



SHRI SAIBABA SANSTHAN TRUST, SHIRDI

Information Technology Department

**Tender document for
Purchase of Firewall**

Po. Shirdi, Tal. Rahata, Dist. Ahmednagar.

Phone No. (02423)-258953

Website: - www.sai.org.in email- it.office@sai.org.in.



TENDER NOTICE

SHRI SAIBABA SANSTHAN TRUST INFORMATION TECHNOLOGY DEPARTMENT

Shirdi, Tal. Rahata, Dist. Ahmednagar.

Phone No. (02423)-258953

Website: - www.sai.org.in email- it.office@sai.org.in

Purchase of Firewall

Online tenders are invited for the **Purchase of Firewall** from Manufacturers/ Authorized partner of the original equipment manufacturer. The tender details will be available on <https://mahatenders.gov.in> for downloading & the tender has view only access on the Sansthan's website www.sai.org.in under tender menu.

Technical Specifications are given in 'Annexure B' in Tender Document.

1.0 Time Table for online tender submission

Online Tender Publish Date	Dt.06-04-2021 Time- 11.00
Online Documents Download/Sales Start Date	Dt.06-04-2021 Time- 11.00
Online Documents Download/Sales End Date	Dt.22-04-2021 Time- 17.00
Queries Submission last Date	Dt.09-04-2021 Time- 11.00
Online Pre Bidding Meeting Date	Dt.09-04-2021 Time- 11.00
Online Bid Submission Start Date	Dt.06-04-2021 Time- 11.00
Online Bid Submission End Date	Dt.22-04-2021 Time- 17.00
Online Technical Bid Opening Date	Dt.24-04-2021 Time- 11.00

Pre bid Meeting.

Considering to COVID-19 situation, pre-bid meeting will be conducted over MS Team instead of in-person meeting at Shirdi. Bidders/OEM need to connect the MS Team 10 min before the scheduled time using following link. For any queries, bidder can call 02423-258953 or mail to it.office@sai.org.in.

https://teams.microsoft.com/l/meetup-join/19%3ameeting_YWU5YTM3OWUtOTUyZC00YTc5LTk1N2ItN2E3YjkwYTJiMGRI%40thread.v2/0?context=%7b%22Tid%22%3a%22e5ced1d2-162f-47f9-9315-3e753d1c9809%22%2c%22Oid%22%3a%2245258baf-91e8-4a28-8c27-ca31997cde16%22%7d

Validity Period:

The offer of the bidder shall remain valid for acceptance for a minimum period of **120 days** from the date of opening of Commercial Bid.

1.1 Scope of Work.

- Supply, installation, testing and commencement of supplied materials along with integration with storage, switches, servers, router, network racks, power etc., for the commencement of Firewall as per SSST expectations.
- Provide product documentation and training to SSST on the configuration being performed and SOP to maintain the devices.

2.0 Tender Cost, Earnest Money Deposit & Security Deposit:

- a) **Tender Fees** : Rs: 4,200 (Four Thousands Two Hundred Only)
- b) **Earnest Money Deposit (EMD)**: Rs: 70,000 (Seventy Thousand Only)
- c) **Security Deposit (SD)**: Successful bidder has to deposit 5% amount of awarded cost as security deposit within 15 days from acceptance of purchase order. This amount will be refunded after warranty period.
- d) No interest will be paid on the EMD and Security Deposit.

Amount of EMD & Tender Fees must transfer online to Sansthan Bank Account, while uploading the e-tender from www.mahatenders.gov.in Security Deposit must be deposited at Sansthan Cashier section and receipt can be collected.

Note:

1. The amount of EMD will be refunded back to all bidders (except L1 bidder) after issuing order to L1 bidder.
2. L1 bidder's - EMD amount will be refunded after receiving security deposit.
3. Even though the tenderers meet the requirements, they are subject to be disqualified in case of misleading or false representations in the forms, statements and attachments submitted in proof of the qualification requirements.

3.0 TENDERING PROCEDURE.

Qualification Criteria:

- 1) Bidder should be the Original Equipment Manufacturer/Authorized partner of the original equipment manufacturer of Firewall.
- 2) Bidder should not be blacklisted by Central / State Government or Government Corporation or statutory Institute.
- 3) Bidder should have experience of minimum two implementations of similar firewall being supplied.
- 4) Bidder need to submit a letter from OEM stating that **"Supplied hardware & Software material will not be declared end of life & support in the next 5 years"**.
- 5) Firewall White papers/ Pamphlets/ Brochure for which you have quoted (Model number and specification).
- 6) Average annual turnover of bidder for last three financial years should be more than one Crore (2017-18, 2018-19, 2019-20). CA certificate is must.

