ANNEXURE A

S.No	Unified Threat Management Appliance specifications	Compliance	Remarks
	GENERAL SPECIFICATIONS		
1.1	Product or OEM should be ISO 9001-2008 Certified		
1.2	OEM should have regional presence for sales & support		
1.3	Proposed appliance should support inbuilt hdd for storage of Logs &		
1.4	Proposed solution should comply FCC and CE norms		
1.5	The proposed solution should match following criteria.		
	a. Hardware platform must be 64 bit		
	b. Must be based on Multicore Parallel Processing Architecture		
	c. 10 number of 10/100/1000 interface with Hardware Bypass		
	d. 25000 number of new connection		
	e. 700,000 number of concurrent connection		
	f. 3.0 Gbps Firewall throughput		
	g. 1000Mbps IPS throughput		
	h. 550Mpbs UTM throughput		
1.6	The proposed solution should have unrestricted user/node license.		
1.7	The proposed solution must work as standalone HTTP proxy server with integrated Firewall, Anti Virus, Anti Spam, Content filtering, IPS.		
1.8	The proposed solution must support User based policy configuration for security & internet management.		
1.9	The proposed solution should provide on appliance reports based on user not only on the base of IP address.		
2.0	Proposed appliance shoulf support MIX mode deployment.		
	Administration, Authentication & General Configuration		
2.1	The proposed solution should support administration via secured communiation over HTTPS, SSH and from Console.		
2.2	The proposed solution should be able to export and import configuration backup including user objects		
2.3	The proposed solution should support Route (Layer 3)/transparent mode (Layer 2).		
2.4	The proposed solution should support integration with Windows NTLM, Active Directory, LDAP, Radius or Local Database for user authentication.		
2.5	The proposed solution must support automatic transparent Single Sign on (ASSO) for user authentication. SSO must be proxy independent and support all applications for authentication.		
2.6	The proposed solution should support Dynamic DNS configuration.		
2.7	The proposed solution should provide bandwidth utilization graph on daily, weekly, monthly or yearly for total or individual ISP link.		
2.8	The proposed solution should provide real time data transffer/bandwidth utilization done by individual user/ip/application.		
2.9	The proposed solution should support Parent Proxy with IP/FQDN support.		
2.10	The proposed solution should support NTP.		
2.11	The proposed solution should support user/ip/mac binding functionality to map username with IP address & MAC address for security reason.		
2.12	The proposed solution should have multi lingual support for Web admin console.		
2.13	The proposed solution should support Version roll back functionality.		
2.14	The proposed solution should support session time out & Idle time out facility to forcefully logout the users.		

2.15	The proposed solution should support ACL based user creation for administration purpose.		
2.16	The proposed solution should support LAN bypass facility in case appliance is configured in Transparent mode.		
2.17	The proposed solution should support inbuilt PPPOE client and should be capable to automatically update all required configuration whenever PPPOE get changed.		
2.18	The proposed solution should support SNMP v1, v2c & v3.		
2.19	The proposed solution must be firmware based instead of normal software with capability to keep three firmware instant roll back.		
2.20	The proposed solution must provide flexible, granular role-based GUI administration.		
2.21	The proposed solution must provide support of multiple authentication servers for each module (Firewall, Different type of VPN)		
2.22	The proposed solution must support of Thin Client (Microsoft TSE, Citrix) authentication and must be able to differentiate users coming from same IP address.		
	Multiple ISP load balancing and Failover		
3.1	The proposed solution should support load balancing & failover for more than 2 ISP.		
3.2	The proposed solution should support explicit routing based on Source, Destination, Username, Application.		
3.3	The proposed solution should support weighted round robin algorithm for Load balancing.		
3.4	The proposed solution should provide option to create failover condition on ICMP, TCP or UDP protocol to detect failed ISP connection.		
3.5	The proposed solution should send alert email to admin on change of gateway status.		
3.6	The proposed solution should have Active/Active (Round Robin) and Active/Passive gateway load balancing and failover support.		
	High Availabiliy		
4.1	The proposed solution should support High Availability Active/Passive or Active/Active		
4.2	The proposed solution should be ICSA certified High Availability solution.		
4.3	The proposed solution should send notification to admin on change of appliance status in High Availability.		
4.4	The HA traffic between two peers must be encrypted.		
4.5	The proposed solution should support Link, device & Session failure.		
4.6	The proposed solution should support automatic & manual synchronization between appliances in cluster.		
	Firewall		
5.1	The proposed solution should be standalone appliance with hardened OS.		
5.2	The proposed solution should be ICSA & Webcoast checkmark certified firewall.		
5.3	The proposed solution should support stateful inspection with user based one-to-one & dynamic NAT, PAT.		
5.4	The proposed solution must support user identity as matching criteria along with Source/Destination IP/Subnet/group, destination Port in firewall rule.		
5.5	The proposed solution should facilitate to apply unified threat policy like AV/AS, IPS, Content filtering, Bandwidth policy & policy based routing decision on firewall rule for ease of use, also unified threat controls must be applied on inter zone traffic.		
5.6	The proposed solution should support user defined multi zone security architecture.		

