Annexure-1

UNIFIED THREAT MANAGEMENT APPLIANCE SPECIFICATIONS	
1	**ARCHITECTURE**
1.1	Product or OEM should be ISO 9001-2000 Certified for its product and ISO 20000 for support and services
1.2	Proposed appliance should support for On appliance reporting for logs and reports
1.3	The Firewall should be ICSA Labs certified and EAL4+ certified for appliance
1.4	Proposed appliance should have firmware residing on Flash
1.5	Proposed solution should comply with FCC and CE norms
1.6	The proposed solution should match the following criteria.
	a. Must have a 64-bit hardware platform
	b. Must be based on Multicore Parallel Processing Architecture
	c. 8 x 10/100/1000 interfaces supporting Hardware Bypass along with 2 slots for flexi port module where port options per slot are GbE Copper / GbE Fiber / 10GbE Fiber as 8/8/4 ratio
	e. 6,400,000 concurrent connections
	f. 200,000 New Sessions per second
	f. 28.5 Gbps UDP and 20 Gbps TCP Firewall throughput
	g. 8.5 Gbps IPS throughput
	h. 5 Gbps NGFW throughput
	i. 5.5 Gbps AV throughput
	j. 750 Mbps SSL VPN throughput
	k. 4200 Mbps IPSec VPN throughput with support for 7250 IPSec VPN Tunnels
	h. 4GB of Flash.
1.7	The proposed solution should support unrestricted user/node license.
1.8	The proposed solution must work as a standalone HTTP proxy server with integrated Firewall, Anti Virus, Anti Spam, Content filtering, IPS and Web Application Firewall.
1.9	The proposed solution must support User based policy configuration for security and Internet management.
1.10	The proposed solution should provide on-appliance reports based not only on IP addresses but also based on users.
1.11	Should support TAP/Discover mode to demonstarte visibilities capabilities of Firewall.
1.12	Should support Text based configuration Import / Export
1.13	The UTM should work as wireless controller and should be able to manage multiple wireless access points Centrally from web admin console.

2	ADMINISTRATION, AUTHENTICATION & GENERAL CONFIGURATION
2.1	The proposed solution should support administration via secured communication over HTTPS, SSH and from Console.
2.2	The proposed solution should allow Guest User authentication via SMS
2.3	The proposed solution should be able to export and import configuration backup including user objects
2.4	The proposed solution must be able to be deployed in Route (Layer 3) and Transparent mode (Layer 2), individually and simultaneously.
2.5	The proposed solution should support integration with Windows NTLM, Active Directory, LDAP, Radius, TACACS+, RSA SecurID, Novell e-Directory or Local Database for user authentication.
2.6	The proposed solution must support Automatic Transparent Single Sign On for user authentication. SSO must be proxy independent and should support all applications for authentication.
2.7	The proposed solution should support Dynamic DNS configuration.
2.8	The proposed solution should provide bandwidth utilization graph on daily, weekly, monthly or yearly for all or individual ISP links.
2.9	The proposed solution should provide real time data transfer/bandwidth utilization details regarding individual user/ip/application.
2.10	The proposed solution should support Parent Proxy deployment with IP/FQDN support.
2.11	The proposed solution should support NTP.
2.12	The proposed solution should support user/ip/mac binding that can map username with corresponding IP and MAC addresses for security reason.
2.13	The proposed solution should have multi lingual support for Web admin console.
2.14	The proposed solution should support Version roll back functionality.
2.15	The proposed solution should be able to force-logout users upon session time-out and idle time-out.
2.16	The proposed solution should support ACL based user creation for administration purposes.
2.17	The proposed solution should support LAN bypass when the appliance is configured in Transparent Mode.
2.18	The proposed solution should support inbuilt PPPoE client and should be capable to automatically update all required configuration whenever PPPoE is updated.
2.19	The proposed solution should support SNMP v1, v2c and v3.
2.20	The proposed solution must be firmware-based rather than software-mounted. It should be able to hold two firmware images on the appliance simultaneously, to facilitate instant roll back.

