



Bharatiya Vidya Bhavan's
Sardar Patel College of Engineering
(Govt. Aided Autonomous Institute Affiliated to University of Mumbai)
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai 400058.



Request for Proposal for Supply, Installation and Configuration of Next Generation Firewall

1. Sealed proposals are invited for **Supply, Installation and Configuration of Next Generation Firewall** for the Institute premises.
2. The vendors need to submit the most competitive bid for the items as per the RFP documents enclosed.
3. The quantities of each item in the BoQ, along with the unit prices in INR and the applicable taxes, should be indicated clearly in the proposal.
4. The submitted proposal shall remain valid for 15 days after the last date of submission.
5. The purchaser will conduct a technical evaluation and a commercial evaluation to compare the received proposals and determine the substantially responsive bidder before placing the PO.
6. Payment will be released within one week after a satisfactory installation and completion report from the technical team of the Institute.
7. The institute reserves the right to withdraw this RFP without assigning any reason.
8. A detailed RFP document is enclosed with this notice.
9. The proposals should be submitted in two parts: (a) Technical bid and (b) Commercial bid in separate sealed envelopes. The envelope containing both the bids should be submitted in one envelope to the **Institute Stores, Room No. 48, Ground Floor, on or before 24.07.2026 upto 5.00 pm.**

Date: 14.07.2026

Encl: As above




V.C. Principal
Bharatiya Vidya Bhavan's
Sardar Patel College of Engineering
(Government Aided Autonomous Institute)
Munshi Nagar, Andheri (W), Mumbai - 58



Request for Proposal Supply, Installation and Configuration of Next Generation Firewall

Sardar Patel College of Engineering (SPCE) intends to procure and deploy a Next-Generation Firewall (NGFW) solution to strengthen the security, visibility, control, and resilience of the Institute's network. The proposed solution shall protect Internet and internal network traffic, support secure user and application access, provide advanced threat prevention, encrypted traffic inspection, VPN, SD-WAN, reporting, logging, and integration with the Institute's existing network and authentication infrastructure.

The selected bidder shall supply, install, configure, integrate, test, commission, document, and support the complete firewall solution in accordance with this RFP. The proposed solution shall be scalable and suitable for the Institute's present requirements and future growth.

Refer to the following sections for technical specifications, scope of work, licenses, qualification and eligibility criteria for bidders, Service warranty and support and other relevant details.

A) Technical Specifications

Supply, Installation and Configuration of Next Generation Firewall (Qty.-1)	
Sr. No.	Technical Specifications
1	The proposed solution shall be an on-premises Next-Generation Firewall (NGFW) appliance based on a multi-core processor architecture with dedicated hardware acceleration for enhanced security processing and performance.
2	The offered NGFW solution shall provide a minimum of 8 × GE or higher-speed RJ45 copper interfaces and 4 × 10 GE SFP+ interfaces. Console, USB and management ports to access device in case of no network availability.
3	Minimum 16 GB RAM and 256 GB SSD local storage or higher.
4	Performance and throughputs: Firewall Throughput:- 20Gbps or higher Threat Protection:- 12Gbps or higher IPS Throughput:- 12Gbps or higher IPsec VPN Throughput:- 10Gbps or higher SSL/TLS Inspection Throughput:- 4 Gbps or higher Concurrent Users: Shall support a minimum of 800 concurrent authenticated users/devices and shall be scalable to accommodate future growth without performance degradation.
5	The offered NGFW Solution should support SSL/TLS 1.3 Inspection, Deep Packet Inspection, Application Control and Filter, Content Filter, URL and Web Filtering, Gateway Anti-Virus & Anti-Malware, Sandboxing / ATP performance, SD-WAN with SLA-based path selection using latency and packet loss, stateful packet inspection, Geo-IP Filtering, Command & Control Protection, Advanced Threat Protection
6	The offered NGFW Solution should support policy creation based on network, protocol, users, groups, applications and services
7	The offered NGFW Solution should support configurable zone-based architecture without fixed interface-to-zone mapping.
8	The offered NGFW Solution should support Local, Active Directory, LDAP, RADIUS authentication.
9	The offered NGFW Solution should support secure remote access VPN (SSL VPN) and standards-based IPsec VPN connectivity.
10	The proposed solution shall support load balancing, Quality of Service (QoS), bandwidth management and traffic shaping based on firewall policies, users/user groups, applications and web categories.

