GOVERNMENT POLYTECHNIC PANAJI
ALTINHO, PANAJI-GOA
STORES & PURCHASE SECTION
Tel no.: 0832-2432667 **Website: www.gpp-goa.gov.in**
Email id: ppl-gpp.goa@nic.in gppstores@rediffmail.com
GSTIN No. 30BLRG06032F1DN TAN No. BLRG06032F

GOA@60

No.19/11/2019/SP/ Date: 05/04/2021

Tender fee: ₹ 500/-

TENDER ENQUIRY

Sealed quotations are invited by the Principal, Government Polytechnic Panaji, super scribed on the envelope as **"QUOTATION FOR SUPPLY, INSTALLATION & COMMISSIONING OF NETWORK FIREWALL"**

The sealed quotation along with EMD & Tender Fee shall reach this Office on or before **30/04/2021** up to 3.00 p.m.

The quotation is subject to Terms and conditions attached herewith. The Quotation will be opened at 3.30 p.m. on the scheduled due date mentioned above in the presence of those vendors who remain present at the time of opening.

Please find the following enclosed documents of the tender:

1. Terms & Conditions.
2. Certificate & Checklist.
3. Annexure (Description of items).

Yours faithfully,

(L.R. Fernandes)
Principal

Copy to:
1. The I/c HOD, Computer Engg. Dept., GPP.
2. The Asst. Accounts Officer, GPP.
3. Office file.

Tender Notice No. :-

Due Date :-

CERTIFICATE

Certified that I/We have gone through the terms and conditions of supply/works and also the tender conditions. I/We hereby agree to abide by the same. In token of acceptance as above I/We affix the signature as below:-

.....

Signature & Seal of the tenderer

Name:- .....

Date :- .....

CHECKLIST

Sr. no.	Submission compliance	Yes/No
1.	Quotation for the items mentioned in Annexure	
2.	Certificate	
3.	Brochures/product literature for the items quoted	
4.	GST registration document	
5.	Manufacturer Authorization letter	
6.	EMD Demand draft (2% of quoted amount)	
7.	Rs.500/- Demand draft as tender fee (non-refundable)	

Signature & Seal of tenderer

NB: The duly filled and signed Certificate & Checklist shall be submitted along with the quotation, without which the tender will not be considered.

a) Where the cost of the item is specified as exclusive of these statutory levies, unless

TERMS AND CONDITIONS

(Subject to legal jurisdiction of Goa)

Tender Conditions:-

1. A) The Principal, Government Polytechnic Panaji, reserves the right to reject all or any of the tenders without assigning any reasons.

   B) Irrespective of whether mention was made in the Notice inviting tenders or otherwise only registered manufacturers or the authorized dealers of the manufacturers who are also registered under the Goods & Service Tax Act, are eligible to submit tenders.

   C) These who are submitting tenders for the first time, shall invariably enclose documentary evidence in support of the status described at (B) above, failing which such tenders/quotations shall be rejected.

   D) Exempt where exemption is granted by the Government of Goa, Earnest Money Deposit (E.M.D.) of 2% of the quoted rates of items shall be enclosed which will be forfeited if the tenderer fails to honour the supply order if and when placed.

   E) If the tenderer desires, he/she will be permitted to be present at the time of opening of the tenders.

   F) The E.M.D. is refundable in case of unsuccessful tenderer & in case of tenders which are acceptable the EMD shall be adjusted against the security deposit which shall be 5% of the order value.

   G) The tenderer shall not be entitled to any interest/compensation in case EMD/SD the same is not returned in time.

   H) The Earnest Money Deposit will be forfeited to the Government if the tenderer fails to honour the order placed and the S.D. will be forfeited to the Government if the tenderer fails to execute the entire supply within the stipulated time.

   H a) The Earnest Money will be liable to be forfeited, if the tenderer withdraws or amends impairs derogates the tender in any respect within the period of availability of his tender.

   I) This office will take all the care to return within the reasonable time which is normally 30 days after opening of the tenders in case of EMD and fifteen days for Security Deposit after satisfactory and full execution of the order and on acceptance of the stores by the Principal, Government Polytechnic Panaji. However if the supplies are covered by warranty period the EMD/SD shall be retained till the warranty period is over.

   J) If the tenderer to claim the EMD/SD within the period of 3 months from the time limit specified above such EMD/SD will be deposited in to the Government treasury at the full risk of the supplier and the Principal shall not be responsible for delay if any to reclaim/return the same.

