

NATIONAL BUREAU OF FISH GENETIC RESOURCES

CANAL RING ROAD, P.O. DILKUSHA,

LUCKNOW-226002 , U.P. INDIA,

PHONE: 91-(0522) 2442440, 2442441; FAX: 91-(0522) 2442403

E-mail: nbfgr@sancharnet.in

ANNEXURE -1

Sr. No.	Name of the Equipment	Quantity required
01	Unified Threat Management	01 Nos.

Technical Specifications for: Unified Threat Management

Sr. No.	Specification
1.1	Product or OEM must be ISO 9001-2000 certified and vendors participating into the bid must have OEM authorization certificate from the manufacturer.
1.2	Regional presence for sales & support
1.3	Appliance supports inbuilt hdd for storage of logs & reports
1.4	Appliance comply FCC and CE norms
1.5	The proposed solution matches following criteria. a. Hardware platform must be 64 bit b. 6 number of 10/100/1000 interface with hardware Bypass c. 10000 number of new connection d. 400000 number of concurrent connection e. 1000 Mbps (TCP) Firewall throughput f. 300 Mbps IPS throughput g. 150 Mbps UTM throughput
1.6	Unrestricted user/node license
1.7	Works as standalone HTTP proxy server with integrated Firewall, Antivirus, Anti-Spam, Content filtering, IPS.
1.8	Supports User based policy configuration for security & internet management.
1.9	Reports based on user not only on the base of IP address.
Administration, Authentication & General Configuration	
2.1	Support administration via secured communication over HTTPS, SSH and from Console.
2.2	Able to export and import configuration backup including user objects
2.3	Supports Route (Layer 3)/transparent mode (Layer 2)
2.4	Supports integration with Windows NTLM, Active Directory, LDAP, Radius or Local Database for user authentication.
2.5	Supports automatic transparent Single Sign on (AS SO) for user authentication. SSO must be proxy independent and support all applications for authentication,
2.6	Supports Dynamic DNS configuration
2.7	Provides bandwidth utilization graph on daily, weekly, monthly or yearly for total or individual ISP link.
2.8	Provides real time data transfer/bandwidth utilization done by individual user/ip/application.
2.9	Supports Parent Proxy with IP/FQDN support
2.10	Supports NTP
2.11	Supports user/ip/mac binding functionality to map username with IP address & MAC address for security reason
2.12	Multilingual support for Web admin console
2.13	Supports Version roll back functionality
2.14	Supports session time out & Idle time out facility to forcefully logout the users.
2.15	Supports ACL based user creation for administration purpose
2.16	Supports LAN bypass facility in case appliance is configured in Transparent mode.

2.17	Supports inbuilt PPPOE client and should be capable to automatically update all required configuration whenever PPPOE get changed
2.18	Supports SNMP v1, v2c & v3
2.19	Firmware based instead of normal software with capability to keep three firmware instant roll back.
2.20	Provides flexible, granular role-based GUI administration
2.21	Provides support of multiple authentication servers for each module (Firewall, Different type of VPN)
2.22	Supports 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	Supports load balancing & failover for more than 2 ISP
3.2	Supports explicit routing based on Source, Destination, Username, Application.
3.3	Supports weighted round robin algorithm for Load balancing
3.4	Option to create failover condition on ICMP, TCP or UDP protocol to detect failed ISP connection
3.5	Sends alert email to admin on change of gateway status
3.6	Active/Active (Round Robin) and Active/Passive gateway load balancing and failover support
High Availability	
4.1	Supports High Availability Active/Passive or Active/Active support
4.2	ICSA certified High Availability solution
4.3	Sends notification to admin on change of appliance status in High Availability
4.4	Encrypted HA traffic between two peers
4.5	Supports Link, device & Session failure
4.6	Automatic & manual synchronization between appliances in cluster
Firewall	
5.1	Standalone appliance with hardened OS
5.2	ICSA & Webcoast checkmark certified firewall
5.3	Supports stateful inspection with user based one-to-one & dynamic NAT, PAT
5.4	Must support user identity as matching criteria along with Source/Destination IP/Subnet group, destination port in firewall rule
5.5	Facilitates 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	Supports user defined multi zone security architecture
5.7	Have predefine application based on port/Signature & also support creation of custom application based on port/protocol number
5.8	Supports inbound NAT load balancing
5.9	802.1q VLAN tagging support
5.10	Supports 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	Provides alert message on Dash Board whenever default password is not changed, non-secure access is allowed & module subscription is expiring.
5.13	Provides Mac Address (Physical Address) based firewall rule to provide OSI Layer 2 to Layer 7 security
5.14	Supports IPv6 as per www.ipv6ready.org guidelines
5.15	Supports 3G UMTS, GSM, GPRS modem via USB interface for VPN and Gateway Failover - Load Balancing
IPS	
6.1	Whether webcoast checkmark certified.
6.2	Have sing nature based and protocol anomaly based Intrusion prevention system.
6.3	Have 3500+ signature databases
6.4	Supports creation of custom IPS signature.
6.5	Must support creation of multiple IPS policy for different zone instead of blanket policy at interface

