

SBICAP Securities Limited

**191 Maker Tower 'F',
Cuffe Parade, Mumbai - 400 005**

REQUEST FOR PROPOSAL ("RFP")

SSL/IT/2009-10/RFP006

2 Nos. FIREWALLS

Proposal Not Later Than : December 10, 2009 - 5.00 PM

**Issuing Office : Head IT,
SBICAP Securities Ltd,
191, Maker Tower 'F',
Cuffe Parade,
Mumbai - 400 005**

**AS PER THE ATTACHED LIST
PURCHASE OF 2 Nos. FIREWALL (BUNDLE)**

We intend to purchase **2 Nos.** Firewall for our offices in Mumbai.
The Configuration and through put Requirements of Firewalls are as under:

All applicable taxes and levies are to be mentioned separately.

Sr No	PART NUMBER	QTY	WARRANTY	PRICE [PER UNIT]	NET PRICE
1	Firewall – 1	1 Nos	3 Year Warranty 24 X 7 4 Hr CTR (Call Time Resolution)		
2	Firewall – 2	1 Nos	3 YEAR WARRANTY 8*5 with NBD(Next Business Day)		

Sr	Features	Remarks	Compliance
1	General Requirements		
1.1	The Firewall must be appliance based and should facilitate multi-application environment.		
1.2	It should be modular to accommodate future growth.		
1.3	The platform must use a hardened OS		
1.4	The Firewall should be ICSA Labs certified for ICSA 4.0, EAL 4 certified and OPSEC Certified		
1.5	The platform should use ASIC hardware that is optimized for packet and application level content processing.		
1.6	Appliance should be rack mountable		
1.7	Licensing: should be per device license for unlimited users for Firewall / VPN / IPS / WCF / AV and not user/IP based license – Please specify if the product does not follow the required licensing policy.		
1.8	Should support IPv6 traffic		
1.9	Should support automatic ISP failover as well as ISP load sharing for outbound traffic.		
1.10	DNS service is available or not (Split DNS, ordinary DNS)		
1.11	Release Date Of Most Current Version		
1.12	Release Number Of Most Current Version		
2	Interface & Connectivity Requirements		
2.1	The platform must be capable of supporting a		

	minimum of 8 Ethernet interfaces with auto sensing 10/100/1000 capability.		
2.2	It should be expandable to an additional Gigabit SFP ports in future. (if not please specify)		
2.3	The platform should support the standards based Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.		
2.4	The platform should support VLAN tagging (IEEE 802.1q)		
3	High Availability		
3.1	The firewall must support Active-Active as well as Active-Passive redundancy.		
3.2	The Firewall must support state full clustering of multiple active firewalls, and the firewalls must load balance the traffic between them to share the load.		
3.3	The cluster should support simple and minimal downtime during upgrade		
4	Performance Requirements		
4.1	The Firewall must support at least 600,000 concurrent connections		
4.2	The Firewall must support at least 20,000 new sessions per second processing.		
4.3	The Firewall should support throughputs of minimum 4 Gbps for both 512 byte packet and 64 byte packet - Should be scalable with additional modules		
4.4	The firewall should support a minimum of at least 1 Gbps of VPN Throughput and should be hardware accelerated		
4.5	The firewall should support a minimum of at least 1 Gbps of IPS Throughput		
5	Layer 2/3 Requirements		
5.1	The Firewall should support IEEE 802.1q VLAN Tagging with about minimum 1024 VLANs supported (in NAT/Route mode)		
5.2	There should be support for increasing bandwidth for links by using IEEE 802.3ad link aggregation		
5.3	Static routing must be supported.		
5.4	Policy based Routing must be supported		
5.5	RIPv1 and RIPv2 routing must be supported.		
5.6	The Firewall should support OSPF & BGP4		
5.7	The device should support multicast routing		
6	Firewall Features Requirements		
6.1	It should be possible to operate the firewall in a "stealth mode" or "bridging" or "transparent mode".		
6.2	The Firewall should also support the standard Layer 3 mode of configuration with Interface IP's.		
6.3	The Firewall must provide NAT functionality,		