3.1 Technical Bid

Technical BID must submit online only.

Scanned copy of following documents must be uploaded as Technical-bid.

(Note: Only 6 documents are allowed to upload, so bidder can merge multiple documents Into a single file ensuring minimum DPI and file size in KB)

1. Certificate of firm registration, GST Registration and PAN.
2. CA certificate mentioning Average Annual Turnover of 1 crore for last three financial years (FY - 2017-18, 2018-19, 2019-20).
3. Authorized partner Documents/Letter from OEM.
4. Letter stating that the Firm/Company is not blacklisted by Central / State Government, Government Corporation, statutory Institute.

5. Firewall White papers/ Pamphlets/ Brochure for which you have quoted (Model number and specification).
6. Supplied hardware & Software material should not be declared end of life & support in the next 5 years. Bidder need to submit a letter from OEM.
7. Letter on company/Firm letter head Stating that "Company/Firm have read all terms and conditions and agree with them"
8. Bidder should fill and upload the Annexure C and D.
9. Bidder should produce purchase orders of setting up similar firewall being supplied along with the sustenance support for the duration of the warranty period.
10. Bidder should provide original OEM URLs/product catalogue references explicitly to each specification stated in this tender document. Generic URLs or one URL quoting for all required specifications strictly not allowed and may lead to disqualification during Technical bid evaluation.

3.2 Commercial Bid

- * Price of all items should be exclusive of Tax.
- * In future, if there is change in GST then it will be make applicable from the date of notification.
- * The tenderer should quote online in BOQ provided.

3.3 Acceptance of Tender:

1. The commercial bid of technically qualified bidders, shall only opened online and lowest offer of the technically qualified bidder shall be accepted. The acceptance of tender will be communicated to the contractor by email or otherwise.
2. The quoted amount in online tender shall be valid for 120 days (Four Months) from the date of opening of the tenders.

3.4 Warranty Period.

1. Warranty period should be for 5 years from date of successful installation.
2. Bidder should provide 24X7 online support within warranty period. And should help our representative to log the call with respective company/OEM.
3. Bidder should ensure quarterly maintenance & support within the warranty period.
4. In case of any hardware/device goes down within the warranty period, bidder/OEM should ensure it is operational within 12 hours. Failing to such case, bidder/OEM should replace the device within 24 hours until it is repaired. In case of software/OS failure, bidder/OEM should replace it within 6 hours.
5. Bidder should maintain their in house technical team to provide timely sustenance support for all issues reported complying with below SLA and escalate to OEM as needed.

Priority	Priority Definition	Response	Resolution	Updates
High	Out of service Example: Any service not working, logs not recording etc.	15 Mins*	4 Hours	30 Min interval
Medium	Partial/Intermittent service Interruptions, Example: Performance degraded but still functioning	30 Mins*	8 Hours	1 Hour interval
Low	All changes requests, Service Requests	1 Hours*	24 Hours	4 Hours interval

*Time starts when the problem is detected / reported by Help Desk team / customer and ends on assistance/ repair as applicable.

4. Payments, Penalty:

1. 95% of payment after supply, successful Installation/configuration and inspection of all ordered material.
2. Remaining 5% of payment after one month from successful installation/configuration and inspection.
3. If Bidder/Supplier fails to deliver & configure the Firewall within stipulated time, Rs. 5000/day will deducted from Security Deposit.
4. During the warranty period, if Bidder/OEM fails to repair the Firewall within stipulated period, Rs. 5000/day will deducted from Security Deposit.

5. Terms and Conditions:

1. Device/Software license registration with respective OEM should be done in the name of 'Chief Executive Officer, Shri Saibaba Sansthan Trust, Shirdi'.
2. The decision of Chief Executive Officer, Shri Saibaba Sansthan Trust, Shirdi will be final and binding in case of any dispute between Trust and the bidder.
3. The bidder should study all the tender documents carefully and understand the tender contract conditions, specifications etc. before quoting online. If there are any doubts, they should get clarifications in writing but this shall not be a justification for submission of late tender or extension of submission date.
4. Each of the tender documents uploaded in technical bid is required to sign by the person/ persons submitting the tender.
5. Chief Executive Officer, Shri Saibaba Sansthan Trust reserves the rights to Accept / Reject Partial / Full Tender.