   K) Tenders submitted without the prescribed form and/or without tender cost amount so also the tenders posted in any other envelopes other than the prescribed envelops shall be supplied along with tender forms.

   L) EMD/SD shall invariably be in the form of Demand Draft made in favour of the Principal, Government Polytechnic Panaji drawn on any nationalized bank. The EMD/SD in any other forms other than the specified above shall not be accepted and tenders accompanied by such EMD shall be rejected.

   M) All tenders received after the due date and/or time shall be rejected. Postal delay if any shall not an excuse for the late receipt of the tenders.

   N) All tenders/quotations shall be neatly typed; overwriting and corrections if any shall be authenticated by the tenderer. Incomplete or illegible tenders/quotations are liable to be rejected without assigning any reasons.

   O) Where applicable following details shall be clearly and specifically indicated by the tenderer.

      (i) Disagreement, if any, with terms and conditions enclosed.
      (ii) Non conformity, if any, of the stores with the specifications given in the tender notice/tender paper.
      (iii) Taxes, Excise Duty, Custom Duty etc. if any to be paid extra.
      (iv) Freight, forwarding, Insurance and Hamali charges, if any to be paid extra.

   P) Taxes & duties.

   a) Where the cost of the item is specified as exclusive of these statutory levies, unless accepted in writing otherwise by the Principal, Government Polytechnic, before placing of the order, the said levies shall be payable only on production of the prescribed documents as below.

      a. GST certificate prescribed by the Principal, Government Polytechnic Panaji.
      b. Excise duty, Gate pass – I certificate prescribed by the Principal, Government Polytechnic Panaji.
      c. Custom duty, certificate issued by the concerned custom office.
      d. Freight & Insurance :

Where the cost is exclusive of freight and Insurance charges the tenderer shall invariably provide the documentary evidence for having actually paid such charges failing which the same shall be disallowed, however, where the rates or amount was not specified in the order it shall be consistent with current market rates.

b) In case where clarity as at (O) above is not adhered to then the Principal, Government Polytechnic Panaji shall be entitled to and it shall be lawful to do so.....
   a. to accept for processing such tenders at the risk of the tenderer and/or .
   b. to reject the tender without assigning any reasons.

c) Irrespective of whether specifically stated in the tender Notice or otherwise following tenders will be rejected.
   a. Where the tenderer has not enclosed documentary evidence of being authorized manufacturer or the authorized dealer of the authorized manufacturer.
   b. Where the tenderer demands advance payment or payment through bank against invoice or similar form of advance payment.
   c. Where tender is not submitted in the prescribed tender paper.
   d. Where tender cost is not enclosed.
   e. Where the stores offered are not of standard quality make.
   f. Where the tenderer has not enclosed any printed leaflets, catalogues etc. giving detailed specification of the products.

General Conditions:-

A) Unless expressly provided in writing by the Principal, Government Polytechnic Panaji, the order placed shall be subject to the terms and conditions and the specifications given herein under and if any of the terms and conditions and/or specifications of the tenderer on whom order is placed is/or contrary or inconsistent with any of the terms and conditions of these terms and conditions, same shall be deemed to be and shall be treated as in applicable and of no effect.

B) Any typographical/clerical error in relation to rates/units/quantity size etc. and/or contradicting/conflicting with the tender specifications and or the terms and conditions shall stand corrected to that effect without any written communication and the tenderer shall not be entitles to any claim what-so-ever, based on such typographical/clerical error.

C) The tenderer shall sign with date on the certificate attached in token of acceptance of the terms and conditions without any reservations and affix the rubber seal or office stamp if available where rubber stamp is not available name of the person who has signed and the tenderer which he/she represents shall be clearly written in ink, quotations/tenders received without being duly signed and stamped are liable to be rejected without assigning any reasons. However, the Principal, Government Polytechnic, Panaji in the public interest any relax this condition.

D) Each and every quotation/tender shall necessarily be accompanied by printed leaflets or catalogues giving complete details of the specifications of the stores. Tenders/quotations stating 'as per your specifications' or just repeating what is already in the tender paper MAY NOT be considered at all.

Validity of Rates :-

A) The rates quoted should be valid for a period of 180 days from the date of opening of the tender.

B) Rates quoted shall be generally exclusive of transport, loading and unloading charges, excise, taxes, etc. However these and other charges/taxes shall clearly be shown separately otherwise it will be deemed that rates quoted are inclusive of all charges/taxes.