5.7	The proposed solution should have predefine application based on port/Signature & also support creation of custom application based on port/protocol number.		
5.8	The proposed solution should support ibound NAT load balancing.		
5.9	The proposed solution should support 802.1q VLAN tagging support.		
5.10	The proposed solution should support dynamic routing like RIP1, RIP2, ISPF, BGP4.		
5.11	The proposed solution should support Cisco compliance command line interface for Static/Dynamic routing.		
5.12	The proposed system should provide alert message on Dash Board whenever default password is not changed, non secure access is allowed & module subscription is expiring.		
5.13	The proposed system must provide Mac Address (Physical Address) based firewall rule to provide OSI Layer 2 to Layer 7 security		
5.14	The proposed solution must be support IPv6 as per www.ipv6ready.org guidelines		
5.15	The proposed solution must support 3G UMTS, GSM, GPRS modem via USB interface for VPN and Gateway Failover - Load Balancing.		
5.16	The proposed solution should support Fully Qualified Domain Name (FQDN) based host and host group.		
5.17	The proposed solution should support Differenciated Services Code Point (DSCP)		
	IPS		
6.1	The proposed solution should be webcoast checkmark certified.		
6.2	The proposed solution should have singnature based and protocol anomaly based Intrusion prevention system.		
6.3	The proposed solution should have 4000+ signature database.		
6.4	The proposed solution must support creation of custom IPS signature.		
6.5	The proposed solution must support creation of multiple IPS policy for different zone instead of blanket policy at interface level.		
6.6	The proposed solution must support configuration option to disable/enable category/signature to reduce the packet latency.		
6.7	The proposed solution should give username along with IP in IPS alerts and reports.		
6.8	The proposed solution should automatically takes update from update server.		
6.9	The proposed solution must support blocking of anonymous open HTTP Proxy running on 80 port or any other port & also should support client based open proxy like Ultra surf. .		
6.10	The proposed solution should able to detect & block known P2P based instant messanging application like skype & known chat application like WLM, Rediffbol etc.		
6.11	The propopsed solution should generate the alerts for attacks		
6.12	The proposed solution should generate historical reports based on top alerts, top attackers, severity wise, top victims, protocol wise.		
	Gateway Anti Virus		
7.1	The proposed solution should have an integrated Anti Virus solution.		
7.2	The proposed solution should have webcoast checkmark certification for Anti virus/Anti Spyware.		
7.3	The proposed solution must work as SMTP proxy not as MTA or relay server.		
7.4	The proposed solution should support scanning for SMTP, POP3, IMAP, FTP, HTTP, FTP over HTTP protocols.		