6. Delivery Schedule

1. Successful bidder should supply the material within 4-6 weeks from the purchase order acceptance date. Bidder should complete the Installation/configuration within 2 weeks from the material delivery date. Bidder can manage the supply and installation/configuration within **Eight weeks** from the purchase order acceptance date.
2. Delivery of material to be done at IT Department, Shri Saibaba Sansthan Trust, Shirdi on working day between 10 am to 6 pm.
3. Transport, freight and other charges will be responsibility of supplier.
4. If successful bidder refuses to deliver the allotted items or fails to deliver the material, EMD will be forfeited and such bidder will be black listed.
5. Bidder should ensure the deployment of the firewall within 14 working days from the arrival of the firewall on premise. In case of any delay identified during first week due to lack of skills or whatsoever reasons, the bidder should engage OEM or their designated trusted partners to configure the firewall without adding to further cost and schedule escalations.

(Kanhuraj Bagate I.A.S.)

Chief Executive Officer

Shri Saibaba Sansthan Trust Shirdi

ANNEXURE- A
Personal & Bank Details for RTGS
All columns are mandatory
(Submit on Company Letter Head)

Sr No	Personal Detail	
1	Name of the Firm	
2	Address	
4	Contact Person and Cell No	
5	GST umber	
6	Bank Details – Name of the Bank	
	Bank City	
	Branch Name and Code	
	Account Type	
	Account Number	
	IFSC CODE	
	MICR NO.	
7	Stamp and Signature of the agency	

ANNEXURE- B

A] Firewall Qty 1

Make (model): Palo Alto (PA850 or higher) OR Fortinet (600E or higher) OR Checkpoint (6600 or higher)
Bidder can quote firewall models with higher configuration than listed.

Sr.No	Features Description
1	Hardware Architecture
1.1	The firewall should be a purpose built hardware appliance supporting zone based firewall using Stateful Inspection, Intrusion Prevention, Web/URL Filtering, Application Control, User Authentication, Gateway DLP, Advanced Routing, Gateway Antivirus and Advanced Threat Protection (Zero-Day Malware Prevention) functions.
1.2	The platform should use either Multi-Core CPU or ASIC-based or equivalent architecture that is optimized for packet and application level content processing.
1.3	The firewall is to be offered in High Availability (1+1) in Active/Active HA or Active/Passive with Active sync of the configuration on the secondary firewall and logs stored locally on the firewall
1.4	Firewall appliance should have a minimum of 2x 10GE SFP+ Slots, 4 x 1GE SFP Slots and 4x 1GE RJ45 GE interfaces from day one. All these interfaces should be available simultaneously.
1.5	Each firewall appliance should be fully populated with SFP transceiver modules from day one.
1.6	Firewall appliance should have redundant power supply.
1.7	The administrator must be able to view report on the CPU usage along with details of process specific utilization in GUI/CLI in real-time.
2	Performance & Scalability
2.1	A Minimum NG Firewall application control throughput in real world/production environment/Application Mix with all modes enabled– up to 2 Gbps. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA.
2.2	Threat Prevention throughput (including FW, IPS, Application Control & Antivirus) must be at least 1 Gbps with real-world / enterprise mix traffic and with all modes and full scan enabled
2.3	NGFW (including FW, IPS, and Application Control) throughput must be at least 2 Gbps with real-world / enterprise mix traffic.
2.4	Firewall should support minimum of 10,000 new sessions per second
2.5	Firewall should support at least 150,000 concurrent sessions
3	Firewall Features
3.1	Firewall should provide native application firewalling , content inspection and user-id integration
3.2	The Firewall solution should support NAT64, DNS64, DNS6 & DHCPv6
3.3	The physical interface should be capable of link aggregation as per IEEE 802.3ad standard.
3.4	The proposed system should have integrated Traffic Shaping functionality.
3.5	The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN) with minimum 1 Virtual Firewall license.
3.6	Firewall solution must support dynamic SDN connectors to Public and Private Cloud vendors like AWS, Azure, GCP, VmWare ESXi/NSX, OpenStack etc. for dynamic object address creation and updation.
3.7	Should support IPSEC, PPTP, L2TP & SSL VPN
3.8	Solution must support at least 500 concurrent SSL VPN users from day one. Any additional licenses should be included from day one.
4	Advanced Routing Capabilities
4.1	The proposed systems should support automatic ISP/link failover as well as ISP/link load sharing for outbound traffic.