	including dynamic and static NAT translations. It should be able to support Port Forwarding.		
6.4	All internet based applications should be supported for filtering like Telnet, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, BGP, IMAP, NFS etc		
6.5	The Firewall should support authentication protocols like LDAP, RADIUS and have support for firewall passwords, token-based products like Secure-ID, RADIUS & TACACS+ authentication servers and digital certificates.		
6.6	The Firewall should provide advanced NAT capabilities, supporting all applications and services (i.e. SIP/H.323 NAT Traversal)		
6.7	Firewall should support Voice based protocols like H.323, SIP, SCCP, MGCP etc		
7	Authentication Requirements		
7.1	Support for authentication at the firewall policy level		
7.2	Support for RSA Secure-ID		
7.3	Support for RADIUS, LDAP and TACACS+ integration for Authentication		
7.4	Support for Native Active Directory Integration		
8	Hiding Internal Network		
8.1	Support for network address translation		
8.2	Support for Port address translation		
8.3	Support for DNS Translation		
8.4	Should support NAT over VPN		
9	Encryption VPN Requirements		
9.1	The VPN should be integrated with firewall and support the full Encryption & other standards and protocols:		
a	DES, 3DES, AES		
b	MD5 and SHA-1 authentication		
c	Diffie-Hellman Group 1 , Group 2 and Group 5		
d	Internet Key Exchange (IKE) algorithm		
e	The new encryption standard AES 128, 192 & 256 (Advanced Encryption Standard)		
9.2	Should have integrated SSL VPN with no license slab restriction		
9.3	Encrypted tunnel support – firewall to firewall		
9.4	Encrypted tunnel support – user to firewall		
9.5	Support for choice of encryption methods		
9.6	Encrypted tunnel support for Internet & dial up connections		
9.7	Support for choice of VPN protocols		
9.8	Availability of Unlimited VPN client software (with no license slab restrictions) if not please specify		
9.9	Has the product been proven to work with other VPN products (proven IPSEC compatibility with other products)		

10	Administration Management Requirements		
10.1	The Firewall must support https & SSH management		
10.2	Should have configurable option to define remote access to the Firewall on any interface and restrict the same to a specific IP/Subnet		
10.3	The Firewall must provide a Graphical User Interface (GUI) as well as Command Line Interface (CLI) for making changes to the firewall rules set.		
10.4	The Firewall must provide a means for exporting the firewall rules set and configuration to a text file.		
10.5	There must be a means of connecting directly to the firewall through a console connection		
10.6	The Firewall must provide statistics about the status of Firewalls within the cluster. (in case of HA scenario)		
10.7	The Firewall must send SNMP traps to Network Management Servers (NMS) in response to System failures.		
10.8	Provision to generate automatic alerts via mails / syslog		
10.9	Provision to send alerts to multiple recipients		
10.10	Support for role based administration of firewall		
10.11	Support for Image upgrade via TFTP and Web-UI		
10.12	The firewall management solution including real-time monitoring, event logs collection, & policy enforcement should be from a single device only (mgt server/appliance)		
10.13	Should support system software rollback to the previous version during upgrade		
11	IPS		
11.1	Should have a built-in Signature and Anomaly based IPS engine on the same unit		
11.2	Able to prevent denial of service and Distributed Denial of Service attacks.		
11.3	Should be able to exclude certain hosts from scanning of particular signatures		
11.4	Supports CVE-cross referencing where applicable.		
11.5	Should provide the facility to configure Profile based sensors (Client/Server) for ease of deployment		
11.6	Should support granular tuning with option to configure Overrides for individual signatures.		
11.7	Supports automatic security updates directly over the internet. (i.e. no dependency of any intermediate device)		
11.8	Security check updates do not require reboot of the unit.		
11.9	Supports attack recognition inside IPv6 encapsulated packets.		
11.10	Supports user-defined signatures with Regular		

