Technical Specification

Sl. No.	Item Description	Test Results / Remarks
	System Specification:	
1	The firewall should be On-premise, Physical, 1U, 19" Rack Mountable Appliance.	Verified through physical inspection
2	Should have x86 based or equivalent multicore processor	Confirmation has been received in the form of the bidder's and OEM's self-declarations, submitted through the bid process.
3	The appliance should have minimum 4GB of RAM	Verified through OEM-provided data sheet
4	Should have minimum of 240GB SSD storage in the appliance	Verified through OEM-provided data sheet
5	Should be equipped with hot swappable redundant power supplies	Verified through physical inspection
6	Should have sufficient no of redundant fans	Verified through physical inspection
7	Should have at least 4 WAN Ports	Verified through physical inspection
8	Should have at least 8 x 1/2.5 GbE Copper ports	Verified through physical inspection
9	Should have at least 4 x 10G SFP+ ports, among them at least 4 should be populated with multimode 10G-SR transceivers. At least two such ports should be on LAN side	Verified through physical inspection
	Performance Parameters:	
1	The overall firewall throughput (mixed traffic) should be at least 25 Gbps	Verified through OEM-provided datasheet The 'iperf3' test was conducted from the ISI LAN to a standard public 'iperf3' server. However, we were able to test up to only 1 Gbps throughput, as the existing NKN link supports a maximum of 1 Gbps. **Summary of test:** While the uplink can reach up to 800 Mbps with negligible data loss, the downlink is experiencing approximately 45% packet drop at the same throughput level.
2	Should have Threat Prevention Throughput of at least 12 Gbps. Threat Prevention throughput must be measured with Gateway Anti-Virus/Malware, IPS, Application Visibility and Control (AVC) features enabled	However, to the best of our understanding, they currently exist without actively scanning any traffic. There were attempts in the past to enable them, but as of now, no tests could be conducted for this functionality. Vendor's help is required.
3	Should have Intrusion Prevention Throughput of at least 15 Gbps	Same as above (could not locate the graph/information, vendor's help is required)

4	Should be able to handle minimum 225K new sessions per second	Verified through OEM-provided datasheet. Please advise whether we should attempt stress testing for this functionality. If so, kindly suggest an appropriate test environment. Current traffic insight indicates a Max connection achieved as ~12K and average as ~6.5K connections on a 5 minutes timeframe based on our live traffic.Picture Attached.
5	Should be able to handle minimum 4M concurrent connections	Verified through OEM-provided datasheet. (Could not locate the specific graph/information, vendor's help is required). A snapshot of the related page is attached.
6	The TLS SSL DPI throughput should be minimum 6Gbps	Verified through OEM-provided datasheet. (Could not locate the graph/information, vendor's help is required). The picture of the SSL/TLS related page is attached.
7	Should support at least concurrent 50 Site to Site IPSec VPN Peers from day one and should have provision for support upto 6000 peers	Confirmation has been received in the form of the bidder's and OEM's self-declarations, submitted through the bid process. Currently 8 Site-to-Site VPN connections are active with our outlying centres. Picture attached.
8	Should support atleast concurrent 500 Client to Site IPSec VPN Peers from day one and should have provision for support upto 4000 peers	Three test connections are created for IPSEC Client-to-Site VPN in the current configuration. Picture attached.
9	Should support atleast concurrent 200 Client to Site SSL VPN Peers from day one and should have provision for support upto 1500 peers	No Client to Site SSL VPN is currently configured. Picture attached.
10	The overall VPN throughput should be minimum 5Gbps	Verified through OEM-provided datasheet. However, stress testing is currently underway. Please note that we are unable to test beyond 1 Gbps, as the current ISI uplink is limited to that capacity. Furthermore, ISI currently does not have active VPN users. Even when combining all CSSC team members, the maximum achievable load is limited to approximately 150 Mbps, as individual home internet connections are typically capped at around 30 Mbps. There is no scope for this test currently based on our connectivity and network traffic.
11	The firewall should be able to provide Threat Prevention Throughput of atleast 4 Gbps, when simultaneously supporting 20 concurrent Site to Site IPSec VPN sessions and 200 concurrent Client to Site SSL VPN sessions.	Confirmation has been received in the form of the bidder's and OEM's self-declarations, submitted through the bid process. Please advise whether we should attempt stress testing for this functionality. If so, kindly suggest an appropriate test environment. There is no scope for this test currently based on our connectivity and network traffic.

