

**National Gallery of Modern Art
Government of India
Jaipur House, New Delhi-110003.**

File No. F. 170002/2014/NGMA

Dated: March , 2015

NOTICE INVITING QUOTATIONS

The Director, National Gallery of Modern Art (NGMA), New Delhi invites quotation for supply and installation of one no. UTM application with three years Subscription manufacturer or their authorised suppliers. Under two bid system.

- (1) The intending tenderers must produce copies of registration under DVAT Act 2004 and furnish their TIN number along with the bids.
- (2) The tenderer should have a local office in NCR Delhi and should be fully equipped to provide after sales service for the same.
- (3) The successful tenderer will have to supply and install at site inclusive of cartage.
- (4) **Warranty:** The equipments supplies shall carry warranty period of at-least 3 years from the date of installation.
- (5) Earnest Money Deposit (EMD) of Rs.20,000/- (Rs. Twenty Thousand Only.) is to be deposited by Demand Draft/Pay Order drawn in the name of "D.D.O, National Gallery of Modern Art" payable at New Delhi along with the Tender. Earnest Money Deposit shall be returned to unsuccessful tenderers
- (6) The successful bidder shall have to supply and Install the equipments within 10 days from the date of the supply orders.
- (7) Copies of tender forms can also obtained from the Administrative Officer, National Gallery of Modern Art, Jaipur House, New Delhi, at cost of Rs. 500/- or can be downloaded free of cost from Central Purchase Portal (<http://eprocure.gov.in>) and NGMA website www.ngmaindia.gov.in.
- (8) The quotations in sealed covers will be received up-to 17 March, 2015 by 2:00 p.m.
- (9) Quotations should be valid at-least for six months.
- (10) The Director (NGMA) reserves the right to accept the tenders in totality or in parts thereof. The Director (NGMA) also reserves the right to accept or reject the tenders without assigning any reasons.

Sd/
(S.K. Misra)
Administrative Officer

Encl: Terms & Conditions (Annexure-'A')
Specification (Annexure-'B')

Instruction for bidders /supplier and Terms & conditions of: -

Tender For supply & Installed One No. UTM Appliance with three years Subscription (by OEM Only) equipment will installed by certified engineer at National Galley of Modern Art, Jaipur House, New Delhi – 110 003. to NGMA.

While furnishing the quotations the following terms & conditions must be carefully noted.

1. Please mention this Reference No. and “Quotations” in block letters including closing date / time on the top of the sealed cover.
2. Apart from Supply & Installation charges, any other charges, such as packing and forwarding, delivery charges, sales tax /TIN/ VAT & Service tax etc., if any, should be mentioned clearly and separately. In the absence of their not being mentioned, no claim for any additional charges may be entertained later.
3. Tender specific authorization letter from the principal OEM should be enclosed in Technical bid.
4. Company should have at least two certified engineer for services support and “OEM” must assured online support for three years. Supplier/bidder must install and configure all the policy over LAN at NGMA and give training/support for the same as and when required during the contract period.
5. NO ADVANCE., payment will be made after Supply & Installation of UTM with 3 Years Subscription Services.
6. TIN /CST / ST / VAT Number must be clearly mentioned in the tender and bill.
7. Please mention the period for which quotations are valid under normal conditions.
8. Attach all technical details, literature, catalog as per the NGMA ask technical specification. Vendor / supplier should meet the following conditions & submit documentary evidence along with technical bid as per the tender.
9. Quotation received after the prescribed date and time will be liable to rejection.
10. The party whose rates are accepted will have to enter into a contract with this office for supply, Installed, Testing with Commissioning of items in accordance with the settled price, delivery, Installation & services, taxes, method of payment including submission of bills, packing, transport etc.
11. The Director, NGMA, reserves the right of rejecting all or any the quotations without assigning reason for their rejection and will not be bound to accept the lowest quotation.
12. During the UTM Service period, the service provider will make periodical preventive check of the UTM Systems to ensure / minimize the break down by site visits. Further, the service provider shall also make site visits at least once a monthly for providing any assistance / maintenance.
13. All UTM Service maintenance will be carried out in the office premises. However, the work that cannot be carried out within the premises can be allowed to be done outside but no extra payment will be made for that.
14. Replacement of all parts of UTM should be of same brand as original and any deviation should be made after obtaining written permission of the NGMA.