	Expressions.		
11.11	Supports several prevention techniques including drop-packet, tcp-rst (Client, Server & both) etc. List all prevention options		
11.12	Supports response adjustment on a per signature basis.		
11.13	Offers a variety of built-in responses including console alerts, email notifications, SNMP traps and packet log. List all response options, excluding prevention responses		
11.14	Should have the feature to exclude certain hosts' traffic (IP addresses) to be scanned for particular signatures		
11.15	IPS should have an option of Software Fail-Open to bypass under heavy load.		
11.16	IPS should have an option to add exceptions for network and services.		
12	Other Requirements		
12.1	Provision to create secure zones / DMZ		
12.2	Support for integration with NMS solution via the standards based SNMP		
12.3	Should Support Packet Capture to capture and examine the contents of individual data packets that traverse the firewall appliance for troubleshooting, diagnostics and general network activity		
12.4	Should have option to configure traffic shaping		
12.5	The firewall must have Jumbo Frame Support		
12.6	Should support Instant Messenger/ P2P access control for AOL-IM, Yahoo, MSN, ICQ, Gnutella, Bit Torrent, WinNY, Skype, eDonkey, KaZaa		
13	Gateway Antivirus		
13.1	The appliance should facilitate embedded anti virus support which is hardware accelerated (preferably ASIC) to ensure high level performance		
13.2	Should have option to schedule automatic updates of the new virus pattern.		
13.3	Gateway AV should be supported for real-time detection of viruses and malicious code for HTTP, FTP, SMTP, POP3 and IMAP, NNTP and IM		
13.4	Should have configurable policy options to select what traffic to scan for viruses		
13.5	Should have option to configure to respond to virus detection at the gateway in several ways i.e. Delete the file, Alert email etc		
13.6	Should have options to prevent user downloads based on file name as well as file type		
13.7	Should have facility to configure the max file/email size which can be downloaded thru internet		
13.8	The solution should be capable scanning Encrypted VPN tunnel traffic originating from the unit for virus		
13.9	In terms of SMTP AV scanning the solution should		

	not act as mail relay or MTA by itself.		
13.9	Should not be a home grown engine and antivirus engine should be from a well known manufacturer		
14	Web Content Filtering		
14.1	Should not be a home grown engine and web content filter should be from a well known manufacturer		
14.2	The appliance should facilitate embedded web content filtering feature		
14.3	Web content filtering solution should work independently without the need to integrate with proxy server.		
14.4	Should have facility to block URL' based on categories.		
14.5	URL database should have at least 40 million + sites and 100 categories.		
14.6	Should be able to block different categories/sites based on users.		
14.7	Should have configurable parameters to block/allow unrated sites		
14.8	Should have configurable options to allow/deny access to web sites in case if the URL rating service is unavailable		
14.9	Should have options to customize the block message information send to end users		
14.10	Should have facility to schedule the configurations so that non work related sites are blocked during office hrs and allow access to all sites except non harmful sites during non office hrs.		
14.11	The solution should have options to block java applets, ActiveX as well as cookies		
14.12	The solution should be able to block URLs hosting spywares / adware's etc.		
14.13	Should have configurable policy options to define the URL exempt list		
15	Training		
15.1	Training & Technical certification for two persons		

Please quote strictly in the following format for the Firewall Bundle

The bids should reach us on the below mentioned address in sealed envelopes by 1700 hours on December 10, 2009. Kindly attach the business card of the company representative on the bid. This person should be available for correspondence and clarification if required.

If there is any deviation from the above specifications, it should be indicated in your bid. The terms and conditions of this bid are enclosed in **Annexure "A"**.

Note: As a token of your acceptance of the "Terms and Conditions" mentioned in Annexure "A", kindly submit the bid duly signed and stamped as "Accepted". Bids will not be considered for evaluation without the "Terms and Conditions" mentioned

in Annexure "A" being accepted.

Bids should be duly sealed and labeled as **"Quotation for 2 Nos Firewalls"** and addressed to the **"Head (IT), SBICAP Securities Limited, 191, Maker Tower "F", Cuffe Parade, Mumbai - 400 005 "**.

Yours faithfully,

Head (IT)

{Space left blank intentionally}

Annexure "A"

TERMS & CONDITIONS:

1) VALIDITY:

The prices should be valid for a period of 3 months. If the model becomes obsolete, the latest model with similar or better configuration should be delivered at the same price. Any downward revision in prices at the time of delivery will be passed on to us. The firewall bundle would be required to be delivered, Installed and supported at our offices in Mumbai.

2) PAYMENT:

90% of the total invoice value (including taxes and other levies) will be released after successful delivery and installation of the firewall[s]. The remaining 10% will be released after the warranty period. This 10% can also be released before the warranty period only against a Bank Guarantee from a Scheduled Bank. Payment will be done within 7-10 working days from receipt of the complete invoice with the installation and sign off reports.