	level.
6.6	Must support configuration option to disable/enable category/signature to reduce the packet latency.
6.7	Gives username along with IP in IPS alerts and reports
6.8	Automatically takes update from update server.
6.9	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	Able to detect & block known P2P based instant messaging application like skype & known chat application like WLM, Rediffbol etc.
6.11	Should generate the alerts for attacks
6.12	Should generate historical reports based on top alerts, top attackers, severity wise, top victims, protocol wise.
Gateway Antivirus	
7.1	Should have an integrated Antivirus solution.
7.2	Should have webcoast checkmark certification for Antivirus/Anti Spyware.
7.3	Must works SMTP proxy not as MT A or relay server.
7.4	Supports 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 Phishing, spyware.
7.6	Should have facility to add signature/ disclaimer in mails.
7.7	The proposed solution must support-on appliance quarantined facility and also personalized 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, suspicious or protected attachments mails. a. Drop mail b. Deliver the mail without attachment c. Deliver original mail d. Notify to administrator
7.10	Should support multiple antivirus policy for sender/recipient email address or address group for notification setting, quarantine setting & file extension setting instead of single blanket policy
7.11	Should update the signature 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 attachment & send notification to recipient & 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	Should provide historical reports based on username, IP address, Sender, Recipient & Virus Names.
7.17	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	Should support RBL database for spam detection.
8.6	Must support mail archive option to keep copy of incoming & outgoing mails to administrator defined email address.
8.7	Should have multiple configurable policy for email id/address group for quarantine setting, different actions instead of blanket policy.
8.8	Must support on appliance quarantined facility and also personalized user based quarantine area with email release option

8.9	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 recipient
8.11	The proposed solution should support IP/Email address white list/Black list facility.
8.12	Should support option to enable/ disable antispam scanning for SMTP authenticated traffic.
8.13	Should support spam detection using Recurrent pattern detection technology (RPD) to identify spam out breaks.
8.14	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	Should provide historical reports based on username, IP address, Sender, Recipient & spam category.
8.17	Must provide Anti-Spam Message Digest feature per user.
8.18	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	Should be webcoast checkmark certified.
9.2	Should be integrated solution with local database instead of querying to database hosted somewhere on the internet.
9.3	Must work as Standalone HTTP proxy.
9.4	Must have 82+ web category with 40 Million URL database.
9.5	Must have following features in built 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 websites 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	Should support application control blocking features as follows 9.7a. Should able to block known Chat application like Yahoo, MSN, AOL, Google, Rediff, Jabber etc 9.8b. Should support blocking of File transfer on known Chat application and FTP protocol.
9.9	Must block HTTP or HTTPS base anonymous proxy request available on the internet.
9.10	Should provide option to customize Access denied message for each category.
9.11	Should be CIPA compliant and should have predefined CIPA based internet access policy.
9.12	Should be able to identify traffic based on Productive, Neutral, unhealthy & non-working websites as specified by admin.
9.13	Should have specific categories that would reduce employee productivity, bandwidth choking sites and malicious websites.
9.14	Should able to generate reports based on username, IP address, URL, groups, categories & category type.
9.15	The proposed solution should block image based spam mails i.e. email message with text embedded in a image file.
9.16	Should support creation of cyclic policy on Daily/ Weekly/ Monthly/ Yearly basis for internet access on individual users/group of users.
9.17	Should support creation of internet access time policy for individual users or on group basis.
9.18	Should support creation of Data transfer policy on daily/ weekly/ monthly/ yearly basis for individual user or group basis.
9.19	Should support creation of cyclic data transfer policy on Daily/weekly/Monthly/yearly basis for