4.2	The proposed system shall support Link SLA Monitoring based on below parameters and perform routing decision change based on configured SLA's for particular IP/User/Application on the basis of:
4.2.1	Latency
4.2.2	Jitter
4.2.3	Packet loss threshold
5	Next Generation Intrusion Prevention System
5.1	Threat Prevention throughput (including FW, IPS, Application Control & Antivirus) must be at least 1 Gbps with real-world / enterprise mix traffic and with all modes and full scan enabled
5.2	Should have the capability to inspect SSL traffic. The SSL inspection throughput should be minimum of 1 Gbps or more
5.3	The proposed firewall shall be able to handle (alert, block or allow) unknown/unidentified applications like unknown UDP & TCP
5.4	The proposed firewall should have the ability to create custom application signatures and categories directly on firewall without the need of any third-party tool or technical support.
5.5	The NGFW must have GUI based packet capture utility within its management console with capability of creating packet capture filters for IPv4 and IPv6 traffic and ability to define the packet and byte count
5.6	The proposed firewall shall be able to implement Zones, IP address, Port numbers, User id, Application id and threat protection profile under the same firewall rule or the policy configuration
5.7	The firewall must support creation of policy based on wildcard addresses to match multiple objects for ease of deployment
5.8	The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application base on the content.
5.9	The proposed firewall shall be able to protect the user from the malicious content upload or download by any application. Example Blocking a malicious file downloads via a chat or file sharing application.
5.11	The firewall must have the ability to manage firewall policy even if management server is unavailable
5.12	The firewall must disallow root access to firewall system all users (including super users) at all times.
5.13	The firewall must be capable of prevention against flooding of new sessions with high-volume single-session and multiple-session attacks.
5.14	IPS solution should have capability to protect against Denial of Service (DoS) attacks. Should have flexibility to configure threshold values for each of the anomaly. DoS protection should be applied and attacks stopped before firewall policy look-ups.
6	Application Control Features:
6.1	Should have the intelligence to identify & control of popular IM & P2P applications like KaZaa, Bit Torrent, Skype, You Tube, Facebook, LinkedIn etc.
6.2	Should have a native capability to enable application based policies on base functionality and block other sub-applications (disabling upload, download, chat but allowing base email functionality)
6.3	The proposed system shall have the ability to detect, log and take action against network traffic based on over 1,000 application signatures
6.4	The proposed system shall have the ability to identify, block or rate limit applications.
6.5	Solution should support creation of custom application signatures.
7	Anti-Virus, Anti-Bot & Advanced Threat Protection
7.1	Should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy or based on firewall authenticated user groups for HTTP, SMTP, POP3, IMAP, FTP, SMB protocols & their encrypted versions
7.2	Firewall must include Anti-bot capability using IP reputation DB, and should be also be able to terminate botnet communication to C&C servers.
7.3	The proposed solution should automatically detect and confirm multistage zero-day malware and targeted attacks without prior knowledge of the malware by performing cloud-based sandboxing of suspicious files.

