent users specified. | | |
| 2 | The appliance should be capable of storing the system logs on the appliance. | | |
| 3 | The appliance should have minimum of 2 x 1 GBE Copper ports. | | |
| 4 | The appliance should have inbuilt HDD with a minimum usable storage capacity of 100GB | | |
| 5 | The appliance should have a minimum of 8GB inbuilt memory. | | |
| 6 | The solution should have option to connect to two different power sources. | | |
| 7 | The appliance should have diagnostic network utilities like trace route, ns lookup, dig and TCP dump/packet capture. | | |
| 8 | The solution should have the option to configure both Ipv4 and IPv6 IPs for the clients to access. | | |
| 9 | All configurations relevant to IPv6 should be done by the bidder as per BHEL's requirement. | | |

| | | | |
|---|---|---|---|
| 10 | The solution should support NTP, SNMP, VLAN tagging on a port etc. | | |
| 11 | The solution should have facility to check the health monitoring status of the appliance like CPU usage, Memory usage , Interface utilization etc | | |
| 12 | The solution should have Inbuilt Caching Mechanism . | | |
| 13 | The solution should be capable of processing at least 10 Mbps throughput (HTTP/HTTPS/FTP). | | |
| 14 | The appliance should be capable of handling at least 200 HTTP/HTTPS/FTP requests per second<br>(mention the exact number of requests supported per second). | | |
| | | | |
| **Web content filter features** | | | |
| 1 | The solution should be a Fast Web Proxy and should support HTTP, FTP and HTTPS proxy. The solution should also support HTTPS scanning. | | |
| 2 | The solution should scan all Incoming traffic, should effectively mitigate malware that attempts to bypass proxy and should block any malicious outbound traffic. | | |
| 3 | The solution should have functionality to control web 2.0 and real time content categorization. | | |
| 4 | The solution should provide Web Reputation Filters that examine every request made by the browser. | | |

| | | | |
|---|---|---|---|
| 5 | The solution should have URL database which should have at least 15 million sites and minimum 50 + pre-defined categories. | | |
| 6 | URL database should be updated regularly by the OEM automatically. | | |
| 7 | The Web Reputation Filters should have capability to analyze web traffic and network-related parameters to accurately evaluate the trustworthiness of a URL or IP address. | | |
| 8 | The solution should detect and block spyware activity trying to connect to the outside Internet through proxy. The solution should effectively mitigate malware that attempts to bypass proxy. | | |
| 9 | The solution should have inbuilt virus engine to block any Virus activity in HTTP, HTTPS and FTP traffic. | | |
| 10 | The solution should be capable of dynamically blocking a legitimate website which has become infected and unblock the site when the threat has been removed. | | |
| 11 | The solution should have inbuilt malware engine to block malware threats. | | |
| 12 | The solution should block web based threats, like adware, browser hijackers, phishing, pharming, rootkits, trojans, worms, system monitors and keyloggers. | | |

| | | | |
|---|---|---|---|
| 13 | The solution should detect Phone Home attempts occurring from the entire Network. | | |
| 14 | The solution should provide facility to define different bandwidth or quota for per user/per user group, per IP address/per IP address group, under different schedules. | | |
| 15 | The solution must be capable of blocking the following types of applications and sites: P2P, VoIP, Games, Remote Control, Chats, Torrents, Instant Messaging Sites, malicious sites and Proxy avoidance sites. | | |
| 16 | The solution should support creation of custom URL categories for allowing/blocking specific destinations as required by the organization. | | |
| 17 | The solution should support application control such as blocking specific versions of browsers. | | |
| 18 | The solution should have facility to enable Real Time Dynamic categorization to classify URLs in real time, in case the URL the user is visiting is not already under the pre-defined or custom categories database. | | |
| 19 | URL check & submission - Provision should be available to check URL category and submit new URL for categorization. | | |
| 20 | The solution should have facility for End User or administrator to report to OEM, in case of mis- categorization of URL. | | |