	individual user or on group.
9.20	Should have integrated bandwidth management.
9.21	Should able to set guaranteed and burstable bandwidth per User/IP/Application on individual or shared basis
9.22	Should provide option to set different level of priority for critical application.
9.23	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	Must provide web category based bandwidth management and prioritization.
9.25	Must provide logging and extensive controls on Instant Messaging (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. Achieve of transferred files. 4. Antivirus scanning on file transferred.
VPN	
10.1	Should be webcoast checkmark certified.
10.2	Should be VPNC Basic interop & AES interop certified.
10.3	Should support Ipsec (Net-to-Net, Host-to-Host, Client-to-site), L2tp & PPTP VPN connection.
10.4	Should support DES, 3DES, AES, Twofish, Blowfish, Serpent encryption algorithm.
10.5	Should support Preshared keys & Digital certificate based authentication. The proposed solution should also support Main mode & Aggressive mode for phase 1 negotiation.
10.6	Should support external certificate authorities.
10.7	Should support export facility of Client-to-site configuration for hassle free VPN configuration in remote Laptop/Desktop.
10.8	Should support commonly available Ipsec VPN clients.
10.9	Should support local certificate authority & should support create/ renew/ Delete self-signed certificate.
10.10	Should support VPN failover for redundancy purpose where more than one connection are in group & if one connection goes down it automatically switch over to another connection for zero downtime.
10.11	Have preloaded third party certificate authority including Verisign/Entrust.net Microsoft and provide facility to upload any other certificate authority.
10.12	Forwards logging information of all modules to syslog servers.
10.13	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	Must have On-Appliance integrated View reporting solution.
11.2	The proposed solution should support minimum 1000+ drill down reports.
11.3	The proposed solution should provide reports in HTML, CSV, PDF, Excel & graphical format.
11.4	Supports logging of Antivirus, Antispam, content filtering, Traffic discovery, IPS, Firewall activity on syslog server.
11.5	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	Provides data transfer reports on the based of application, username, IP address.
11.7	Provides connection wise reports for user, source IP, destination IP, source port, destination port or protocol.
11.8	Facility to send reports on mail address or on FTP server.
11.9	Provides approximate 45 regulatory compliance reports for SOX, HIPPA, PCI, FISMA and GLBA compliance.
11.10	Supports Auditing facility to track all activity carried out Security appliance.
11.11	Supports multiple syslog servers for remote logging.
11.12	Forwards logging information of all modules to syslog servers.

11.13	Have configurable option for email alerts/automated Report scheduling.
11.14	Able to provide detailed reports about all mails passing through the firewall.
11.15	Provides reports for all blocked attempts done by users Ip address.
11.16	Must be capable to derive logs and reports of proprietary devices including UTMs, Proxy Firewalls, Custom Applications and Syslog-compatible devices.
11.17	Must be capable to provide Multiple Dashboard Report along with custom to customize the dashboards.
11.18	The in built 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.
Warranty	
12.1	Three years (3) comprehensive onsite warranty on labour, hardware parts and software
	Free upgrade/ update of software in warranty period
Amount/ Price details (in Indian Rupees)	
	Price of whole unit
	Price of Hardware component
	Price of Software component (Pl. give the price of each software component)
	Annual Renewal price for Software update/ upgrade/ license (separately for each software component)
	Annual Maintenance charge/ price of unit after expiry of warranty
	a. Hardware
	b. Software (Separately for each software component)
	Total

Administrative Officer

NATIONAL BUREAU OF FISH GENETIC RESOURCES
CANAL RING ROAD, P.O. DILKUSHA,
LUCKNOW-226002 , U.P. INDIA,
PHONE: 91-(0522) 2442440, 2442441; FAX: 91-(0522) 2442403
E-mail: nbfgr@sancharnet.in