C) The rates shall approximately conform to the current market rates specified by Government/Government approved appropriate agencies where applicable. In case, if at any stage it is discovered that the rates quoted by the tenderer are/were not conforming to the then prevailing market rates, in such cases Principal, Government Polytechnic, except the actual cost of stores as per normal rates less whatever penalty levied by Principal, Government Polytechnic Panaji and for this purpose "Normal Rates" means the actual cost of the stores on par with market rates of similar stores exclusive of taxes, excise, transport, freight etc. plus reasonable profit margin acceptable as decided by the arbitrator, see clause no.9.

4. Execution of Order :-

A) Acceptance of the order shall be conveyed by the tenderer by submitting a Security Deposit equivalent to 5% of the value of the order, within 15 days from the date of receiving order, in the form of Bank call Deposit Receipt/demand Draft drawn in favour of the Principal, Government Polytechnic, Panaji on any Nationalized Bank, failing which the order shall stand cancelled unless informed otherwise in writing by the Principal.

B) The Security Deposit will be refunded to the supplier after full execution of the order or on expiry of the period specified in the order and where the stores are under warranty, the S.D. shall be returned after expiry of such warrantee period. If the supplier fails to honour the warrantee as agreed, the S.D. will be forfeited.

C) Entire order shall be executed within six weeks from the date of issue unless specified otherwise, in the order. However Principal, Government Polytechnic, Panaji reserves the right to grant the extension of the time limit, if in his opinion public interest does not suffer, Violation of this clause attracts provisions of clauses 5 (i) (ii) (iii) .

D) The stores shall be properly packed and dispatched insured if necessary with any Indian Government approved Insurance Company or its branch at a cost consistent with Government regulations and the cost of the consignment against loss, damages or breakage etc. upto destination by goods/Passengers Train/Road Transport on freight paid basis only.

E) It shall be primarily the responsibility of the tenderer to in-respect and satisfy that the stores to be supplied exactly conform to the specifications given in the order. In case of lapse on the part of the tenderer in this regard the Principal, Government Polytechnic Panaji reserves the right to reject the stores.

F) In case of rejection of the stores supplied by the tenderer on the grounds specified above at D & E. or if found defective or not conforming to specifications or any other grounds in accordance with the terms and conditions, it shall be the responsibility of the tenderer to make arrangement to collect back the stores.

G) If the tenderer so desires the rejected stores may be dispatched back to the tenderer provided.

i) The tenderer gives undertaking in the prescribed from accepting full responsibility for losses/damages which may be caused during transit due to accidents or any other reasons.

ii) The tenderer shall send on advance payment for packing, forwarding and transport charges by way of Demand Draft drawn in favour of the Principal Government Polytechnic, Panaji payable at Panaji on any Nationalised Bank.

5. The (delivery period stipulated) is essence of the contract. In case the tenderer fails to deliver the stores or any part thereof within the stipulated period of delivery or in case the stores are found not to be in accordance with the specifications, the Principal, Government Polytechnic, Panaji shall have the right to exercise his discretionary powers as under :-

i) either to recover as liquidated damages a sum not exceeding half percent of the price of stores which the tenderer has failed to deliver as aforesaid per each week or part there of during which the delivery of each stores may be in arrears but subject to a maximum limit of 5 % of the stipulated cost of the stores.

ii) To purchase from elsewhere at the cost and risk of the tenderer the stores, so undelivered or stores of a similar description without canceling the order in respect of the consignment not yet delivered.

iii)Or to cancel the entire/part of the order as deemed fit in the sole discretion.

6. Inspection/Acceptance of Stores :-

A) Inspection of the store shall invariably be done at the Polytechnic premises. The stores shall be deposited by the tenderer at his/her risk at the Polytechnic premises. In such cases acknowledgement will not be deemed as acceptance of the stores.

B) In case the stores are delivered in packed cases either personally or through transport agencies including Rail/Road agencies the acknowledgement given by the storekeeper shall be "On said to contain basis". In such cases the Principal, Government Polytechnic Panaji reserves the right to verify actual contents after opening and therefore, the responsibility for damaged/defectives/shortages or the consequences of a similar nature shall be solely the responsibility of the tenderer. Therefore the tenderer may prefer to give open delivery by making suitable arrangements.

C) In cases where the stores are deposited in open container/open condition the acknowledgement of the Storekeeper shall be to the extent of physical quantity and in no case the Storekeeper shall be responsible as to the exact nature/identity/conformity of the stores with the specification mentioned in the order.