11	The offered NGFW Solution should support Real-Time Alert & Monitoring, Health Monitoring (CPU, Memory, Interface & VPN)
12	Management must be accessible via a web-based interface by any. The proposed solution shall support secure Command Line Interface (CLI) access for configuration, administration, monitoring and troubleshooting.
13	The proposed solution shall provide on-appliance and/or OEM-supported reporting and logging capabilities with a minimum of 30 days of log retention. It shall support log search, filtering, categorization and report export in commonly used formats such as PDF, HTML and/or CSV/XLS.
14	One/Two/Three-Year Subscription License for Firewall, Gateway Anti-Virus, Anti-Malware, DPI-SSL/SSL Inspection, Web/URL Filtering, Application Control, Botnet/C&C Protection, Advanced Threat Protection (ATP)/Sandboxing, Intrusion Prevention System (IPS), DNS Security, Threat Intelligence and Signature Updates, Reporting and Management, 24x7 Technical Support, Security, Software and Firmware Updates, and Advance Exchange Warranty for a period of one/two/three years.
15	The OEM shall have valid ISO 9001 certification and applicable information security management certification. The proposed firewall operating system/product family shall have valid Common Criteria certification. Documentary proof and applicable certificate scope shall be submitted with the bid.

B) Scope of the Work

1. The bidder shall supply, transport, insure, install, configure, integrate, test and commission the proposed NGFW appliance and all associated licenses and accessories.
2. The bidder shall integrate the firewall with the Institute's existing LAN, VLANs, Internet links, Active Directory/LDAP/RADIUS infrastructure, VPN and external Syslog server, wherever applicable.
3. The bidder shall migrate the existing firewall configuration, including security policies, NAT policies, address/service objects, VLAN interfaces, routing, VPN configuration, content filtering and application control policies, after validation with SPCE.
4. The bidder shall prepare and submit a detailed implementation plan, migration plan, rollback plan and acceptance test plan before deployment.
5. Installation and migration shall be carried out by OEM-certified engineers of the bidder/OEM with minimum disruption to the Institute's network services.
6. The bidder shall demonstrate all features specified in the technical specification and provide OEM datasheets/documentary proof for compliance.
7. The bidder shall provide architecture, configuration, deployment, policy, NAT, VPN, routing, logging, backup and troubleshooting documentation in electronic form.
8. The bidder shall provide administrator training and knowledge transfer to the SPCE IT team after successful commissioning.
9. Any hardware, software, transceiver, cable, license or accessory required for successful implementation but not explicitly mentioned shall be identified and quoted by the bidder.
10. The warranty/support period shall commence from the date of successful installation, commissioning and acceptance by SPCE.
11. Installation, Configuration and Final deployment must be done within 30 days of delivery of the product.

C) Licenses and Subscription

1. The proposed firewall shall be supplied with the one/two/three-year subscription covering 3 Year subscription license for Firewall, Gateway Anti-Virus, Anti-Malware, DPI-SSL/SSL Inspection, Web/URL Filtering, Application Control, Botnet/C&C Protection, Advanced Threat Protection (ATP)/Sandboxing, Intrusion Prevention System (IPS), DNS Security, Threat Intelligence and Signature Updates, Reporting and Management, 24x7 Technical Support, Security, Software and Firmware Updates, and Advance Exchange Warranty for a period of one/two/three years.
2. All specified security features and required licenses shall be included with no hidden or additional licensing costs.
3. The subscription shall include 24x7 technical support, security signature updates, threat intelligence updates, firmware/software updates and advance exchange hardware warranty for one/two/three years.

4. The bidder shall submit a detailed license Bill of Materials (BOM), including license name, SKU/part number, quantity and validity.
5. The firewall management solution shall be from the same OEM as the proposed firewall.

D) Qualification Criteria for Bidder and OEM

1. The bidder shall be an authorised partner/system integrator of the proposed firewall OEM and shall submit a tender-specific Manufacturer Authorisation Form (MAF).
2. The OEM shall have an established presence and technical support capability in India.
3. The bidder shall have OEM-certified technical engineers for installation, configuration and support of the proposed NGFW solution.
4. The bidder/OEM shall have local or readily available support capability in Maharashtra.
5. The bidder shall submit valid PAN and GST registration documentary proof.
6. The bidder shall submit relevant experience/performance details for supply, installation and commissioning of enterprise firewall/security solutions during the last one/two/three years.
7. The OEM shall provide documentary evidence for the quoted performance specifications and security features through official datasheets or technical documentation.
8. The proposed appliance and management solution shall be genuine, new and supported by the OEM.