ANNEXURE -II

Technical Compliance Statement of Equipment for: Unified Threat Management

Sr. No.	Specification	Yes/No.
1.1	Product or OEM must be ISO 9001-2000 certified and vendors participating into the bid must have OEM authorization certificate from the manufacturer.	
1.2	Regional presence for sales & support	
1.3	Appliance supports inbuilt hdd for storage of logs & reports	
1.4	Appliance comply FCC and CE norms	
1.5	The proposed solution matches following criteria. a. Hardware platform must be 64 bit b. 6 number of 10/100/1000 interface with hardware Bypass c. 10000 number of new connection d. 400000 number of concurrent connection e. 1000 Mbps (TCP) Firewall throughput f. 300 Mbps IPS throughput g. 150 Mbps UTM throughput	
1.6	Unrestricted user/node license	
1.7	Works as standalone HTTP proxy server with integrated Firewall, Antivirus, Anti-Spam, Content filtering, IPS.	
1.8	Supports User based policy configuration for security & internet management.	
1.9	Reports based on user not only on the base of IP address.	
Administration, Authentication & General Configuration		
2.1	Support administration via secured communication over HTTPS, SSH and from Console.	
2.2	Able to export and import configuration backup including user objects	
2.3	Supports Route (Layer 3)/transparent mode (Layer 2)	
2.4	Supports integration with Windows NTLM, Active Directory, LDAP, Radius or Local Database for user authentication.	
2.5	Supports automatic transparent Single Sign on (AS SO) for user authentication. SSO must be proxy independent and support all applications for authentication,	
2.6	Supports Dynamic DNS configuration	
2.7	Provides bandwidth utilization graph on daily, weekly, monthly or yearly for total or individual ISP link.	
2.8	Provides real time data transfer/bandwidth utilization done by individual user/ip/application.	
2.9	Supports Parent Proxy with IP/FQDN support	
2.10	Supports NTP	
2.11	Supports user/ip/mac binding functionality to map username with IP address & MAC address for security reason	
2.12	Multilingual support for Web admin console	
2.13	Supports Version roll back functionality	
2.14	Supports session time out & Idle time out facility to forcefully logout the users.	
2.15	Supports ACL based user creation for administration purpose	
2.16	Supports LAN bypass facility in case appliance is configured in Transparent mode.	
2.17	Supports inbuilt PPPOE client and should be capable to automatically update all required configuration whenever PPPOE get changed	

2.18	Supports SNMP v1, v2c & v3	
2.19	Firmware based instead of normal software with capability to keep three firmware instant roll back.	
2.20	Provides flexible, granular role-based GUI administration	
2.21	Provides support of multiple authentication servers for each module (Firewall, Different type of VPN)	
2.22	Supports 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	Supports load balancing & failover for more than 2 ISP	
3.2	Supports explicit routing based on Source, Destination, Username, Application.	
3.3	Supports weighted round robin algorithm for Load balancing	
3.4	Option to create failover condition on ICMP, TCP or UDP protocol to detect failed ISP connection	
3.5	Sends alert email to admin on change of gateway status	
3.6	Active/Active (Round Robin) and Active/Passive gateway load balancing and failover support	
High Availability		
4.1	Supports High Availability Active/Passive or Active/Active support	
4.2	ICSA certified High Availability solution	
4.3	Sends notification to admin on change of appliance status in High Availability	
4.4	Encrypted HA traffic between two peers	
4.5	Supports Link, device & Session failure	
4.6	Automatic & manual synchronization between appliances in cluster	
Firewall		
5.1	Standalone appliance with hardened OS	
5.2	ICSA & Webcoast checkmark certified firewall	
5.3	Supports stateful inspection with user based one-to-one & dynamic NAT, PAT	
5.4	Must support user identity as matching criteria along with Source/Destination IP/Subnet group, destination port in firewall rule	
5.5	Facilitates 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	Supports user defined multi zone security architecture	
5.7	Have predefine application based on port/Signature & also support creation of custom application based on port/protocol number	
5.8	Supports inbound NAT load balancing	
5.9	802.1q VLAN tagging support	
5.10	Supports 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	Provides alert message on Dash Board whenever default password is not changed, non-secure access is allowed & module subscription is expiring.	
5.13	Provides Mac Address (Physical Address) based firewall rule to provide OSI Layer 2 to Layer 7 security	
5.14	Supports IPv6 as per www.ipv6ready.org guidelines	
5.15	Supports 3G UMTS, GSM, GPRS modem via USB interface for VPN and Gateway Failover - Load Balancing	
IPS		
6.1	Whether webcoast checkmark certified.	
6.2	Have signature based and protocol anomaly based Intrusion prevention system.	
6.3	Have 3500+ signature databases	
6.4	Supports creation of custom IPS signature.	
6.5	Must support creation of multiple IPS policy for different zone instead of blanket policy at	