D) The Storekeeper/indenting Dept. of the Government Polytechnic, shall take maximum precaution for the safety of the stores in their custody. However in case of loss/losses caused to the stores deposited by the tenderer in the Polytechnic premises due to fire, natural calamities and due to any other reasons caused beyond the human control of the Principal, Government Polytechnic Panaji. The Government shall not be responsible to make good the losses/either in full/part or to pay any compensation of whatsoever nature in that regard.

E) It shall be the responsibility of the tenderer to arrange to deliver the stores at the Polytechnic premises at Altinho, Panaji Goa, during the office hours from 9.30 a.m. to 12.30 pm. & from 2.00 pm. to 4.30 p.m. The stores dispatched by rail transport or by

other means other than the specified above may not be accepted if received after the specified office hours unless agreed to otherwise in writing by Principal, Government Polytechnic Panaji before placing of the order /before dispatch of the stores.

F) Advance intimation of the dispatch of the stores with information like mode of transport name and address of the transport agency, likely date of arrival of the stores at Polytechnic, Premises and necessary documents if any to release the consignment must be sent by the tenderer to the Principal, Government Polytechnic Panaji.

G) Where applicable Instruction/Operating manuals, literature shall be sent directly to the Stores Officer, under registered post, however if the same are sent along with the goods, will be received at the cost and risk of the supplier.

7. Warrantee/Guarantee :-

A) Unless specified otherwise in writing the machine/equipment supplied shall carry a warrantee/guarantee against manufacturing defects for a period of 12 months from the date of final acceptance of such machine or equipment by the Principal, Government Polytechnic Panaji.

B) During the warrantee/guarantee period the firm responsible for supplying the machine and/or equipment under question shall provide free repairs and servicing periodically subject to a minimum of two services in the said period failing which security Deposit will be forfeited and incase where the S.D. had been returned the firm's name will be removed from the list of approved supplier.

C) During the warrantee if it becomes essential to send/take the equipment to the works/factory of the manufacturer/supplier for replacing/and or servicing bank guarantee in the prescribed form shall be provided by manufacturer/supplier towards the cost of such equipment / machines. The bank guarantee so drawn shall be for the period for which equipment remains with the manufacturer/supplier.

8. Terms of Payment :-

A) All bills shall be drawn in the name of the Principal, Government Polytechnic Panaji only and shall be submitted in triplicate with original being affixed with revenue stamp of Rupee one.

B) Unless accepted otherwise in writing before placing of the order all payments towards the supplies will be made against valid bills only and if the equipment is found in good working condition and conforming to our specifications given in the order.

C) Normally as per Government rules the payment of bills shall be made within a period of 30 days provided the supply reaches, Government Polytechnic Panaji in the last week of the month. However in case of delays no interest shall be paid by the Principal, Government Polytechnic Panaji on whatsoever ground.

9. Arbitration Clause :-

In the event of there arising any dispute or difference of opinion concerning or touching any clause of this agreement any of the terms and conditions contained in any of the documents which are made integral part of this agreement. Such a dispute of difference of opinion shall be referred to the sole arbitration of a person appointed by the Governor of Goa and it shall be lawful for the Governor of Goa to appoint any Officer who has in the discharge of his duties as such Officer either expressed any opinion or issued any direction in the matter and the provision of the arbitration Act. 1940 shall apply to such arbitration.

