Annexure - 2

SPECIFICATIONS FOR NEXT GENERATION FIREWALL

SCOPE OF WORK

The CSIR-Indian Institute of Chemical Technology, Hyderabad, is a premier multi-disciplinary research Institute under the Ministry of Science and Technology (CSIR family institutes), Government of India.

Currently, the institute is looking for procuring a new firewall. The LAN/WAN security solution should offer advanced firewall support, SSL/TLS, intrusion prevention, application control, anti-malware protection, web protection, IPsec, VPN, and network protection.

The vendor can quote a single box or multiple boxes solution, which is a vendor choice that does not compromise overall performance.

Vendor should mention:

Make –

Model –

Country of Origin -

SN	REQUIREMENT
1	**OEM CRITERIA** This solution should be robust in accordance with the research institute's network environment. The proposed solution equipment should have a minimum life of 60 months (EOS) and an end-of-life (EOL) of 84 months (as of the supply date). The institute is currently requesting a 36-month subscription license for the solution.
	1. Manufacturer Authorization (MAF) is necessary for the proposed solution.
	2. OEM Support (TAC) Presence in India,should be in a position to provide 24x7 onsite support in Hyderabad.
2	**GENERAL FEATURES** 1. The firewall should support CLI and GUI-based access to the firewall modules.
	2. Should support Local authentication and integration with third-party authentication solutions like Active Directory, LDAP Server, RADIUS, TACACS+, e-Directory, and Kerberos
	3. Centralized, daily, automatic, manual or offline updates.
	4. Security and Software Updates
	5. Firewall should have advanced threat protection (detect and block network traffic when attempting to contact command and control servers).
3	**GENERAL REQUIREMENT** 1. It is necessary to have a 64-bit hardware platform built on a Multi-Core Architecture with Optimization for exceptional throughput for all key processes.
	2. Without effecting performance, the proposed solution should offer an alternative to inspect encrypted traffic flows and supporting TLS 1.3.
	3. The device should have security functions like a Firewall, VPN, Gateway level antivirus, Category-based web and application filtering, Intrusion prevention system, Traffic shaping, DoS, DDoS, Anti-Spam.
	4. The solution should offer a Central management solution with the option to manage multiple firewalls from day one. The Data Centre should be in India.
	5. The solution should support multi-factor authentication on the appliance or by using

	an external authentication server for VPN users, and the same MFA should also be applicable for the user portal and Web admin from day one.
	6. The solution must be capable of using multiple WAN links, including auto-link health check, automatic failover, automatic & weighted balancing, and granular multipath rules. It also needs to be able to support more than two ISPs.
4	**PHYSICAL INTERFACES** The firewall should meet firewall standards and should have the following Ethernet interfaces. Integrating these ports with a device unit or external integration solution is an option. A combination of flexible or fixed port modules may be used.
	1. 08 x 10GbE SFP+ with an MM module, with cables (MM LC-LC, 10Mt.)
	2. 08 x 1GbE copper with factory crimped CAT-6 UTP cables (10 Mt.)
	3. Local Storage /SSD should have minimum 250GB SSD (should have capability to at least store logs for 120 days)
	4. Management ports; 1 x RJ45 MGMT, 1 x COM RJ45, 1 x Micro-USB including connecting cables
	5. Multi-function LCD display
	6. 1 x USB 3.0 port, 1 x USB 2.0 port
	7. 19” rack mountable railing kit with screws
	8. 2 x hot-swap redundant power supply units with Indian Power Cord [Full loaded]
	9. Form Factor 1U or higher
5	**LICENSES** 1. 36 months Subscription licenses for Firewall
	2. Advanced Threat Protection
	3. Intrusion Prevention System (IPS)
	4. Anti-malware
	5. Web and App visibility control
	6. 24x7 on-site support
6	**SUPPLY, ON-SITE INSTALLATION AND TRAINING** 1. To ensure optimal performance as per the claim documentation, supply the equipment, on-site installation, configureand tune it, backup and restore the existing policy configuration.
	2. The vendor must examine the current firewall policy rules and create similar rules for the new firewall unit.
	3. Firewall Integration that is streamlined with the current network setup without any downtime.
	4. Expert-level training is necessary for the staff until they are well-versed in firewall operation.
	5. Complete installation and operational documentation is needed for the firewall.
7	**FIREWALL PERFORMANCE** 1. It is necessary for the firewall to have a minimum SSL/TLS inspection throughput of 18 Gbps.
	2. It is necessary for the firewall to have a minimum NGFW/Threat Protection

	throughput - (Measured with Firewall, IPS, Application control, Antispam, Malware prevention, etc. enabled) Minimum 25 Gbps or above.
8	**INTRUSION PREVENTION SYSTEM** 1. Intrusion Prevention System should have an IPS deep packet inspection engine with an option to select IPS patterns that can be applied to firewall rules for better protection. It should have the option to create a custom signature policy.
	2. Advanced threat protection, such as inbound and outbound SSL decryption.
	3. Botnet and malware protection, multiple attack correction, command, and control.
	4. Advanced intrusion prevention includes an allow list, block list, host quarantine, and IP defragmentation.
	5. DoS and DDoS prevention, heuristic-based detection, self-learning, and host-based connection limiting.
9	**WEB FILTERING** 1. Should have the flexibility to create a network, user, Web, and app-based traffic shaping (quality of service) policy.
	2. Exceptions based on defined network objects. Notification for custom messages or URL redirections.
10	**APPLICATION CONTROL** 1. The firewall should have a feature that can identify, permit, block, or restrict the use of applications beyond ports and protocols.
	2. The firewall should protect against potentially unwanted applications.
11	**LOGGING & REPORTING** 1. The logging retention period should be 60 months for internal/external/hybrid modes.
	2. Information about the firewall policy rule that triggered the log must be included in firewall logs.
	3. The firewall must provide, at a minimum, basic statistics about the health of the firewall and the amount of traffic traversing it.
	4. The firewall should have support to log all blocked connections or pass through the firewall in detail.
	5. It is important for the firewall to support the generation of performance statistics in real-time.
	6. The firewall must be capable of producing reports that measure usage.