15. For any emergency, a site visit is mandatory.
16. Each bidder must clearly mention any exclusion separately.
17. The successful bidder will prepare separate maintenance log book for each of the machine to be taken under the Engineer Service support.
18. Rates should be quoted on enclosed format only.
19. The NGMA reserves the right to terminate the OEM Service Engineer support anytime without assigning any reason in case and no damages would be liable to be paid to the service provider thereupon.
20. Details along-with photo ID of the representatives authorized to make site visits would be furnished to the NGMA soon after award of the Contract and also whenever any representative in changed.
21. UTM Subscription Service Contract Validity: The contract shall be initially valid for a period of Three year that may be extended by an advance notice of 7-15 days at the sole discretion of the National Gallery of Modern Art for a further maximum period of one year and at the same terms & conditions, the extension shall be based on the satisfactory performance of the contract. The validity of contract comes to an end ipso facto by efflux of time unless otherwise renewed / terminated.
22. The successful bidder shall ensure and guarantee the conduct, behavior and honesty of the workers deputed by them. In case of any misconduct or any other damage or theft of the property of the NGMA, the successful bidder shall be responsible to make good all losses and damages.
23. **LATE RECIPITS OF THE OFFERS:** NGMA will not be responsible for late receipt of any quotation (i.e. After due date) sent through assured mail/speed post, the same will be not be entertained. The quotation will be accepted upto 17 March, 2015 on or before 2. p.m. an it will be opened on the same day at 4. p.m. in the presence of participating tenderer or their authorized representatives. (if available).

(Note: In the event of office being closed due to any reason whatsoever on the proposed date of opening of tender / quotation, the quotation will be opened on the next working day at the scheduled time without giving any notice.)

24. **DELIVERY:** The delivery date is the essence of the contract and supplier shall, therefore, supply the item within 10-15days from the date of confirmed order from NGMA.(Note: NGMA does not accept partial delivery of consignment.)
25. **LIQUIDATE DAMAGES.** In case the supplier default in the delivery and the supplier does not explain the position to the purchaser will in time and the purchaser has not accepted in extension of delivery period, the purchaser may forfeit the security tender. Purchaser reserves the right to claim damages of 2% per month for the delay in supply/service support or 100% for defective and sub standard goods supplied by the vendor even, if goods were inspected by the purchaser, prior to receipts at vendor/supplier site.
26. **TERMS OF PAYMENT:** Payment for UTM device with 3 years UTM subscription will be released within 30days from the date of satisfactory delivery, Installation, Testing & commissioning at NGMA.
27. **BID/PRICE VALIDITY:** The prices quoted must be firm during the tenure of the contract and the offer must remain open for acceptance, minimum up to 90 days from the date of opening of tender.

6. **Defect Liability Period**

The Defect Liability /Warranty period shall be at least **3 years (three years)** from the date of completion of supply and installation. The successful tenderer (s) shall be responsible for all defects for a period of **3 years** from the date of completion of the supply and installation. The successful tenderer(s) shall rectify/ replace the defect/defective parts within one week the specified time without any cost whatsoever upto the complete satisfaction of the competent authority of NGMA. The security deposit at 10% of contract amount shall be furnished by the successful tenderer in the form of Bank Guarantee favouring deposit of furnished by the tenderer. The Bank guarantee should be valid for 90 days beyond three years of warranty period. No interest will be paid on the Security Deposit.

Note: **The Technical Bid & Commercial Bid (Price Bid) should be sealed by bidders in separate cover duly super scribe and both these sealed cover along with their cover containing to be put in a envelop kept in bigger cover which should also be sealed and duly superscripted. The technical bid are to be opened at the first instance and evaluated. At the second stage Financial Bid of only technically accepted / qualified offers will be opened for further evaluation and ranking before awarding the contract.**

All interested parties should make sure that they fulfill the above terms and conditions before submitting their quotations.

Sd/
(S.K. Misra)
Administrative Officer

(FORM FOR TECHNICAL BID)

Tender No. _____

Tender DATE. _____

To, National Gallery of Modern Art Jaipur House, India Gate New Delhi – 110 003.	FROM:- M/s
---	------------

Subject: - Tender For supply & Installed One No. UTM Appliance with three years Subscription (by OEM Only) by certified engineer at National Galley of Modern Art, Jaipur House, New Delhi – 110 003.