ANNEXURE

Unified Threat Management System Appliance Specifications
No. of users: 500
Warranty: 3 years
Appliance Requirements
Firewall should be ICSA Labs Certified
Inbuilt Hard Drive for storage of detailed graphical Logs & Reports
Should comply FCC and CE norms
OEM should be ISO 9001-2015 Certified
Proposed solution should enforce for authentication to roaming users while accessing Internet/LAN/DMZ network
Proposed solution should have bandwidth quota and time quota for manageability of users
Proposed solution should have multicore processor based architecture and not ASIC based architecture
Firewall should be Gateway level DLP compliant
Appliance Throughput
Ethernet Interfaces 10/100/1000 - 6 numbers of 1Gbps Copper ports
Concurrent Sessions - 8500000
New Sessions/second - 135000
Firewall Throughput - 16.5 Gbps
VPN Throughput - 1.5 Gbps
UTM Throughput - 2.5 Gbps
Antivirus Throughput - 2.75 Gbps
IPS Throughput - 3 Gbps
VPN Tunnels - 4000
Ethernet Interfaces (Expandable Ports - Ethernet/Fiber 1G/Fiber 10G)
1 number of Expandable Slots
Configurable WAN/LAN/DMZ ports
Firewall Requirement
The firewall should be dedicated standalone appliance.
The firewall should be ICSA certified.
The proposed system should have HA Active-Active / Active-Passive.
The proposed system must be able to create firewall rules with username as matching criteria along with host/network group/Subnet
The proposed system should have firewall with stateful packet filtering technology & must support one-to-one and dynamic user based NAT with a facility to create rules based on usernames, Source & Destination IP address, Hosts, network, IP Range
The firewall of the proposed system should be based on a hardened OS, should be capable of delivering network protection services at all layers along with options of network gateway level antivirus, anti spam, intrusion detection and prevention, content filtering, multiple ISP load balancing, failover and VPN solutions.
The firewall of the proposed system should be able to support transparent mode, Bridge mode, layer 3 transparent proxy for Seamless deployment into an existing network without changing IP configurations in the network.
The firewall of the proposed system should provide Predefined services based on port numbers and Layer 7 application and ability to create user-definable services which can be used to define firewall rules
The proposed system must provide inbuilt PPPoE client and should be capable to automatically update all required configuration (NAT Policies, VPN Configuration, Firewall Rules) whenever PPPoE IP get changed.
The firewall of the proposed system should support 802.1q based VLAN tagging to segregate devices logically
The proposed solution should have option to configure firewall policies to block or allow rules for a particular country or for a country group.
The proposed system must provide support static & dynamic routing protocol like RIP & OSPF
the proposed solution should support Multicast forwarding.
The proposed system must provide default MAC whitelist/blacklist based filtering
The proposed system must provide support for IP-MAC Binding.
The proposed system should support zone based firewall rules.
The proposed system should support users/user group based firewall rules.
The proposed solution should support NTP.
The proposed solution should support stateful inspection bypass per firewall rule.
The proposed solution should support DHCP server.

The proposed solution should support access control list based DHCP Server.
The proposed solution should support SIP & H.323 VOIP protocols.
The proposed solution should have support for Dynamic DNS.
BYOD (Bring Your Own Device)
The proposed system should give visibility & control of mobile device.
The proposed system should be able to create firewall rules based on mobile devices.
The proposed system should be able to assign separate ISP for mobile devices.
The proposed system should be able to assign QoS policies for mobile devices.
The proposed system should be able to assign Data Leak Prevention, Application & URL filtering policies for mobile devices.
The proposed system should be able to detect & determine Data Leak Prevention policies for a same user but on different devices i.e. Mobile & PC.
The proposed system should be able to detect & determine Application filtering policies for a same user but on different devices i.e. Mobile & PC.
The proposed system should be able to detect & determine URL filtering policies for a same user but on different devices i.e. Mobile & PC.
The proposed system should be able to control internet access based on time schedule for different type of devices i.e. Mobile & PC.
The proposed system can display users login details based on the devices used to access internet.
The proposed system should be able to identify & have an option to disconnect the internet connections of the mobile devices.
The proposed system should forcefully log off the mobile devices.
The proposed system has reporting based on mobile devices & PC.
The proposed system can distinguish bandwidth based on mobile devices & PC.
Application Filtering
The proposed solution should support Application Filtering in the same UTM appliance.
The proposed solution should have inbuilt Application category database.
The proposed solution should provide visibility and control by Application for Users, Groups, IP address & Network.
The proposed solution should provide policy-based control over applications for Users, Groups, IP address & Network.
The proposed solution should provide policy-based traffic shaping by application for User, Group, IP address & Network.
The proposed solution should be able to detect & block known applications like P2P & IM.
The proposed solution should provide guaranteed and burstable bandwidth for applications.
The proposed solution should be able to detect & block known applications based on time schedule.
The proposed solution must allow/block/log the applications regardless of port, protocols & encryption (SSL/TLS).
The proposed solution should have 2500+ application database.
The proposed solution must give reports based on username / IP address.
The proposed solution should be capable to block applications like file transfer.
The proposed solution should be capable to block applications like online games.
The proposed solution should be capable to block applications like IM & web chats.
The proposed solution should be capable to block applications like P2P.
The proposed solution should be capable to block Web 2.0 applications.
The proposed solution should be capable to block applications that provide remote control.
The proposed solution should be capable to block web and software based streaming applications.
The proposed solution should be capable to block VOIP based applications.
The proposed solution should be able to identify hidden applications running over standard ports (80, 443, etc.)
Administration, Authentication & Configuration
The proposed system should support Windows NTLM Database, LDAP, RADIUS TACACS+ & single sign on (SSO) for Active Directory and in built database of the appliance for User Authentication.
The proposed system should provide Guest User Network Management System
The proposed system should provide guest users authentication via SMS
The proposed system should be able to support user mapping with single IP address for firewall authentication.
The proposed system must provide connection level details using a web interface of bandwidth used for each user/IP address/ISP.
The proposed System should support to configure syslog with option to store logs on local/remote/local + remote.
The proposed System should do Real time monitoring of data transfer done by user/IP address.