7.5	The basic virus signature database of proposed solution should comprise complete wild list signatures and variants as well as malware like Phising, spyware.		
7.6	The proposed solution should have facility to add signature/disclaimer in mails.		
7.7	The proposed solution must support on appliance quarantined facility and also personlized user based quarantine area.		
7.8	The proposed solution should support blocking of dynamic/executable files based on file extension.		
7.9	For SMTP traffic, the proposed solution should support following actions for infected, suspisious or protected attachments mails.		
	a. Drop mail		
	b. Deliver the mail without attachment		
	c. Deliver original mail		
	d. Notify to administrator		
7.10	The proposed solution should support multiple anti virus policy for sender/recipient email address or address group for notification setting, quarantine setting & file extension setting instead of single blanket policy		
7.11	The proposed solution should update the singature database at a frequency of less than one hour & it should also support manual update.		
7.12	For POP3 & IMAP traffic, the proposed system should strip the virus infected attachement & send notification to receipient & Admin.		
7.13	The proposed solution should scan http traffic based on username, source/destination IP address or URL based regular expression.		
7.14	The proposed solution should provide option to bypass scanning for specific HTTP traffic.		
7.15	The proposed solution should support real mode & batch mode for HTTP virus scanning.		
7.16	The proposed solution should provide historical reports based on username, IP address, Sender, Recepient & Virus Names.		
7.17	The proposed solution should have virus detection rate above 98%. Submit the required document.		
	Gateway Anti Spam		
8.1	The proposed solution should have an integrated Anti Spam solution.		
8.2	The proposed solution should have webcoast checkmark certification for Anti Spam.		
8.3	The proposed solution should have configurable policy options to select what traffic to scan for spam.		
8.4	The proposed solution should support spam scanning for SMTP, POP3, IMAP.		
8.5	The proposed solution should support RBL database for spam detection.		
8.6	The proposed solution must support mail archive option to keep copy of incoming & outgoing mails to administrator defined email address.		
8.7	The proposed solution should have multiple configurable policy for email id/address group for quarantine setting, different actions instead of blanket policy.		
8.8	The proposed solution must support on appliance quarantined facility and also personlized user based quarantine area with email release option		
8.9	The proposed solution should support real time spam detection & also supports proactive virus detection technology which detects and blocks the new outbreaks immediately and accurately.		
8.10	For Smtp traffic, the proposed solution support following actions		
	a. Tagging		
	b. Drop		
	c. Reject		

	d. Change recepient		
	e. Deliver the mail to recepient		
8.11	The proposed solution should support IP/Email address white list/Black list facility.		
8.12	The proposed solution should support option to enable/disable antispam scanning for SMTP authenticated traffic.		
8.13	The proposed solution should support spam detection using Recurrent pattern detection technology (RPD) to identify spam out breaks.		
8.14	The proposed solution should support language independent spam detection functionality.		
8.15	The proposed solution should block image based spam mails i.e. email message with text embedded in a image file.		
8.16	The proposed solution should provide historical reports based on username, IP address, Sender, Recepient & spam category.		
8.17	The proposed solution must provide Anti-Spam Message Digest feature per user.		
8.18	The proposed solution must save bandwidth by blocking 85% of spam messages at gateway level itself without downloading the message using advanced IP Reputation Filtering feature.		
	Proxy Solution Web content filtering		
9.1	The proposed solution shoule be webcoast checkmark certified.		
9.2	The proposed solution should be integrated solution with local database instead of quering to database hosted somewhere on the		
9.3	The proposed solution must work as Standalone HTTP proxy.		
9.4	The proposed solution must have 82+ web category with 40 Million URL database.		
9.5	The proposed solution must have following features inbuilt		
	a. Should able to block HTTPS based URLs with the help of Certificates.		
	b. Should able to block URL based on regular expression		
	c. Should support exclusion list based on regular expression		
	d. Must have support to block any HTTP Upload traffic.		
	e. Should able to block google cached websites on based of category.		
	f. Should able to block websited hosted on Akamai.		
	g. Should able to identify & block requests coming from behind proxy server on the base of username & IP address.		
	h. Should able to identify & block URL translation request.		
9.6	The proposed solution should support application control blocking features as follows		
9.7	a. Should able to block known Chat application like Yahoo, MSN, AOL, Google, Rediff, Jabber etc		
9.8	b. Should support blocking of File transfer on known Chat application and FTP protocol.		
9.9	The proposed solution must block HTTP or HTTPS based anonymous proxy request available on the internet.		
9.10	The proposed solution should provide option to customize Access denied message for each category.		
9.11	The proposed solution should be CIPA compliant and should have predefined CIPA based internet acess policy.		
9.12	The proposed solution should be able to identify traffic based on Productive, Neutral, unhealthy & non working websites as specified by admin.		
9.13	The proposed solution should have specific categories that would reduce employee productivity, bandwidth choking sites and malicious websites.		
9.14	The proposed solution should able to generate reports based on username, IP address, URL, groups, categories & category type.		
9.15	The proposed solution should support search criteria in repoprts to find the relevant data.		