12	Firewall should be capable of acting as primary firewall for a reputed academic campus having more than 2000 users. The appliance should be equipped with enough hardware resources (including but not limited to CPU and RAM) to avoid any hardware contention issues, with usual traffic load	With the current usage (~400 Mbps), the firewall appliance is utilizing approximately 46% of RAM and 7% of CPU. Picture Attached. During a typical active 'iperf3' session with target throughput 1Gbps, the CPU usage increases to around 20–25% while achieving a throughput of 800 Mbps. RAM usage remains largely unchanged.
	Firewall Features:	
1	Solution should support Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Route-based VPN over OSPF, RIP, BGP	Verified through OEM-provided datasheet IPSec NAT Traversal and route-based VPN (configured using static routes) have already been set up.
2	Should be IPv6 Ready from day one	Verified through OEM-provided datasheet
3	The Firewall solution should support policy based routing, application based routing and multi-path routing	Verified through OEM-provided datasheet. Could not locate specific graph/interface to check the functionality.
4	Should support Application Visibility and Control (AVC), User Identity, Next Generation Intrusion Prevention System (IPS), Zero Day Protection/Advance Malware protection, HTTP/HTTPS Web content filtering, along with email filtering for spam and malware	Verified through OEM-provided datasheet. Picture with list of available services attached.
5	The NGFW should support stateful packet inspection and filtering technology with dynamic user-based NAT with provision to create rules based on source & destination IP address, hosts, network, IP range and Geolocation.	All these features are present as per the compliance declarations submitted by the bidder and the OEM. They have been partially implemented in the current configuration state.
6	Should provide policy-based traffic shaping by application. User, Group, IP address and Network	All these features are present as per the compliance declarations submitted by the bidder and the OEM. Testing is currently in progress. Features are shown as available in the appliance. Picture attached.
7	The Intrusion Prevention System should be integrated with the NGFW solution to enable it to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities, Should automatically update the signatures database from a central database server at least on a daily basis	All these features are present as per the compliance declarations submitted by the bidder and the OEM
8	Gateway level Anti-Virus/Malware solution should be appliance based and available from day one, The Firewall should scan for threats in inbound, outbound and intra-zone traffic for malware in files across all ports and TCP streams by Gateway Anti-Virus/Malware. In case there is any upper limit on size of files, potentially to be scanned, such upper limit should not be less than 30Mb	All these features are present as per the compliance declarations submitted by the bidder and the OEM

9	Should have the option to automatically update the new virus pattern updates. Gateway level Anti-Virus/Malware should be supported for HTTP,HTTPS, FTP, SMTP, POP3	All these features are present as per the compliance declarations submitted by the bidder and the OEM. However, the current configuration is inadequate to observe these features in action.
10	Compliance declarations submitted by the bidder and the OEM	All these features are present as per the compliance declarations submitted by the bidder and the OEM
11	Should support HTTP/HTTPS Web content filtering.	All these features exist as per the datasheet.
12	Should support various form of user authentication methods simultaneously, including Local Database, LDAP, and RADIUS, for Single Sign On	Compliance declarations submitted by the bidder and the OEM. Screenshot having list of available such services attached.
13	The Firewall should support deep packet SSL to decrypt HTTPS traffic for Scanning(IPS, Gateway Antivirus, Content Filtering, Application control) transparently for future requirement and then re-encrypt and send to destination if no threat found	All these features are present as per the compliance declarations submitted by the bidder and the OEM, and have also been verified through the OEM-provided datasheet. Testing is currently in progress.
14	Should have at least 5000 IPS Signatures ,3000+ application Signature and 80+ URL categories	Compliance declarations submitted by the bidder and the OEM
15	Should support device configuration and management through Web Console, CLI , SNMP and API integration	Verified through OEM-provided datasheet
16	Should support TCP/UDP protocols for syslog collection	Verified through OEM-provided datasheet. Syslog server has been configured. Picture attached.
	High Availability:	
1	The Firewall should be configured in an Active-Passive High Availability mode with real-time switch-over without any session being reset in case of malfunction	Configured but yet to be tested. Screenshot of the related page from the web console is attached.
	Certifications:	
1	The quoted Firewall model should be TEC certified	Verified through OEM-provided documents
2	Should have at least Common Criteria (India or Global)/NDPP/NSS/ICSALabs certification.	Verified through OEM-provided documents.
	Warranty and Licensing:	
1	The Firewall appliance (both active and passive units) including any additional hardware module associated to it supplied by the OEM at the time of installation must be covered under 3 years Onsite Comprehensive Warranty with Advanced RMA	Compliance declarations submitted by the bidder and the OEM. Also verified through the OEM portal.
2	OEM should have 24x7 TAC support with Toll Free number and R&D center in India. Refer to the service assurance terms mentioned under Scope of Work, specifically point no. 5	Compliance declarations submitted by the bidder and the OEM. Enhance Support has been provided. Screenshot from the Firewall web console attached.
3	License for all the software modules purchased with the appliance must be appliance based with minimum 3 years support	Compliance declarations submitted by the bidder and the OEM. Also verified through the OEM portal. Screenshot from the Firewall web console attached.

4	Crucial services like VPN (SSL and IPSec), networking, and Access & NAT rules should continue to work without any requirement for active license in an event of any license subscription of a software/hardware module getting expired	Compliance declarations submitted by the bidder and the OEM. Screenshot from the Firewall web console attached.
5	License for NGFW high availability with next generation firewall security applications, including intrusion protection, application control, URL filtering, Anti-Bot, Anti-Virus, DNS protection, advanced threat protection, cloud sandboxing and reporting etc., should be included from day one	Compliance declarations submitted by the bidder and the OEM. Web console page shows that the HA is configured. The functionality needs to be checked in the presence of bidder. Screenshot of the related page attached.
6	In case of a dispute in terms of performance parameters during commissioning and testing, the testing equipment e.g., traffic generator to test and verify the performance parameters should be provided by the bidder	
7	The solution should not go out of service in next 5 years starting from the date of purchase	Compliance declarations submitted by the bidder and the OEM.

Output of some commands suggested by the external expert:

1. **show ips-settings: output**
2. **system diagnostics utilities bandwidth-monitor: output**
3. **conntrack –L: output**