The proposed system should allow Network admin to view data consumed by each individual user in the network in real time basis.
The proposed system must send an alert to admin email address on changes of firewall configurations.
The proposed system must be able detect real time traffic reports IP address wise & user wise.
The proposed system should provide facility for Web-based & Secure console based remote administration and should have centralized configuration and device management options.
The proposed system should be able to function as SNMP agent and should be able to support all SNMP software's.
The proposed solution should have Console/WebUI/Command Line Interface support for Software/ Firmware update and status check.
The proposed solution should have option to configure Two Factor Authentication for Console/WebUI/Command Line Interface with OTP (One Time Password) option for each new session.
The proposed solution should have option to configure OTP authentication for selected WebUI admin and browsing users.
The proposed solution should have option to configure password policies based on specified constraints, for creating a password for sub-admin users. Also, it should have an option to define actions on their usage and expiry.
The proposed should be able to support high availability.
The proposed system must provide session timeout to forcefully logout user after login session gets timed out.
The proposed system must send an alert to admin email address on system health check threshold value configured.
The proposed solution should provide connection level details on the firewall dashboard for active connections.
The proposed solution should provide different firewall administrator roles.
The proposed solution should have full access & read-only admin access with multiple roles such as Restart Service, Reports, Diagnosis, Shutdown and Change Password rights.
The proposed solution should have internet diagnostic tools option available
The proposed solution should have an option to capture packet on multiple interfaces on real time with an option to filter traffic on IP address, port & protocol.
The proposed system should have full configuration backup & restore option.
The proposed system should have full configuration schedule backup on local device, email and FTP.
The proposed system should have minimum 5 full configuration schedule backup on local device.
The proposed system should allow the admin to logoff the authenticated users.
The proposed system should allow the admin to disconnect live connections of the authenticated users.
The proposed system should allow single user multiple logins based on user, group & global configuration.
The proposed system should allow integration of multiple authentication schemes.
The proposed system should allow to set priority for multiple authentication schemes.
Bandwidth Management
The proposed system must have integrated Bandwidth Management
The proposed system must be able to set bandwidth per User/IP on individual or shared basis.
The proposed system must be able to set bandwidth per User/IP on individual or shared basis.
The proposed system should provide bandwidth management on incoming & Outgoing traffic.
The proposed system must be able to create Bandwidth Policies based on applications, IP address & Users / User Group.
The proposed system should provide Users & Group wise Bandwidth allocation
The proposed system should support bandwidth management on browsing, for URL, Category & external IP.
The proposed system should support Guaranteed Bandwidth
The proposed system should support Shared Bandwidth.
The proposed system should support Protocol Based Bandwidth
The proposed system should support IP Based Bandwidth.
Intrusion Prevention/Intrusion Detection
Intrusion Prevention system should be appliance based.
The proposed system should have signature and anomaly base intrusion detection and prevention system
The proposed system should have configuration options to prevent all the common DOS and DDOS attacks like syn flood, ICMP flood, UDP flood, Ping of death. Should have prevention option for more than 30 common attacks. Real-time intrusion detection for minimum 6000+ signatures.
The IPS should be able to detect, respond to and alert any unauthorized activity. Product detects the attacks and the network misuse that represent risk to the customer.
NIDS shall be able to detect incidents that originate from inside the network perimeter as well as from outside the network perimeter and shall be able to take action on the basis of configured policies.
Support at least 6000+ or more signatures with online download support of newer signatures.
The proposed system should automatically update the attack signatures database from a central database