2.21	The proposed solution must provide flexible, granular role-based GUI administration.
2.22	The proposed solution must provide support of multiple authentication servers for each module (e.g. Firewall, Different type of VPN)
2.23	The proposed solution must support multiple Thin Client (Microsoft TSE, Citrix) authentication mechanisms and must be able to differentiate between requests originating from the same IP address.
2.24	The proposed solution should support:
	1. DHCP Server
	2. DHCP Relay Agent
	3. DHCP support over Ipsec VPN
2.25	The proposed solution should work as DNS Proxy
2.26	The proposed solution must provide customizable login security settings
2.27	The proposed solution must provide customizable administrator password complexity setting
3	**MULTIPLE ISP LOAD BALANCING AND FAILOVER**
3.1	The proposed solution should support Load Balancing and Failover among more than 2 ISP Links.
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 options for failover condition which includes detecting a failed ISP link on ICMP, TCP or UDP protocol.
3.5	The proposed solution should send alert emails to the administrator(s) notifying any change in gateway status.
3.6	The proposed solution should have Active/Active (Round Robin) and Active/Passive Gateway Load Balancing and Failover support.
4	**HIGH AVAILABILITY**
4.1	The proposed solution should support High Availability Active/Passive and Active/Active
4.2	The High Availability feature in the proposed solution should be ICSA certified.
4.3	The proposed solution should notify administrator(s) on change of appliance status in High Availability.
4.4	The traffic between the two HA peers must be encrypted.
4.5	The proposed solution should tend to Link, Device and Session failure.
4.6	The proposed solution should support automatic and manual synchronization between appliances in cluster.
5	**FIREWALL**

5.1	The proposed solution should be standalone appliance with hardened OS.
5.2	The proposed solution should have an ICSA and WestCoast Labs Checkmark certified firewall.
5.3	The proposed solution should support stateful inspection with user based one-to-one and dynamic NAT and PAT.
5.4	The proposed solution should use User Identity as a matching criteria along with Source/Destination IP/Subnet/group, destination Port in firewall rule.
5.5	The proposed solution should facilitate the application of UTM policies like AV/AS, IPS, Content filtering, Bandwidth policy and policy-based routing decision on the firewall rule itself. Also UTM controls should be able to 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 predefined applications based on port/signature and also should support creation of custom application based on port/protocol number.
5.8	The proposed solution should support inbound NAT load balancing with different load balancing methods like First Alive,Round Robin,Random,Sticky IP and failover with server health check by TCP or ICMP probe.
5.9	The proposed solution should support 802.1q VLAN tagging.
5.10	The proposed solution should support dynamic routing like RIP1, RIP2, OSPF, 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 messages on Dash Board in events like default password has not been changed, non-secure access is allowed or module subscription is to expire soon.
5.13	The proposed system must provide Mac Address (Physical Address) based firewall rule configuration to provide OSI Layer 2 to Layer 7 security
5.14	The proposed solution must 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 must support Application-based Bandwidth Management which allows administrator to create application-based bandwidth policies.
6	**INTRUSION PREVENTION SYSTEM**
6.1	The proposed solution should be WestCoast Labs 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+ signatures in its database.
6.4	The proposed solution must support creation of custom IPS signatures.
6.5	The proposed solution must support creation of multiple IPS policies for different zones instead of a single blanket policy at interface level.
6.6	The proposed solution must allow disabling/enabling of IPS categories/signatures to reduce packet latency.
6.7	The proposed solution should display username along with the IPs in IPS alerts and reports.
6.8	The proposed solution should update automatically by synchronizing with an update server.
6.9	The propopsed solution should generate alerts in case of attacks.
6.10	The proposed solution should generate historical reports based on top alerts, top attackers, severity wise, top victims, protocol wise.
6.11	The proposed solution must be capable to provide session based IPS signature control with actions like: a. Drop Session: To drop the entire session if the traffic in that session matches with any IPS signature. b. Bypass Mode: To bypass the entire session if any traffic matches with IPS signature which is allowed to pass.
6.11	The proposed solution must be capable to provide IPS scanning for IPv6 traffic.
7	**GATEWAY ANTI VIRUS**
7.1	The proposed solution should have an integrated Anti Virus solution.
7.2	The proposed solution should have WestCoast Labs Checkmark certification for Anti virus/Anti Spyware.
7.3	The proposed solution must work as an SMTP proxy rather than an MTA or relay server.
7.4	The proposed solution should support scanning for SMTP, SMTPS,POP3, IMAP, FTP, HTTP, HTTPS, FTP over HTTP protocols.
7.5	The basic virus signature database of proposed solution should comprise all wild list signatures and variants, as well as those for malware like Phising, spyware.
7.6	The proposed solution should provide the facility to add signature/disclaimer in mails.
7.7	The proposed solution must support on-appliance quarantine facility and also a personlized user-based quarantine area.
7.8	The proposed solution should be able to block dynamic/executable files based on file extensions.