Sir,

Our Company profile is as under :

1. Name of Company with Complete address:- _____
2. Name of organization Owner/company Owner /Director/ Proprietor/ of the firm :- _____
3. Phone No. _____ Email address _____
Mobile No. _____ Office Fax No. _____
4. Income-tax PAN No./TIN No. Registration No.:
_____ (also copy enclosed.)
5. TENDER SPECIFIC MAF (OEM) Authorization letter copy enclosed.
6. An undertaking on company's letter head stating that the firm is not blacklisted by any Govt. Department / Institution / Public Enterprises / undertaking and no arbitration case is laying pending with this office as on date.
7. EMD of Rs.20,0000 is Eclosed herewith D.D.No. _____ Bank dated _____

(Signature with stamp of Tenderer)

FORM FOR COMMERCIAL BID (PRICE BID)

Tender No. _____

Tender DATE. _____

To, National Gallery of Modern Art Jaipur House, India Gate New Delhi – 110 003.	FROM:- M/s
---	------------

Sir,

We have examined the tender for **Tender For supply & Installed One No. UTM Appliance with three years Subscription (by OEM Only) equipment will installed by certified engineer at National Galley of Modern Art, Jaipur House, New Delhi – 110003.**, the prescribed specification and read the Terms & conditions of Tender. Our rate for the items according to your technical specification & Terms are as under:-

SI. No.	Description of the product	UNIT PRICE (In Rs.)	Qty.	Amount	TAX @ (if any)	Other Charges (if any)	Total Amount (in Rs.)
	Product Make & Model	(a)	(b)	(C)	(D)	(E)	(c+d+e)
01							
02	3 Years Total value Subscription by "OEM"						

Grand Total Amount in words: _____ _____

(Signature with stamp of Tenderer)

UNIFIED THREAT MANAGEMENT APPLIANCE SPECIFICATIONS		COMPLIANCE	REMARKS
ARCHITECTURE			
1.1	Specifications		
1.2	Proposed appliance should support for On appliance reporting for logs and reports		
1.3	Proposed appliance should have firmware residing on Flash		
1.4	Proposed solution should comply with FCC and CE norms		
1.5	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 10/100/1000 interfaces supporting Hardware Bypass		
	e. 1,000,000 concurrent connections		
	f. 30,000 New Sessions per second		
	f. 3 Gbps Firewall throughput		
	g. 700 Mbps IPS throughput		
	h. 700 Mbps UTM throughput		
	i. 1000 Mbps AV throughput		
	k. 400 Mbps IPSec VPN throughput		
	h. 4Gb of Flash.		
1.6	The proposed solution should support unrestricted user/node license.		
1.7	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.		
1.8	The proposed solution must support User based policy configuration for security and Internet management.		
1.9	The proposed solution should provide on-appliance reports based not only on IP addresses but also based on users.		
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, 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		
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.		
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.		
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.		
INTRUSION PREVENTION SYSTEM			
6.1	The proposed solution should be WestCoast Labs Checkmark certified.		
6.2	The proposed solution should have signature-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 proposed 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.		
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, 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 personalized 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, suspicious 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, Recipient & Virus Names.		
7.17	The proposed solution should have a virus detection rate of above 98%.		
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 recipient		
	e. Deliver the mail to recipient		
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, Recipient 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.		
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+ URLs categorized 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 access 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 Messaging (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.		
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 certificate 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.		
LOGGING AND REPORTING			
11.01	The proposed solution must support Four Eye (4-Eye) authentication to comply with Internet Privacy laws		
11.02	The proposed solution must have On-Appliance, integrated reporting solution.		
11.03	The proposed solution should be able to be integrated with iView reporting solution.		
11.04	The proposed solution should support minimum 1000+ drill down reports.		
11.05	The proposed solution should allow exporting of reports in PDF and Excel format.		
11.06	The proposed solution should support logging of Antivirus, Antispam, Content Filtering, Traffic discovery, IPS, Firewall activity on syslog		

	server.		
11.07	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.		
11.08	The proposed solution should provide data transfer reports on the basis of application, username, IP address.		
11.09	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.		
APPLICATION FILTERING SOLUTION			
12.01	The proposed solution must provide inbuilt Application Filtering solution		
12.02	The proposed solution must identify (Allow/Block/Log) the applications regardless of port, protocols, encryption including SSL/TLS.		
12.03	The proposed solution should have be able to control 1500+ applications.		
12.04	The proposed solution's application database must get updated automatically without any manual intervention		
12.05	The proposed solution must give Identity based reports (username along with IP)		
12.06	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		
12.07	The proposed solution must be capable of identifying hidden applications running over standard ports (80, 443, 22 etc)		