7.4	The solution must employ a cloud sandbox analysis engine using virtual execution to detect zero day and unknown threats and must not be reliant only on signatures.
7.5	The Sandbox functionality of proposed solution should utilize a state-full attack analysis including Bare-Metal Analysis to detect the entire infection lifecycle, and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.
7.6	The Sandboxing environment should provide an update signature for unknown threat
7.7	The proposed firewall shall perform content based signature matching beyond the traditional hash base signatures
7.8	Should have DNS sink holing for malicious DNS request from inside hosts to outside bad domains and should be able to integrate and query third party external threat intelligence data bases to block or sinkhole bad IP address, Domain and URLs
7.9	The proposed solution must be able to identify DGA and DNS tunneling.
7.10	The proposed solution must have DNS security that provides Tight integration with next-generation firewalls eliminates the need for standalone tools and enables automated threat response.
7.11	The proposed solution must have Automated enforcement of Policies that can be configured for dynamic action to block malicious domains, sinkhole DNS Queries, and identify infected machines.
7.12	There should be no limit to the DNS signatures per hardware. New signatures should be identified and threats should be prevented immediately.
7.13	The URL filtering service should be able to override categorization of a site by creating custom categories.
7.14	The solution must be able to define AV scanning on per application basis such that certain applications may be excluded from AV scan while some applications to be always scanned
7.15	Should be able to call 3 rd party threat intelligence data on malicious IPs, URLs and Domains to the same firewall policy to block those malicious attributes and list should get updated dynamically with latest data
7.16	Vendor should automatically push dynamic block list with latest threat intelligence data base on malicious IPs, URLs and Domains to the firewall policy as an additional protection service
7.17	The NGFW should have native protection against credential theft attacks(without the need of endpoint agents) with ability to prevent the theft and abuse of stolen credentials and the following : <ul style="list-style-type: none"> · Automatically identify and block phishing sites · Prevent users from submitting credentials to phishing sites.
8	User Authentication
8.1	The proposed solution shall be able to support various form of User Authentication methods simultaneously, including:
8.2	Local Database entries
8.3	LDAP server entries
8.4	RADIUS server entries
8.5	Windows AD (Single Sign On capability - both Agent-based and Agentless)
9	Data Leakage Prevention
9.1	Firewall should have DLP functionality. Any additional hardware/ software/ license should be included from day one.
9.2	System should allow administrator to prevent sensitive data from leaving the network. Administrator should be able to define sensitive data patterns, and data matching these patterns that should be blocked and/or logged when passing through the unit.
9.3	Solution must detect, protect and log sensitive data travelling through HTTP and HTTPS channels
9.4	DLP actions should be : Log only, block, quarantine user/IP/Interface
10	High Availability
10.1	System should have built-in High Availability (HA) features.
10.2	Should support state full session maintenance in the event of a fail-over to a standby unit.
10.3	Firewall in HA should support seamless up gradation activity for all major and minor versions

10.4	High Availability feature must be supported for either NAT/Route or Transparent mode
10.5	High Availability Configurations should support Active/Active & Active/ Passive.
11	Logging Reporting & Management
11.1	Solution must include internal logging and reporting. . There should be a log forwarding feature to forward firewall logs to logging server. In case of virtual appliance for logging underlying server hardware to be provisioned by bidder.
11.2.1	Traffic reports: availability, bandwidth usage per access circuit, bandwidth usage per application, QoS per access circuit with bytes , sessions , source and destination
11.2.2	Security reports: all antivirus, web filtering, application control, intrusion prevention, email filtering, data leak prevention with user ID , source IP , Source and Destination region should be available within the firewall.
11.2.3	Audit logs like admin authentications, detailed configuration changes including previous configuration and modified configuration.
11.3	It should show near real-time traffic statistics
11.4	Logging and Reporting solution should be able to perform Historic Retrospective Scan on the collected logs and reports. It should be able to scan previously received DNS, web filter, traffic logs back in time, so that when new definitions are received from threat intelligence server it can use new information to compare against old logs to check if there was any successful communication with malicious domains/URLs in the recent past.
11.5	Logging and Reporting solutions should have minimum 240GB storage capacity and forward older logs to centralized logging server as per retention policy
11.6	The management solution must have the native capability to optimize the security rule base and offer steps to create application based rules
11.7	The proposed solution must allow single policy rule creation for application control, user based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS
11.8	Should have real time logging base on all Traffic, Threats, User IDs, URL filtering, Data filtering, Content filtering, unknown malware analysis, Authentication, Tunneled Traffic and correlated log view base on other logging activities
11.9	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis
11.11	Should allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.
11.12	Should have built in report templates base on Applications, Users, Threats, Traffic and URLs
11.13	Should be able to create report base on SaaS application usage
11.14	Should be able to create reports base user activity
11.15	Should be able to create custom report base on custom query base any logging attributes
11.16	On device management service should be able to provide all the mentioned features in case of central management server failure
12	Support and RMA
12.1	Proposed solutions including Firewall & Reporting Solution should include licenses required to support above mentioned features and functionalities along with 24x7 remote support directly from OEM and Next Business Day RMA replacement for 5 years.

ANNEXURE- C
Compliance Sheet

(To be filled by bidder on letter head and submit with technical Bid)

A] Firewall Qty 1

Make (model): Palo Alto (PA850 or higher) OR Fortinet (600E or higher) OR Checkpoint (6600 or higher)

Bidder can quote firewall models with higher configuration than listed.