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 administrator
7.10	The proposed solution should support multiple anti virus policies based on sender/recipient email address or address group, notification setting, quarantine setting and file extension setting. There should not be just a single blanket policy.
7.11	The proposed solution should update the signature database at a frequency of less than one hour and it should also support manual update.
7.12	For POP3 and IMAP traffic, the proposed solution should strip the virus infected attachment and then notify the recipient and administrator.
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 the option to bypass scanning for specific HTTP traffic.
7.15	The proposed solution should support real mode and 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 a virus detection rate of above 98%.
7.18	The proposed solution should provide Security policies support for SMTP/SMTPS/POP/IMAP mail traffic of IPv6 network.
8	**GATEWAY ANTI SPAM SOLUTION**
8.1	The proposed solution should have an integrated Anti Spam solution.
8.2	The proposed solution should have WestCoast Labs 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 allow mail archiving to store copies of incoming and outgoing mails from particular email address(s).
8.7	The proposed solution should support multiple configurable policies based on email ID/address group, for quarantine setting, etc. There should not be just a single blanket policy.

8.8	The proposed solution must support on-appliance quarantine facility and also a personalized user-based quarantine area which allows you to release legitimate emails.
8.9	The proposed solution should support real time spam detection and proactive virus detection technology which detects and blocks new outbreaks immediately and accurately.
8.10	For SMTP traffic, the proposed solution should support the 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.
8.12	The proposed solution should allow enabling/disabling of antispam scanning for SMTP authenticated traffic.
8.13	The proposed solution should support spam detection using Recurrent Pattern Detection technology (RPD) to identify spam outbreaks.
8.14	The proposed solution should support language independent spam detection.
8.15	The proposed solution should block image based spam mails i.e. email message with text embedded in an image file.
8.16	The proposed solution should provide historical reports based on username, IP address, Sender, Recepient and spam category.
8.17	The proposed solution must provide Anti-Spam Message Digest feature per user.
8.18	The proposed solution must have the ability to save bandwidth by blocking 85% of spam messages at gateway level itself without downloading the message. This is possible using advanced IP Reputation Filtering feature.
9	**WEB FILTERING SOLUTION**
9.1	The proposed solution should be WestCoast Labs Checkmark certified.
9.2	The proposed solution should have a local database integrated into the system to avoid frequently querying a database hosted elsewhere.
9.3	The proposed solution must be able to work as a Standalone HTTP proxy.
9.4	The proposed solution must have a database containing 40 Million+ URLscategorized into 82+ web categories.
9.5	The proposed solution must have the following features inbuilt
	a. Should be able to block HTTPS based URLs
	b. Should be able to block URL based on regular expression