| | | | |
|---|---|---|---|
| 21 | File download restrictions: The solution should be capable of blocking file downloads based on MIME File types. | | |
| 22 | Time based : The solution should be able to allow/restrict time based internet access based on per user/per user group | | |
| 23 | DNS Splitting : The solution should support configuration to use split DNS. It should be able to refer to different DNS for Different Domains (e.g. root dns for all external domains and internal DNS for organization domain). | | |
| 24 | The solution should allow to deploy the appliance in explicit proxy as well as transparent mode. | | |
| 25 | The solution should support explicit forward proxy mode deployment. | | |
| 26 | The solution should also support transparent mode deployment using WCCP | | |
| 27 | The solution should have facility to inform end user with notification page informing them of organization internet usage policies and provide reasons as to why they have been blocked. (The page should be customizable by the administrator). | | |

| | | | |
|---|---|---|---|
| **Client/Browser support** | | | |
| 1 | The content filter should be accessible from IPv6-only clients/desktops also. | | |
| 2 | Apart from http access from popular web browsers, the solution should allow FTP clients like Filezilla/Winscp to access FTP Sites. | | |
| **User authentication and Active directory Integration** | | | |
| 1 | The solution should integrate with existing Windows Active Directory server for user authentication. | | |
| 2 | The solution should support automatic transparent Single Sign On for user authentication. | | |
| 3 | The solution should support Multiple Auth Servers / Auth Failover using Multi Scheme Auth (NTLM, LDAP etc). | | |
| 4 | The solution should support configuration of at least two authentication servers, so that, in case of failure of one authentication server, the other authentication server should authenticate without any manual intervention. | | |
| 5 | The solution should be able to define access to internet, based on client IP addresses, range of IP addresses and IP subnets. | | |
| 6 | The solution must support user based policy configuration for security and Internet access based on Active directory groups. This allows administrator to define user or group based access policies to Internet. | | |

| Management Features | | | |
|---|---|---|---|
| 1 | Secure Web Based management - The appliance should be manageable via HTTP or HTTPS Management console. | | |
| 2 | CLI based management - The appliance should be manageable via command line using SSH/Telnet. | | |
| 3 | Serial Console access - The appliance should have serial console access connectivity. | | |
| 4 | The solution should have the provision to backup and restore the appliance configuration to local disk or remote host. | | |
| 5 | Admin access restriction - Access to management console GUI should be restricted based on IP addresses or range of IP addresses. | | |
| 6 | The Management console provides Security administrators with a comprehensive, up-to-date view of threat characteristics and response, user activity, network load, system stats. | | |
| 7 | Admin access logs, Event logs and System logs should be should be available in the appliance. | | |

| Notification, Reporting and logging | | | |
|---|---|---|---|
| 1 | The solution should have reporting solution bundled. | | |
| 2 | The solution should provide connection-wise reports for user, source IP, destination IP, source port, destination port and protocol. | | |

| | | | |
|---|---|---|---|
| 3 | User Report should be Informative and exhaustive on User Activity and URL filtering activities. The report should give details of : | | |
| 3.1 | Top web browsing users by page and bandwidth, categories per page views, sites viewed by users, sites blocked, malware request blocked by sites, Search engine usage etc. | | |
| 3.2 | Graphical report should be provided for the above. | | |
| 4 | Web Browsing request per day of a week, per hour of day. | | |
| 5 | Bandwidth Reports should contain reports on Bandwidth Consumed / Bandwidth Saved for an hour/day/week. | | |
| 6 | Details of browsers and version used from client machines. | | |
| 7 | List of clients with potential threats. | | |
| 8 | The solution should have customizable email alerts, automated report scheduling and message alerts. | | |
| 9 | The solution should allow exporting of reports in PDF and Excel format. | | |
| 10 | The solution should forward logging information of all modules to syslog servers. | | |
| 11 | The solution should be able to transfer the logs to a remote FTP server or remote database. | | |

| | | | |
|---|---|---|---|
| 12 | The report should give detailed proxy access logs that can be searched via filters, for easy location of any desired access of the user. | | |
| 13 | The retention period of the reporter details should be for a period of atleast 30 days with no db size limitation . The retention period should also be customizable. (The database license should be bundled with the solution). | | |
| **Technical support** | | | |
| 1 | Remote support from OEM should be available via India Toll free and email (Should be 24x7) | | |
| 2 | OEM Support Portal access should be provided for Case management, knowledgebase, new version information, tools, download of Patches, Updates and Upgrades etc. | | |
| 3 | The bidder should provide direct support and should not engage a third party for support and service. | | |
| 4 | Next business day support shall be available for appliance with instant replacement. | | |