3) DELIVERY:

The firewall bundle should be delivered to us within a period of 2 weeks from the date of receipt of purchase order. In case of delayed delivery, penal charges @ Rs. 5,000/- per day will be levied. The delay will be calculated and deduction will be done accordingly at the time of payment. The penal charges can be waived off subject to the vendor providing a standby (up to a maximum period of one week from the last day of delivery of the original product) of a similar or better configuration retaining the make and model mentioned in the accepted proposal. Failure of the above provision will invoke the penalty as mentioned above.

4) WARRANTY:

- a) 36 months free onsite comprehensive warranty including free provision of spares, parts, as and when necessary, from the date of acceptance of the firewall (excluding consumables). The warranty will also cover software related to the firewall in the form of licenses, updates, patches etc. for all modules installed.
- b) During the warranty period, your service engineer should be available at our office 24X7 4 Hr CTR for item number 1 and for the other one it's 8*5 Next Business Day [NBD]. Your failure to adhere to this stipulation would invite a penalty of Rs 500/- Per hour for item number 1 and Rs. 1000/- per day for item number 2. This penalty will be adjusted from the 10% bank guarantee. If the amount exceeds the 10% bank guarantee then the equivalent calculated amount will be debited to the vendor at each instance of failure.

5) ACCEPTANCE:

We will accept the firewall bundle only after testing it thoroughly.

6) TRANSFER OF OWNERSHIP:

Transfer of ownership of the property will be effective as soon as the equipment is installed at the site and accepted by SBICAP Securities Limited (SSL). The vendor should adequately insure the goods till the ownership passes on to SSL.

7) SUPPORT:

The vendor will support for any configuration (new/change) to be carried out in the Firewall Bundle as and when required during the warranty period. They will also support in shifting and installing along with configuring the Firewall Bundle at any other location within Mumbai.

8) ANNUAL MAINTENANCE CONTRACT:

The terms and conditions for the Annual Maintenance Contract will remain the same as mentioned in this RFP. Warranty will be replaced by AMC wherever applicable. **Vendors should quote for after warranty AMC, separately in the bid for the Firewall Bundle.**

9) MISCELLANEOUS:

- a) The vendor and its employees will strictly undertake not to communicate or allow to be communicated to any person or divulge in any way, any information relating to the ideas, know-how, technique, data, facts, figures and any information whatsoever concerning or relating to SSL and its affairs to which the said employees have access in the course of the performance of the contract.
- b) Within the period of warranty/maintenance cover stipulated, SSL would have the right to:
 - I. Shift the firewalls to an alternate site at its choice.
 - II. Disconnect/connect peripherals acquired from another vendor.

The warranty and service contract terms would not be considered violated if any one of the above takes place. Should there be a fault in the operations of the Firewall, you shall not unreasonably assume that the cause lie with those components not acquired from you.

- c) All disputes and differences of any kind whatsoever arising out of or in connection with the purchase order shall be referred to arbitration. The arbitrator may be appointed by both the parties or in case of disagreement; each party may appoint an arbitrator and the decision of the arbitrator(s) shall be final. Such arbitration is to be governed by the provisions of the Indian Arbitration Act and the jurisdiction shall be restricted to Mumbai only.
- d) **Firewall should strictly conform to the specifications stipulated by us.** In case of any deviation, we reserve the right to reject the quotation. **In case of any deviation is**

detected after acceptance, you should replace the identified Firewall (s) free of cost.

- e) You will pass on to SSL the benefits due to any downward revision of price before shipment of the equipment to SSL as well as lowering of taxes/statutory levies.

In this connection, you will not be entitled to claim any additional amount on account of any increase in statutory duties/exercise/taxes etc. or any fresh imports of currency devaluation at any time up to delivery of the equipment.

- f) Proof of Octroi (if any) paid should be produced in original for payment.
- g) Any component other than those that are part of the standard model should be quoted separately.
- h) We reserve the right to modify /alter the terms and conditions of the tender. We also reserve the right to cancel the tender / revise the number of firewalls to be procured if considered necessary. SSL's decision in this regard shall be final and binding on the vendor.
- i) Incomplete tenders are likely to be rejected outright.
- j) Please submit a copy of SLA

-----END OF DOCUMENT-----