	c. Should support exclusion list based on regular expression
	d. Should be able to block any HTTP / HTTPS upload traffic.
	e. Should be able to block google cached websites based on category.
	f. Should be able to block websites hosted on Akamai.
	g. Should be able to identify and block requests coming from behind a proxy server on the basis of username and IP address.
	h. Should be able to identify and block URL translation request.
9.6	The proposed solution should support application control blocking features as follows
	a. Should be able to block known Chat applications like Yahoo, MSN, AOL, Google, Rediff, Jabber etc.
	b. Should support YouTube Education Filter
	c. Should support blocking of File transfer on known Chat applications and FTP protocol.
9.7	The proposed solution must block HTTP or HTTPS based anonymous proxy requests.
9.8	The proposed solution should allow customization of Access Denied message for each category.
9.9	The proposed solution should be CIPA compliant and should have predefined CIPA based Internet acess policy.
9.10	The proposed solution should be able to classify traffic as Productive, Neutral, Unhealthy or Non-working as specified by administrator.
9.11	The proposed solution should have specific categories that broadly classify websites. For instance, websites that reduce employee productivity, bandwidth choking sites or malicious websites.
9.12	The proposed solution should be able to generate reports based on username, IP address, URL, groups, categories and category type.
9.13	The proposed solution should allow searching in reports to filter relevant data.
9.14	The proposed solution should support creation of cyclic policies on Daily/Weekly/Monthly/Yearly basis for Internet access on individual users/group of users.
9.15	The proposed solution should support creation of Internet access time policies for individual users or user group.
9.16	The proposed solution should support creation of cyclic data transfer policies on Daily/weekly/Monthly/yearly basis for individual user or group.
9.17	The proposed solution should have integrated bandwidth management capability.
9.18	The proposed solution should be able to set guaranteed and burstable bandwidth per User/IP/Application on individual or shared basis.

9.19	The proposed solution should provide option to set higher priority for critical applications.
9.20	The proposed solution should provide option to define different bandwidth for different schedule in a single policy and bandwidth should change as per schedule on the fly.
9.21	The proposed solution must provide web category based bandwidth management and prioritization.
9.22	The proposed solution must provide logging and extensive controls on Instant Messeging (IM) traffic for Yahoo and MSN messengers such as: 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. Archiving of transfered files. 4. Antivirus scanning on file transfered.
10	**VPN**
10.1	The proposed solution should be WestCoast Labs Checkmark certified.
10.2	The proposed solution should be VPNC Basic interop and AES interop certified.
10.3	The proposed solution should support IPSec (Net-to-Net, Host-to-Host, Client-to-site), L2TP, PPTP and SSL VPN connection.
10.4	The proposed solution should support DES, 3DES, AES, Twofish, Blowfish, Serpent encryption algorithms.
10.5	The proposed solution should support Preshared keys as well as Digital certificate based authentication.
10.6	The proposed solution should support Main mode and Aggressive mode for phase 1 negotiation.
10.7	The proposed solution should support external certificate authorities.
10.8	The proposed solution should support export facility for Client-to-site configuration which ensures hassle free VPN configuration in remote Laptop/Desktop.
10.9	The proposed solution should support commonly available IPSec VPN clients.
10.10	The proposed solution should support local certificate authority & should support create/renew/Delete self signed certificate.
10.11	The proposed solution should support VPN failover for redundancy purpose wherein more than one connections are grouped together. If one connection goes down it automatically switches over to another working connection ensuring zero downtime.
10.12	The proposed solution must support automatic failover of Point to Point link (MPLS) with VPN for redundancy purpose.