	interface level.	
6.6	Must support configuration option to disable/enable category/signature to reduce the packet latency.	
6.7	Gives username along with IP in IPS alerts and reports	
6.8	Automatically takes update from update server.	
6.9	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	Able to detect & block known P2P based instant messaging application like skype & known chat application like WLM, Rediffbol etc.	
6.11	Should generate the alerts for attacks	
6.12	Should generate historical reports based on top alerts, top attackers, severity wise, top victims, protocol wise.	
Gateway Antivirus		
7.1	Should have an integrated Antivirus solution.	
7.2	Should have webcoast checkmark certification for Antivirus/Anti Spyware.	
7.3	Must works SMTP proxy not as MT A or relay server.	
7.4	Supports 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 Phishing, spyware.	
7.6	Should have facility to add signature/ disclaimer in mails.	
7.7	The proposed solution must support-on appliance quarantined facility and also personalized 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, suspicious or protected attachments mails. a. Drop mail b. Deliver the mail without attachment c. Deliver original mail d. Notify to administrator	
7.10	Should support multiple antivirus policy for sender/recipient email address or address group for notification setting, quarantine setting & file extension setting instead of single blanket policy	
7.11	Should update the signature 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 attachment & send notification to recipient & 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	Should provide historical reports based on username, IP address, Sender, Recipient & Virus Names.	
7.17	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	Should support RBL database for spam detection.	
8.6	Must support mail archive option to keep copy of incoming & outgoing mails to administrator defined email address.	
8.7	Should have multiple configurable policy for email id/address group for quarantine setting, different actions instead of blanket policy.	

8.8	Must support on appliance quarantined facility and also personalized user based quarantine area with email release option	
8.9	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 recipient	
8.11	The proposed solution should support IP/Email address white list/Black list facility.	
8.12	Should support option to enable/ disable antispam scanning for SMTP authenticated traffic.	
8.13	Should support spam detection using Recurrent pattern detection technology (RPD) to identify spam out breaks.	
8.14	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	Should provide historical reports based on username, IP address, Sender, Recipient & spam category.	
8.17	Must provide Anti-Spam Message Digest feature per user.	
8.18	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	Should be webcoast checkmark certified.	
9.2	Should be integrated solution with local database instead of querying to database hosted somewhere on the internet.	
9.3	Must work as Standalone HTTP proxy.	
9.4	Must have 82+ web category with 40 Million URL database.	
9.5	Must have following features in built 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	Should support application control blocking features as follows 9.7a. Should able to block known Chat application like Yahoo, MSN, AOL, Google, Rediff, Jabber etc 9.8b. Should support blocking of File transfer on known Chat application and FTP protocol.	
9.9	Must block HTTP or HTTPS base anonymous proxy request available on the internet.	
9.10	Should provide option to customize Access denied message for each category.	
9.11	Should be CIPA compliant and should have predefined CIPA based internet access policy.	
9.12	Should be able to identify traffic based on Productive, Neutral, unhealthy & non-working websites as specified by admin.	
9.13	Should have specific categories that would reduce employee productivity, bandwidth choking sites and malicious websites.	
9.14	Should able to generate reports based on username, IP address, URL, groups, categories & category type.	
9.15	The proposed solution should block image based spam mails i.e. email message with text embedded in a image file.	
9.16	Should support creation of cyclic policy on Daily/ Weekly/ Monthly/ Yearly basis for	

