SHREE SAIBABA SANSTHAN TRUST, SHIRDI

AP-SHIRDI. TAL-RAHATA. DIST-AHILYANAGAR MS 423 109

email it.office@sai.org.in

QUOTATION FOR FIREWALL.

Sealed quotations are invited from authorized dealers for purchase of Firewall. The detailed specification of Firewall is as mentioned below.

Specification of Firewall	**Qty**
Make: Fortigate or Palo Alto 10 x GE RJ45 ports (including 7x Internal Ports, 2 x WAN Ports, 1 x-DMZ Port). With subscription- 3 Years 24x7 Unified Threat Protection Support includes Comprehensive Support, Advanced Hardware Replacement (In case of failure and confirmation of RMA next business day dispatch of replacement. Firmware and General Upgrades, UTP Services Bundle (Application Control, IPS, AV, Botnet IP/Domain, Mobile Malware Service, Web Filtering, Antispam, Cloud Sandbox including Virus Outbreak and Content Disarm & Reconstruct Services) Check Annexure B for detailed Specification of Firewall 3 Years subscription and onsite NBD warranty.	1

Documents Required with Quotation.

1. Photocopy of PAN Card and GST registration.
2. Firm registration.
3. Authorization from OEM.
4. Firm details as given in Annexure A.
5. Compliance Sheet Annexure B

Terms and Condition.

1. Incomplete quotations with conditions and received late will be summarily rejected.
2. Supply of firewall should done within 15 days after receiving the Purchase order.
3. Licenses if any, should be registered in the name of "Chief Executive Officer, Shree Saibaba Sansthan Trust, Shirdi".
4. Payment conditions: 100% after delivery and Inspection.
5. Quotation Submission:
   Quotations should be submitted in sealed Envelope as:

   Quotation for Firewall – Information Technology Department.

   Chief Executive Officer,
   Shree Saibaba Sansthan Trust, Shirdi
   Ap-Shirdi. Tal - Rahata.
   Dist- Ahilyanagar
   Pin code - 423109.
6. Quotation submission from 18-April-2025 to 28-April2025 5:00 PM in Sansthan Inward office.
7. Rate should inclusive of all Taxes.
8. Delivery and Installation of Firewall to be done at Hyderabad Office.

For any of the Technical queries contact 02423-258953 or mail at it.office@sai.org.in

Chief Executive Officer

Shree Saibaba Sansthan Trust, Shirdi

Annexure-A

Personal & Bank Details
All columns are mandatory
(Submit on Company Letter Head)

SN	Personal Detail	
1	Name of the Agency.	
2	Address	
3	Contact Person and Cell No	
4	PAN and GST number	
5	Bank Details –	
	Name of the Bank	
	Bank City	
	Branch Name and Code	
	Account Type	
	Account Number	
	IFSC CODE	
	MICR NO.	