erver
The proposed system should be able to detect and block HTTP proxy traffic both from Content filtering solution & also from IDP
The proposed system should be able to detect and block P2P based Instant Messaging applications like Skype
Web based management through https and command line interface support
IPS shall be able to detect and shall be able to stop Pre-Attack Probes various types of TCP/UDP scanners.
The software on the IPS should support online software reconfiguration to ensure that changes made to a IDS configuration take place with immediate effect.
Product can process traffic at an acceptable rate with all of the attack signatures active.
The IPS should be able to support high availability, so that in case if the primary fails the secondary appliance will become active without any manual intervention.
IPS shall be able to be configured such that attack signature and traffic analysis focus only on all interfaces.
The IDS should be able to monitor all of the major TCP/IP protocols, including IP, Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP).
Vendor updates its attack signature database regularly and it should be configurable to update the signatures automatically without manual intervention.
E-mail alerts about the IPS attack on configured email addresses.
URL Filtering
Should support 85+ Web categories
Should support blocking of category based HTTPS sites without having to provide the URL of the site to be blocked
Should support HTTPS transparent proxy
The proposed system should support browsing proxy and gateway mode simultaneously
The proposed solution should block HTTPS URLs with complete path instead of only sites names
The proposed solution should support regex in blocking of HTTPS sites
Should enforce Google/Yahoo Images strict filtering through a web interface.
Web based management through https and command line interface support
Should have facility to block URL' based on categories
Should have restriction on per download size.
Should have local cache, for faster browsing.
Should support default site block for groups create on the firewall. This should not allow any users to visit sites till allowed.
Should support default block of all downloads.
The proposed solution should be licensed per unit as against per user.
URL database should have at least 100 million sites and 85+ categories.
URL Database should be updated regularly
Should support strict search enforcement for filtering pornographic images on Google search, Google images, yahoo search and yahoo images based on Google & yahoo safe search.
Should be able to block different categories/sites based on users.
Should have options to customize the block message information send to end users
Should have facility to schedule the configurations so that department wise browsing can be allowed or blocked.
Should have configurable policy options to block urls based on web patterns (e.g.. Mail.* to block web mail related sites)
Should have configurable policy options to define the URLs what needs to be blocked.
Should have configurable policy options to define the URL exempt list
The solution should be able to block spywares/adware's etc.
The solution should be able to block java applets, activeX as well as cookies
Browsing time restriction to single users & user Group using time quota.
Download & upload control for single users & user Group using browsing quota.
The proposed system should have an option to provide Inclusive & Exclusive browsing quota for single users & user Group
Browsing bandwidth policies can be applied on entire network, single user & user Group.
Browsing bandwidth policies can be scheduled.
Browsing bandwidth policies can be allocated to single URL/browsingCategory /External IP. (e.g. YouTube site/Audio & Video Category for YouTube/ YouTube IP can be given bandwidth of 1024kbps) for single & group users.
Browsing bandwidth policies can be routed via different gateways for single URL/browsing Category/ External IP (e.g. YouTube site/ Audio & Video Category for YouTube/YouTube IP can be routed via ISP1 & the other web browsing traffic will be routed via ISP2) for single users & user Group.
The proposed system should support IP address & username based browsing configuration