	internet access on individual users/group of users.	
9.17	Should support creation of internet access time policy for individual users or on group basis.	
9.18	Should support creation of Data transfer policy on daily/ weekly/ monthly/ yearly basis for individual user or group basis.	
9.19	Should support creation of cyclic data transfer policy on Daily/weekly/Monthly/yearly basis for individual user or on group.	
9.20	Should have integrated bandwidth management.	
9.21	Should able to set guaranteed and burstable bandwidth per User/IP/Application on individual or shared basis	
9.22	Should provide option to set different level of priority for critical application.	
9.23	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	Must provide web category based bandwidth management and prioritization.	
9.25	Must provide logging and extensive controls on Instant Messaging (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. Achieve of transferred files. 4. Antivirus scanning on file transferred.	
VPN		
10.1	Should be webcoast checkmark certified.	
10.2	Should be VPNC Basic interop & AES interop certified.	
10.3	Should support Isec (Net-to-Net, Host-to-Host, Client-to-site), L2tp & PPTP VPN connection.	
10.4	Should support DES, 3DES, AES, Twofish, Blowfish, Serpent encryption algorithm.	
10.5	Should support Preshared keys & Digital certificate based authentication. The proposed solution should also support Main mode & Aggressive mode for phase 1 negotiation.	
10.6	Should support external certificate authorities.	
10.7	Should support export facility of Client-to-site configuration for hassle free VPN configuration in remote Laptop/Desktop.	
10.8	Should support commonly available Isec VPN clients.	
10.9	Should support local certificate authority & should support create/ renew/ Delete self-signed certificate.	
10.10	Should support VPN failover for redundancy purpose where more than one connection are in group & if one connection goes down it automatically switch over to another connection for zero downtime.	
10.11	Have preloaded third party certificate authority including Verisign/Entrust.net Microsoft and provide facility to upload any other certificate authority.	
10.12	Forwards logging information of all modules to syslog servers.	
10.13	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	Must have On-Appliance integrated View reporting solution.	
11.2	The proposed solution should support minimum 1000+ drill down reports.	
11.3	The proposed solution should provide reports in HTML, CSV, PDF, Excel & graphical format.	
11.4	Supports logging of Antivirus, Antispam, content filtering, Traffic discovery, IPS, Firewall activity on syslog server.	
11.5	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	Provides data transfer reports on the based of application, username, IP address.	

11.7	Provides connection wise reports for user, source IP, destination IP, source port, destination port or protocol.	
11.8	Facility to send reports on mail address or on FTP server.	
11.9	Provides approximate 45 regulatory compliance reports for SOX, HIPPA, PCI, FISMA and GLBA compliance.	
11.10	Supports Auditing facility to track all activity carried out Security appliance.	
11.11	Supports multiple syslog servers for remote logging.	
11.12	Forwards logging information of all modules to syslog servers.	
11.13	Have configurable option for email alerts/automated Report scheduling.	
11.14	Able to provide detailed reports about all mails passing through the firewall.	
11.15	Provides reports for all blocked attempts done by users Ip address.	
11.16	Must be capable to derive logs and reports of proprietary devices including UTM's, Proxy Firewalls, Custom Applications and Syslog-compatible devices.	
11.17	Must be capable to provide Multiple Dashboard Report along with custom to customize the dashboards.	
11.18	The in built 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.	
Warranty		
12.1	Three years (3) comprehensive onsite warranty on labour, hardware parts and software	
	Free upgrade/ update of software in warranty period	
Amount/ Price details (in Indian Rupees)		
	Price of whole unit	
	Price of Hardware component	
	Price of Software component (Pl. give the price of each software component)	
	Annual Renewal price for Software update/ upgrade/ license (separately for each software component)	
	Annual Maintenance charge/ price of unit after expiry of warranty	
	a. Hardware	
	b. Software (Separately for each software component)	
	Total	

Mark (YES) if specification offered is as per tender or better. If not, specify the specification offered.

An item-by-item commentary on the purchaser's Technical Specifications demonstrating substantial responsiveness of the goods and services to those specifications or a statement of deviations and exceptions to the provision of the Technical Specifications.

(Technical literature/brouchers/manuals should be attached along with this format)

Please Note:-

1. Compliance/Deviation statement comparing the specification of the quoted model to the required specifications. This statement should also give the last page of the technical literature where the relevant specification is mentioned.
2. Bids must have supporting documents (technical) literature of copies of relevant pages from the service manual or factory test (data) for the points noted above, failure regarding which may result in rejection of bid.

SIGNATURE WITH STAMP OF THE BIDDERS

NATIONAL BUREAU OF FISH GENETIC RESOURCES

CANAL RING ROAD, P.O. DILKUSHA,

LUCKNOW-226002, U.P. INDIA,

PHONE: 91-(0522) 2442440, 2442441; FAX: 91-(0522) 2442403

E-mail: nbfg@sancharnet.in

(to be returned by Bidders along with the tender duly completed and signed)

Name of Item:

Quantity:

Sr. No.	Description	Quantity	Unit Rate	Total

Gross total cost Rs. _____ (in Figures) (Rupees _____)

_____ (in words).

We agree to supply the above goods in accordance with the Technical specifications for a total

Contract price of Rs. _____ (in figures) (Rupees _____)

_____ (in words) within the period

Specified in the invitation for Quotations.

We also confirm that the normal commercial warranty/guarantee of _____ months shall apply to the offered goods.

(Bidder)

Name: _____

Signature: _____

Date: _____