Sr.No	Features Description	Compliance (Yes/No)	Variation (in any)
1	Hardware Architecture		
1.1	The firewall should be a purpose built hardware appliance supporting zone based firewall using Stateful Inspection, Intrusion Prevention, Web/URL Filtering, Application Control, User Authentication, Gateway DLP, Advanced Routing, Gateway Antivirus and Advanced Threat Protection (Zero-Day Malware Prevention) functions.		
1.2	The platform should use either Multi-Core CPU or ASIC-based or equivalent architecture that is optimized for packet and application level content processing.		
1.3	The firewall is to be offered in High Availability (1+1) in Active/Active HA or Active/Passive with Active sync of the configuration on the secondary firewall and logs stored locally on the firewall		
1.4	Firewall appliance should have a minimum of 2x 10GE SFP+ Slots, 4 x 1GE SFP Slots and 4x 1GE RJ45 GE interfaces from day one. All these interfaces should be available simultaneously.		
1.5	Each firewall appliance should be fully populated with SFP transceiver modules from day one.		
1.6	Firewall appliance should have redundant power supply.		
1.7	The administrator must be able to view report on the CPU usage along with details of process specific utilization in GUI/CLI in real-time.		
2	Performance & Scalability		
2.1	A Minimum NG Firewall application control throughput in real world/production environment/Application Mix with all modes enabled- up to 2 Gbps. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA.		
2.2	Threat Prevention throughput (including FW, IPS, Application Control & Antivirus) must be at least 1 Gbps with real-world / enterprise mix traffic and with all modes and full scan enabled		
2.3	NGFW (including FW, IPS, Application Control) throughput must be at least 2 Gbps with real-world / enterprise mix traffic.		
2.4	Firewall should support minimum of 10,000 new sessions per second		
2.5	Firewall should support at least 150,000 concurrent sessions		
3	Firewall Features		
3.1	Firewall should provide native application firewalling , content inspection and user-id integration		
3.2	The Firewall solution should support NAT64, DNS64, DNS6 & DHCPv6		
3.3	The physical interface should be capable of link aggregation as per IEEE 802.3ad standard.		
3.4	The proposed system should have integrated Traffic Shaping functionality.		

3.5	The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN) with minimum 1 Virtual Firewall license.		
3.6	Firewall solution must support dynamic SDN connectors to Public and Private Cloud vendors like AWS, Azure, GCP, VmWare ESXi/NSX, OpenStack etc. for dynamic object address creation and updation.		
3.7	Should support IPSEC, PPTP, L2TP & SSL VPN		
3.8	Solution must support at least 500 concurrent SSL VPN users from day one. Any additional licenses should be included from day one.		
4	Advanced Routing Capabilities		
4.1	The proposed systems should support automatic ISP/link failover as well as ISP/link load sharing for outbound traffic.		
4.2	The proposed system shall support Link SLA Monitoring based on below parameters and perform routing decision change based on configured SLA's for particular IP/User/Application on the basis of:		
4.2.1	Latency		
4.2.2	Jitter		
4.2.3	Packet loss threshold		
5	Next Generation Intrusion Prevention System		
5.1	Threat Prevention throughput (including FW, IPS, Application Control & Antivirus) must be at least 1 Gbps with real-world / enterprise mix traffic and with all modes and full scan enabled		
5.2	Should have the capability to inspect SSL traffic. The SSL inspection throughput should be minimum of 1 Gbps or more.		
5.3	The proposed firewall shall be able to handle (alert, block or allow) unknown/unidentified applications like unknown UDP & TCP		
5.4	The proposed firewall should have the ability to create custom application signatures and categories directly on firewall without the need of any third-party tool or technical support.		
5.5	The NGFW must have GUI based packet capture utility within its management console with capability of creating packet capture filters for IPv4 and IPv6 traffic and ability to define the packet and byte count		
5.6	The proposed firewall shall be able to implement Zones, IP address, Port numbers, User id, Application id and threat protection profile under the same firewall rule or the policy configuration		
5.7	The firewall must support creation of policy based on wildcard addresses to match multiple objects for ease of deployment		
5.8	The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application base on the content.		
5.9	The proposed firewall shall be able to protect the user from the malicious content upload or download by any application. Example Blocking a malicious file downloads via a chat or file sharing application.		
5.11	The firewall must have the ability to manage firewall policy even if management server is unavailable		
5.12	The firewall must disallow root access to firewall system all users (including super users) at all times.		
5.13	The firewall must be capable of prevention against flooding of new sessions with high-volume single-session and multiple-session attacks.		
5.14	IPS solution should have capability to protect against Denial of Service (DoS) attacks. Should have flexibility to configure threshold values for each of the anomaly. DoS protection should be applied and attacks stopped before firewall policy look-ups.		
6	Application Control Features:		