E) Service Level Agreement - Warranty & Support

1. One/two/three years of 24x7 OEM/bidder technical support shall be provided for the complete firewall solution.
2. Critical security or firewall outage incidents shall receive immediate remote response and escalation to OEM TAC where required.
3. Faulty hardware shall be replaced under advance exchange warranty in accordance with the committed OEM support SLA.
4. Firmware updates, software updates, security patches and security signature updates shall be provided throughout the subscription period.
5. The bidder shall provide configuration assistance, troubleshooting and policy fine-tuning during the warranty/support period.
6. Periodic health checks shall cover CPU, memory, interfaces, routing, VPN, security services, logs, storage and overall appliance health.
7. The bidder shall maintain escalation details of the support team and OEM TAC and submit the escalation matrix to SPCE.
8. Configuration backup and restore procedures shall be documented and demonstrated to the SPCE IT team.
9. After installation, the bidder shall provide as-built documentation, configuration backup, network/security integration details, troubleshooting guide and administrator training material.

F) Performance and Acceptance Testing

1. The bidder shall demonstrate firewall throughput and security service capability using OEM-published documentation and validate the deployed configuration during acceptance testing.
2. Acceptance testing shall include Internet connectivity, routing, VLAN communication, NAT, security policies, user authentication, IPS, anti-malware, web filtering, application control, SSL/TLS inspection, VPN, SD-WAN, logging and reporting.
3. The solution shall be tested with all subscribed security services enabled in the production configuration.
4. Logging to the local appliance and integration with the external Syslog server shall be validated.
5. Administrator audit logs, report generation, log search, configuration backup and restore shall be demonstrated.
6. Any deviation identified during acceptance testing shall be rectified by the bidder before final acceptance.



ANNEXURE I - Bidder's Information

Name of the Bidder	
Address of the Bidder	
PAN No.	
GSTIN No.	
State of GST Registration	
Email ID	
Contact Person's Name & Designation	
Mobile No.	

ANNEXURE II – QUESTIONNAIRE

Sr. No.	Questions	Response
1	Whether all the terms and conditions of the SPCE document have been complied with. Compliance (Yes/No)	
2	Whether all the items specified in the technical specification have been compiled and quoted in the bidding engine. Compliance (Yes/No)	
3	Confirm that you have read all the instructions carefully and have complied with the instructions accordingly. Compliance (Yes/No)	
4	In case the bidder does not manufacture goods, they have submitted the Manufacturer's Authorisation letter. Compliance (Yes/No)	
5	Mention the Delivery period.	
6	Mention the Warranty of the material.	
7	Mention the HSN/SAC code of the material.	
8	Confirm availability of OEM TAC and escalation support in India. (Yes/No)	



ANNEXURE III – MANUFACTURING AUTHORIZATION FORM

Date:

Ref No.:

To,
The Principal
SPCE, Mumbai

Subject: Manufacturer Authorisation for Supply, Installation and Configuration of Next Generation Firewall

Dear Sir/Madam,

We, [Name of Manufacturer / OEM], having our registered office at [OEM Address], do hereby authorise [Name of Bidder / Partner Company], having its registered office at [Bidder Address], to quote, supply, install, configure, and provide support for our Next-Generation Firewall products against your RFQ No. [Reference Number] for the project titled: "Supply, Installation and Configuration of Next Generation Firewall for SPCE"

We hereby confirm that:

1. The products quoted by the bidder are genuine, new, and sourced directly from us.
2. We authorise the bidder to participate in the above-mentioned tender for our products.
3. We shall provide full technical support, firmware updates, and warranty support for a minimum period of 3 years as specified in the tender.
4. The products supplied shall comply with all technical specifications mentioned in the RFQ.
5. We confirm the availability of spare parts and technical support in India.
6. If the authorised bidder fails to fulfil its warranty obligations, we shall provide the necessary support directly or through our authorised service channels.

This authorisation is valid only for the above-mentioned tender.

For [OEM Name]

Authorized Signatory

Name:

Designation:

Email:

Contact Number:

Company Seal & Signature



Chairman - IT Infra. Committee
Sardar Patel College of Engineering