10.13	The proposed solution should have preloaded third party certicate authorities including verisign/Entrust.net/Microsoft and should provide the facility to upload other certificate authorities.
10.14	The proposed solution should support Threat free IPSec/L2TP/PPTP VPN tunnelling.
10.15	The proposed solution must support Apple iOS and Android VPN clients
10.16	The proposed solution must provide on-appliance SSL VPN solution with Web Access (Clientless), Web Application Access (Most common used protocols), Full Tunnel and Split Tunnel control. Solution should provide per user / group SSL VPN access (Which involves free license for unlimited users)
10.15	SSL VPN solution should be certified by VPNC for SSL Portal / FireFox Compatibility / Java Script / Basic and Advanced Network Extensions.
11	**LOGGING AND REPORTING**
11.1	The proposed solution must support Four Eye (4-Eye) authentication to comply with Internet Privacy laws
11.2	The proposed solution must have On-Appliance, integrated reporting solution.
11.3	The proposed solution should be able to be integrated with Syslog reporting solution.
11.4	The proposed solution should support minimum 1200+ drill down reports.
11.5	The proposed solution should allow exporting of reports in PDF and Excel format.
11.6	The proposed solution should support logging of Antivirus, Antispam, Content Filtering, Traffic discovery, IPS, Firewall activity on syslog server.
11.7	The proposed solution should provide detailed reports for all files uploaded via HTTP or HTTPS protocol. The report should include username/IP address/URL/File name/Date and Time.
11.8	The proposed solution should provide data transfer reports on the basis of application, username, IP address.
11.9	The proposed solution should provide connection-wise reports for user, source IP, destination IP, source port, destination port or protocol.
11.10	The proposed solution should facilitate sending of reports on email address.
11.11	The proposed solution should provide compliance reports for SOX, HIPPA, PCI, FISMA and GLBA compliance.
11.12	The proposed solution should support Auditing facility to track all activity carried out on the appliance.
11.13	The proposed solution should support multiple syslog servers for remote logging.

11.14	The proposed solution should forward logging information of all modules to syslog servers.
11.15	The proposed solution should have customizable email alerts/automated Report scheduling.
11.16	The proposed solution should be able to provide detailed reports about all mails passing through the firewall.
11.17	The proposed solution should provide reports for all blocked attempts by users/IP address.
11.18	The proposed solution must be capable of deriving logs and reports of proprietary devices including UTMs, Proxy Firewalls, Custom Applications and Syslog-compatible devices.
11.19	The proposed solution must be capable to provide Multiple Dashboard Report along with the facility to customize the dashboards.
11.20	The proposed solution should be capable of forensic analysis to help organizations reconstruct the sequence of events that occurred at the time of security breach.
12	**APPLICATION FILTERING SOLUTION**
12.1	The proposed solution must provide inbuilt Application Filtering solution
12.2	The proposed solution must identify (Allow/Block/Log) the applications regardless of port, protocols, encryption including SSL/TLS.
12.3	The proposed solution should have be able to control 1500+ applications.
12.4	The proposed solution's application database must get updated automatically without any manual intervention
12.5	The proposed solution must give Identity based reports (username along with IP)
12.6	The proposed solution must be capable of blocking the following type of applications:
	a. Applications that allow file transfer
	b. Online Games
	c. Instant Messengers (Including Non-English Versions)
	d. Peer-to-Peer (P2P) applications (Including Non-English Versions)
	e. Browser Based Proxy (Regardless of IP address or Port Number)
	f. Web 2.0 based applications (Facebook, CRM etc)
	g. Applications that provide Remote Control
	h. All type of streaming media (Both Web and Software Based)
	i. VOIP Applications
12.7	The proposed solution must be capable of identifying hidden applications running over standard ports (80, 443, 22 etc)
13	**WAF**
13.1	Should support minimum of 1750 Mbps WAF throughput

13.2	The proposed solution should support protocol like HTTP/0.9/1.0/1.1
13.3	The proposed solution should have a Positive Protection Model.
13.4	The proposed solution should support the following:
	a. Cookie Protections Measures
	b. Session Attacks Mitigation
	c. Cryptographic URL and Parameter Protection
	d. Strict Request Flow Enforcement
	e. HTTPS (SSL) encryption offloading
	f. Banner-grabbing Protection
	g. Hidden field manipulation Protection
	h. SQL injection Protection
	i. OS command injection Protection
	j. Cross-site scripting Protection (XSS)
	k. Dangling pointer Protection
	l. Stealth commanding Protection
	m. Buffer overrun Protection
	n. URL Hardening engine
	o. Form field meta data validation
	p. Directory traversal prevention
	q. Response control
	r. Outbound data theft Protection
	s. Protocol limit checks
13.5	The proposed solution should not be signature based
13.6	The proposed solution should provide complete logging and monitoring