9.16	The proposed solution should support creation of cyclic policy on Daily/Weekly/Monthly/Yearly basis for internet access on individual users/group of users.		
9.17	The proposed solution should support creation of internet access time policy for individual users or on group basis.		
9.18	The proposed solution should support creation of Data transfer policy on daily/weekly/monthly/yearly basis for individual user or group basis.		
9.19	The proposed solution should support creation of cyclic data transfer policy on Daily/weekly/Monthly/yearly basis for individual user or on group.		
9.20	The proposed solution should have integrated bandwidth management.		
9.21	The proposed solution should able to set guaranteed and burstable bandwidth per User/IP/Application on individual or shared basis.		
9.22	The proposed solution should provide option to set different level of priority for critical application.		
9.23	The proposed solution should provide option to define different bandwidth for different schedule in a single policy & bandwidth should change as per schedule on the fly.		
9.24	The proposed solution must provide web category based bandwidth management and priotization.		
9.25	The proposed solution must provide logging and extensive controls on Instant Messanging (IM) traffic for Yahoo and MSN messengers 1. Log of chat sessions for all or specific set of users. 2. Rules to control allow or deny chat, voice, web cam and file transfer for specific ID or Group of IDs. 3. Archieve of transfered files. 4. Antivirus scanning on file transfered.		
	VPN		
10.1	The proposed solution should be webcoast checkmark certified.		
10.2	The proposed solution should be VPNC Basic interop & AES interop certified.		
10.3	The proposed solution should support Ipsec (Net-to-Net, Host-to-Host, Client-to-site), L2tp & PPTP VPN connection.		
10.4	The proposed solution should support DES, 3DES, AES, Twofish, Blowfish, Serpent encryption algorithm.		
10.5	The proposed solution should support Preshared keys & Digital certificate based authentication.		
	The proposed solution should support Main mode & Aggressive mode for phase 1 negotiation.		
10.6	The proposed solution should support external certificate authorities.		
10.7	The proposed solution should support export facility of Client-to-site configuration for hassle free VPN configuration in remote Laptop/Desktop.		
10.8	The proposed solution should support commonly available Ipsec VPN clients.		
10.9	The proposed solution should support local certificate authority & should support create/renew/Delete self signed certificate.		
10.10	The proposed solution should support VPN failover for redundancy purpose where more than one connections are in group & if one connection goes down it automatically switch over to another connection for zero downtime.		
10.11	The proposed solution should have preloaded third party certicate authority including verisign/Entrust.net/Microsoft and provide facility to upload any other certificate authority.		
10.12	The proposed solution should support Threat free Ipsec/L2TP/PPTP VPN tunnel.		
10.13	The propsed solution must provide on appliance SSL-VPN solution with Web Access (Clientless), Full Tunnel and Split Tunnel control. Solution should provide per user / group SSL-VPN access (Must be free license for unlimited users)		

10.14	SSL-VPN solution should be certified by VPNC for SSL Portal / FireFox Compatibility / Java Script / Basic and Advanced Network Extensions.		
	Logging & Reporting		
11.1	The proposed solution must have On-Appliance integrated iView reporting solution.		
11.2	The proposed solution should support minimum 1000+ drill down reports.		
11.3	The proposed solution should provides reports in HTML, CSV, PDF, Excel & graphical format.		
11.4	The proposed solution should support logging of Antivirus, Antispam, content filtering, Traffic discovery, IPS, Firewall activity on syslog server.		
11.5	The proposed solution should provides detailed reports for all files uploaded via HTTP or HTTPS protocol. The report should include username/IP address/URL/File name/Date and Time.		
11.6	The proposed solution should provide data transfer reports on the based of application, username, Ipaddress.		
11.7	The proposed solution should provide connection wise reports for user, source IP, destination IP, source port, destination port or protocol.		
11.8	The proposed solution should have facility to send reports on mail address or on FTP server.		
11.9	The proposed system solution provide approximate 45 regulatory compliance reports for SOX, HIPPA, PCI, FISMA and GLBA compliance.		
11.10	The proposed solution should support Auditing facility to track all activity carried out Security appliance.		
11.11	The proposed solution should support multiple syslog server for remote logging.		
11.12	The proposed solution should forward logging information of all modules to syslog servers.		
11.13	The proposwed solution should have configurable option for email alerts/automated Report scheduling.		
11.14	The proposed solution should be able to provide detailed reports about all mails passing through the firewall.		
11.15	The proposed solution should provide reports for all blocked attempts done by users/Ipaddress.		
11.16	The proposed solution must be capable to derive logs and reports of proprietary devices including UTMs, Proxy Firewalls, Custom Applications and Syslog-compatible devices.		
11.17	The proposed solution must be capable to provide Multiple Dashboard Report along with custom to customize the dashboards.		
11.18	The proposed inbuilt reporting solution should be capable to do the forensic analysis to help organizations reconstruct the sequence of events that occurred at the time of security breach through iView logs and reports.		