The proposed system should have browsing mode like web proxy & transparent proxy.
The proposed solution should support browsing bandwidth policies backup & restore for changes on browsing bandwidth policies.
The proposed system should support username bypass from authentication for browsing with report in transparent mode.
The proposed system should support username to IP address or username to MAC address or username to IP address & MAC address binding in transparent mode.
The proposed system should support username to IP address binding in web proxy mode.
Should have an option to white list URL's for blocked categories assigned to user group.
The proposed system should support browsing and global policy based download email alert, to the network admin.
The proposed system should support email alert on large file downloads.
Gateway Anti-Virus
Gateway level Antivirus solution should be a appliance based.
The proposed system should scan for viruses even for downloads from HTTPS sites
Embedded antivirus support. Should have option to automatically update the new virus pattern updates. AV should be supported for HTTP, HTTPS, FTP, IMAP, SMTP, SMTPS (Port 465), SMTPTLS (Port 587), POP3. Antivirus scanning should be signature based and should provide **ZERO HOUR Antivirus support.**
Gateway level Anti Virus should provide high-performance protection against viruses in SMTP, SMTPS (Port 465), SMTPTLS (Port 587), POP3, HTTP, HTTPS and FTP traffic. It should block viruses and worms from penetrating into an organization's internal network through e-mail attachments, malicious Web pages, and files obtained through FTP.
Virus gateway should provide real-time detection of viruses and malicious code at the gateway for IMAP SMTP, SMTPS (Port 465), SMTPTLS (Port 587), POP3, HTTP, HTTPS and FTP Internet traffic.
The proposed solution should be licensed per unit as against per user.
Frequent updates of virus pattern files should be available in the proposed system.
The proposed system should have an option to configures antivirus from firewall policies.
In terms of SMTP AV scanning the solution should not act as mail relay or MTA by itself.
Should have configurable policy options to select what services to be scan for viruses
Web based management through https and command line interface support
The proposed solution should have reporting facility to generate reports on virus detected.
Should have configurable policy options to bypass URL from antivirus engine.
VPN
This feature should be easy to configure and use. Should have a support inbuilt for IPSEC VPNs, SSL VPN, PPTP, L2TP, VPN CLIENT pass through, should support DES, 3 DES and AES encryption, IKE certificate authentication , RSA secure ID & Vasco Token support
Support for IPSec, L2TP, PPTP & SSL VPN.
Configurable option to allow or block VPN users or IPSec tunnel network to access internal network & vice versa.
Support Encryption : DES, 3DES, AES, twofish, blowfish & serpent encryption
Authentication support: Preshared Key, Digital Certificates.
Support for Automatic IKE (Internet Key Exchange) and manual key exchange.
Supports IPSEC NAT traversal
Supports Xauth
Supports Hash Algorithms – MD5, SHA1, SHA2.
Should support for IPSEC and PPTP VPN pass through so that computers or subnets on your internal network can connect to a VPN gateway on the Internet
Should support authentication through Hardware token : RSA, VASCO
Should support Deed peer detection and PFS.
Enterprise Cloud
The proposed solution should have an integrated cloud security solution in appliance.
The proposed solution should have option to download 32 and 64 bit Enterprise cloud clients.
Enterprise Cloud gives complete reporting of roaming users (mobile users), as if they are in your local network.
The proposed solution should protect roaming users even when on the Internet, this helps to secure their data and not just their LAN network.
The proposed solution should have ISP failover for cloud client.
The proposed solution should have DLP reporting for cloud client.
The proposed solution should have URL filtering, Anti-virus, Anti-Spam, IPS on cloud client.
The proposed solution should have centralized reporting of cloud client users.
Encryption supported (Blowfish, 3DES & AES) for data exchange through cloud client.
Data compression on cloud client users.
Cloud Client can connect LAN & DMZ networks after creating access policies & vice versa

The proposed solution should enforce for authentication to cloud users when accessing internet, LAN & DMZ network.
Multiple ISP Load Balancing and Failover
The proposed system should have integrated multiple ISP load balancing and failover for outbound traffic
The proposed system should support load balancing and failover for minimum 2 WAN links & maximum up to the interfaces available on the appliance.
The proposed system should be able to do weighted round robin based load balancing of traffic over multiple links
The proposed system should be able to detect link failure based on user configurable set of rules based on ICMP probe.
The proposed system should be able to detect link failure and alert admin on email.
The proposed system should support separate bandwidth queues on each ISP interface during failover/failback & load balancing using same firewall policy.
Logging and Reporting solution
The proposed system should have integrated on appliance reporting solution.
The proposed system should provide individual users download & Upload data usage report.
The proposed system should email daily group browsing reports to respective group heads in pdf format.
The proposed system should provide user and IP address based reports.
The proposed system should have options to create users with different access rights (E.g. users who can only view reports and not manage the system)
The reporting solution of the proposed system should be able to provide detailed Audit log for auditing and tracking system
Should support logging on the UTM appliance only and should not require additional Hardware or Software for Logging. It should provide various kinds of reports like virus reports, URL filtering reports, Top visited websites, Systems infected by Spywares, User or IP wise download for the day. It should have graphical reports of usages ISP wise, Application wise and IP wise.
The proposed system should have option to quarantine spam email on appliance.
The proposed system should have drill down reporting on appliance dashboard.
The proposed system store DLP reports on same appliance.
Email daily web & smtp upload reports on admin email address.
The proposed system should have live browsing & download report.
The proposed system should have Virus report.
The proposed system should have Administration logs.
The proposed system should have live firewall logs.
The proposed system should have live packet capture report.
The proposed system should have IPS report.
The proposed system should have bandwidth queue report.
The proposed system should have download report with mime & file extension blocked.
The proposed system should have configurable option in internet activity pdf reports which are send on email.
The proposed system should have an option to set retention period for logs.
The proposed system should provide connection details using a web interface with browsing data used for any point of time.
The proposed system should have an option to generate browsing report in pdf on the bases of search patterns like user name, IP address, URL & keywords.
The proposed system should have options to show browsing logs which are allowed as well as of blocked.