6.1	Should have the intelligence to identify & control of popular IM & P2P applications like KaZaa, Bit Torrent, Skype, You Tube, Facebook, LinkedIn etc.		
6.2	Should have a native capability to enable application based policies on base functionality and block other sub-applications (disabling upload , download , chat but allowing base email functionality)		
6.3	The proposed system shall have the ability to detect, log and take action against network traffic based on over 1,000 application signatures		
6.4	The proposed system shall have the ability to identify, block or rate limit applications.		
6.5	Solution should support creation of custom application signatures.		
7	Anti-Virus, Anti-Bot & Advanced Threat Protection		
7.1	Should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy or based on firewall authenticated user groups for HTTP, SMTP, POP3, IMAP, FTP , SMB protocols & their encrypted versions		
7.2	Firewall must include Anti-bot capability using IP reputation DB, and should be also be able to terminate botnet communication to C&C servers.		
7.3	The proposed solution should automatically detect and confirm multistage zero-day malware and targeted attacks without prior knowledge of the malware by performing cloud-based sandboxing of suspicious files.		
7.4	The solution must employ a cloud sandbox analysis engine using virtual execution to detect zero day and unknown threats and must not be reliant only on signatures.		
7.5	The Sandbox functionality of proposed solution should utilize a state-full attack analysis including Bare-Metal Analysis to detect the entire infection lifecycle, and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.		
7.6	The Sandboxing environment should provide an update signature for unknown threat		
7.7	The proposed firewall shall perform content based signature matching beyond the traditional hash base signatures		
7.8	Should have DNS sink holing for malicious DNS request from inside hosts to outside bad domains and should be able to integrate and query third party external threat intelligence data bases to block or sinkhole bad IP address, Domain and URLs		
7.9	The proposed solution must be able to identify DGA and DNS tunneling.		
7.10	The proposed solution must have DNS security that provides Tight integration with next-generation firewalls eliminates the need for standalone tools and enables automated threat response.		
7.11	The proposed solution must have Automated enforcement of Policies that can be configured for dynamic action to block malicious domains, sinkhole DNS Queries, and identify infected machines.		
7.12	There should be no limit to the DNS signatures per hardware. New signatures should be identified and threats should be prevented immediately.		
7.13	The URL filtering service should be able to override categorization of a site by creating custom categories.		
7.14	The solution must be able to define AV scanning on per application basis such that certain applications may be excluded from AV scan while some applications to be always scanned		

7.15	Should be able to call 3 rd party threat intelligence data on malicious IPs, URLs and Domains to the same firewall policy to block those malicious attributes and list should get updated dynamically with latest data		
7.16	Vendor should automatically push dynamic block list with latest threat intelligence data base on malicious IPs, URLs and Domains to the firewall policy as an additional protection service		
7.17	The NGFW should have native protection against credential theft attacks(without the need of endpoint agents) with ability to prevent the theft and abuse of stolen credentials and the following : <ul style="list-style-type: none"> · Automatically identify and block phishing sites · Prevent users from submitting credentials to phishing sites. 		
8	User Authentication		
8.1	The proposed solution shall be able to support various form of User Authentication methods simultaneously, including:		
8.2	Local Database entries		
8.3	LDAP server entries		
8.4	RADIUS server entries		
8.5	Windows AD (Single Sign On capability - both Agent-based and Agentless)		
9	Data Leakage Prevention		
9.1	Firewall should have DLP functionality. Any additional hardware/ software/ license should be included from day one.		
9.2	System should allow administrator to prevent sensitive data from leaving the network. Administrator should be able to define sensitive data patterns, and data matching these patterns that should be blocked and/or logged when passing through the unit.		
9.3	Solution must detect, protect and log sensitive data travelling through HTTP and HTTPS channels		
9.4	DLP actions should be : Log only, block, quarantine user/IP/Interface		
10	High Availability		
10.1	System should have built-in High Availability (HA) features.		
10.2	Should support state full session maintenance in the event of a fail-over to a standby unit.		
10.3	Firewall in HA should support seamless up gradation activity for all major and minor versions		
10.4	High Availability feature must be supported for either NAT/Route or Transparent mode		
10.5	High Availability Configurations should support Active/Active & Active/Passive.		
11	Logging Reporting & Management		
11.1	Solution must include internal logging and reporting. . There should be a log forwarding feature to forward firewall logs to logging server. In case of virtual appliance for logging underlying server hardware to be provisioned by bidder.		
11.2.1	Traffic reports: availability, bandwidth usage per access circuit, bandwidth usage per application, QoS per access circuit with bytes , sessions , source and destination		
11.2.2	Security reports: all antivirus, web filtering, application control, intrusion prevention, email filtering, data leak prevention with user ID , source IP , Source and Destination region should be available within the firewall.		
11.2.3	Audit logs like admin authentications, detailed configuration changes including previous configuration and modified configuration.		
11.3	It should show near real-time traffic statistics		