ANNEXURE B FIREWALL SPECIFICATION

SN	Specification	Compliance (Yes/No)
	Hardware	
1	The Firewall must be hardware appliance based.	
2	Should support 5 or more gigabit RJ45 interfaces.	
3	Should support 1 or more SFP slots (up to 1G).	
4	Should have 1 console port (RJ45) and 1 USB port.	
	Firewall Performance	
5	Should have Firewall throughput of minimum 6 Gbps or more.	
6	IPSec VPN throughput should be 1.5 Gbps or more.	
7	Proposed appliance shall provide 700 Mbps of NGFW performance measured with Firewall, IPS, Application Control, and logging enabled on IMIX/Enterprise Mix/Production Traffic.	
8	Proposed appliance shall provide 600 Mbps of Threat Protection performance measured with Firewall, IPS, Application Control, Malware Protection, and logging enabled on IMIX/Enterprise Mix/Production Traffic.	
9	Must support at least 1,000,000 or more concurrent connections.	
10	Must support at least 30,000 or more new sessions per second processing.	
11	Should support up to 10 Virtual Domains (VDOMs or VSYS) with appropriate licensing.	
	Firewall Features	
12	Should support both “bridge mode” or "transparent mode” apart from the standard NAT mode.	
13	Should provide NAT functionality, including PAT. Should support NAT66, NAT64, Static NAT IPv4 to IPv6 and vice versa (VIP64 and VIP46), and IPv6-IPv4 tunnelling or dual stack.	
14	Should support IPv4 & IPv6 policies.	
15	Provision to create secure zones/DMZ (i.e., Multi-Zone support).	
16	Should support standards-based Multi-Link aggregation technology (IEEE 802.3ad) for higher bandwidth.	
17	Should support VLAN tagging (IEEE 802.1q) in NAT/Route mode.	
18	Should support Static routing and Dynamic Routing (RIP, OSPF, and BGP).	
19	Firewall should support stateful failover of sessions in Active/Standby mode.	
20	Firewall shall support redundant interfaces to provide interface-level redundancy before device failover.	
21	Should support ISP Load balancing/Link Sharing and Failover.	
22	Should support multi-path intelligence based on link quality criteria.	
23	Should support link performance checks based on packet loss, latency, and jitter.	
24	Should support WAN path controllers providing high application performance.	
25	Should support application-specific rules based on SLA strategy.	
26	Firewall should support capability to limit bandwidth on the basis of apps/groups, networks/Geo, ports, etc.	
27	Should support high-performance deep packet inspection for application identification and control.	
	Authentication	
28	Should support User-Group-based Authentication (Identity-based Firewalling) & Scheduling.	
29	Should support authentication servers – RADIUS, LDAP, and Active Directory.	
30	Support for RSA Secure ID or other Token-based products.	
	VPN	

SN	Specification	Compliance (Yes/No)
31	Should support protocols such as DES & 3DES, MD5, SHA-1, SHA-256 authentication, Diffie-Hellman Groups 1, 2, 5, 14, Internet Key Exchange (IKE) v1, as well as IKE v2 algorithms, and AES (128/192/256).	
32	Should support a minimum of 200 IPSec Site-to-Site and 200 IPSec Site-to-Client VPN tunnels.	
33	Should support NAT within IPSec/SSL VPN tunnels.	
34	Should support Stateful failover for both Firewall and VPN sessions.	
	IPS	
35	Should have a built-in Signature and Anomaly-based IPS engine on the same unit.	
36	Should have protection for 5,000+ signatures.	
37	Able to prevent denial-of-service and distributed Denial-of-Service attacks.	
38	Supports user-defined signatures (i.e., Custom Signatures) with Regular Expressions.	
39	Solution must provide IP reputation feed comprising regularly updated collections of poor reputation IPs determined by the vendor.	
40	Firewall OEM must have its own threat intelligence analysis center and use the global footprint of security deployments for comprehensive network protection.	
41	Should be able to identify attacks based on Geo-location and define policy to block them.	
42	Solutions should allow configuring DoS policies used to associate DoS settings with traffic that reaches an interface.	
	Application Control	
43	Should have an Application Control feature with 2,000 or more application signatures.	
44	Should perform Traffic Shaping/Rate Limiting based on applications.	
45	Should control popular IM/P2P, proxy applications regardless of port/protocol.	
	Gateway Antivirus	
46	The appliance should facilitate embedded antivirus/anti-malware support.	
47	Gateway AV/Anti-malware should support real-time detection for HTTP, HTTPS, FTP, SMTP, SMTPS, POP3, and IMAP protocols.	
48	Should also include Botnet filtering and detecting and preventing Botnet command-and-control traffic.	
49	Should have configurable policy options to select traffic to scan for viruses.	
	Web Filtering	
50	The appliance should facilitate embedded Web Content and URL Filtering features.	
51	Web content and URL filtering should work independently without the need to integrate with an external proxy server.	
52	URL database should have 100 million or more URLs under 50+ categories.	
53	Should be able to block different categories/sites based on user authentication.	