11.4	Logging and Reporting solution should be able to perform Historic Retrospective Scan on the collected logs and reports. It should be able to scan previously received DNS, web filter, traffic logs back in time, so that when new definitions are received from threat intelligence server it can use new information to compare against old logs to check if there was any successful communication with malicious domains/URLs in the recent past.		
11.5	Logging and Reporting solutions should have minimum 240GB storage capacity and forward older logs to centralized logging server as per retention policy		
11.6	The management solution must have the native capability to optimize the security rule base and offer steps to create application based rules		
11.7	The proposed solution must allow single policy rule creation for application control, user based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS		
11.8	Should have real time logging base on all Traffic, Threats, User IDs, URL filtering, Data filtering, Content filtering, unknown malware analysis, Authentication, Tunneled Traffic and correlated log view base on other logging activities		
11.9	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis		
11.11	Should allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.		
11.12	Should have built in report templates base on Applications, Users, Threats, Traffic and URLs		
11.13	Should be able to create report base on SaaS application usage		
11.14	Should be able to create reports base user activity		
11.15	Should be able to create custom report base on custom query base any logging attributes		
11.16	On device management service should be able to provide all the mentioned features in case of central management server failure		
12	Support and RMA		
12.1	Proposed solutions including Firewall & Reporting Solution should include licenses required to support above mentioned features and functionalities along with 24x7 remote support directly from OEM and Next Business Day RMA replacement for 5 years.		

Annexure D
Compliance Sheet for technical Document

Srno.	Tender Requirement.	Document uploaded in Online Bid.
1	PAN, Certificate of registration for GST, Company /Firm Registration	
2	CA certificate mentioning Average Annual Turnover of 1 crore for last three financial years (FY - 2017-18, 2018-19, 2019-20).	
4	Letter stating that the Firm/Company is not blacklisted by Central / State Government, Government Corporation, statutory Institute. (On letter head of Firm)	
5	Bidder should be the authorized dealer of the original equipment manufacturer of Firewall. (Authorization letter from company)	
6	Firewall White papers/ Pamphlets/ Boucher for which you have quoted (Model number and specification)	
7	Supplied hardware & Software should not be declared end of life & support in the next 5 years. Bidder need to submit a letter from OEM along with the quote.	
8	Letter stating that Firm/Company has read all terms & conditions, and agreed with them. (On letter head of Firm)	
9	Bidder should produce experience letter in setting up similar firewall make OR model being supplied along with the sustenance support for the duration of the warranty period.	
10	Bidder should provide original OEM URLs/product catalogue references explicitly to each specification stated in this tender document. Generic URLs or one URL quoting for all required specifications strictly not allowed and may lead to disqualification during Technical bid evaluation.	


BOQ format

Sn	Specification	Qty	Rate	Amount
1	Next Generation Firewall covering all the required specifications with 5 years warranty Make (model): Palo Alto (PA850 or higher) OR Fortinet (600E or higher) OR Checkpoint (6600 or higher) Bidder can quote firewall models with higher configuration than listed.	1		


Note:-

- 1) Fill-up the Rates in BOQ provided online of Website www.mahatenders.gov.in
- 2) Technical and Commercial Bid to submitted online only. No physical Bid will be accepted.

Approved


1/4/21

(Kanhuraj Bagate, I.A.S.)
Chief Executive Officer
Shri Saibaba Sansthan Trust, Shirdi


01/04/2021
