SPECIFICATION OF THE FIREWALL FOR THE SRI LANKA LAW COLLEGE

No	Minimum Specification	Bidder's Response	Technical Reference
		Yes / No (If No indicate your offer)	
1	Make		
2	Model		
3	Type of the firewall (Hardware/Software)		
4	Country of Origin		
5	The vendor should be in leaders quadrant as per last 5 years Gartner Reports for Unified Threat Management and Enterprise Firewall		
6	The vendor should be in leaders quadrant Gartner Reports for SD-WAN		
7	Vender should have ICSA certification for AntiVirus ,IPS, Firewall, IPSec and SSL VPN technologies		
8	The Firewall must be appliance based platform with security-hardened, purpose-built operating system		
9	The Firewall Appliance must include the Hardware Warranty , 24*7 vendor technical support and licenses for all the requested features and Softwares for 3 Years.		
10	The platform should use hardware acceleration architecture to optimize the packet, encryption/decryption and application level content processing.		
11	The Firewall should be able to upgrade using UTM feature licenses or downgrade to the basic license in the renewal.		
12	Licensing should be per device license for unlimited users for Firewall / VPN (IPSec & SSL) and other features. There should not have any user/IP/host based licenses – Please specify if the product does not follow the required licensing policy.		
13	Should support USB interfaces for config backup/restore, upgrading images and for connecting 3G Modems as fall-back.		
14	Should support more than one ISP with automatic ISP failover as well as ISP load sharing for outbound traffic.		
15	Should support inbuilt SDWAN functionality from day 1 and able to manage multiples ISP links using SD-WAN without additional licenses.		
16	No of concurrent users (200 minimum)		
17	Should have support for DHCP servers without any additional licenses.		
18	Should support L4-7 Server Load Balancing		

19	The platform must be capable of supporting a minimum of 4 configurable 1G copper interfaces for WAN links, 1 configurable 1 gigabit copper interface for DMZ links, 4 Copper interfaces for LAN Links		
20	The platform should support VLAN tagging(IEEE 802.1q) with about 4096 VLANs supported (in NAT/Route mode)		
21	The platform should support the standards based Multi-Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.		
22	The Firewall must support at least 1.5 Million concurrent connections		
23	The Firewall must support at least 35,000 new sessions per second processing.		
24	The Firewall should support Next Generation Firewall throughputs of minimum 1.0 Gbps for IMIX		
25	The firewall should support a minimum of at least 1.8 Gbps of Application control throughput		
26	Static routing must be supported		
27	Policy based Routing must be supported		
28	Dynamic Routing (RIP, OSPF,BGP & IS-IS) must be supported for both IPv4 and IPv6		
29	Multicast Routing must be supported		
30	Should support netFlow or sFlow		
31	It should be possible to operate the firewall in “bridge mode” or "transparent mode” apart from the standard NAT mode		
32	The Firewall must provide NAT functionality, including PAT.		
33	Should support “Policy-based NAT”		
34	Firewall should support Voice based protocols like H.323, SIP, SCCP, MGCP etc and RTP Pinholing.		
35	The Firewall should support User-Group based Authentication (Identity based Firewalling) & Scheduling		
36	Should support device and OS based policies		
37	IPv6 support for both NAT and Transparent Mode		
38	Should support dual stack architecture for both IPv4 and IPv6 traffic and routes , tunnelling IPv6 over IPv4, tunnelling IPv4 over IPv6 and IPv6 traffic over IPsec VPN		
39	Support for authentication at the firewall policy level (Local and Remote)		
40	Support for external RADIUS, LDAP and TACACS+ integration for User and Administrator Authentication		

41	Support for Native Windows Active Directory Integration		
42	Should support PKI / Digital Certificate based two-factor Authentication for both Users and Firewall Administrators		
43	The VPN should be integrated with firewall. Should support the following protocols DES,3DES, MD5, SHA-1,SHA-256, MD5, Diffie-Hellman Group 1, Group 2, Group 5, IKE v1/2, AES 128/192/256		
44	Should support Hub and Spoke VPN topology		
45	IPSec VPN should support XAuth over RADIUS and RSA SecurID or similar product.		
46	Should have integrated SSL VPN with no user license slab restriction. Please specify if the product does not follow the required licensing policy		
47	Should support SSL Two-factor Authentication with Digital Certificates		
48	Should support Single Sign-On Bookmarks for SSL Web VPN		
49	Should support Windows, Linux and MAC OS for SSL-VPN (Should have always-on clients for these OS apart from browser based access)		
50	Should support NAT within IPSec/SSL VPN tunnels		
51	Should also support PPTP and L2TP over IPSec VPN protocols.		
52	The device must support Active-Active as well as Active-Passive High Availability modes.		
53	The Firewall must support stateful failover for both Firewall and VPN sessions in High Availability.		
54	The HA Architecture should have the ability for Device Failure Detection and Notification as well as Link Status Monitor		
55	Should support VRRP and Link Failure Control		
56	The device must support Web UI (HTTP/HTTPS) and CLI (Telnet / SSH) based Management		
57	Should have configurable option to define remote access to the Firewall on any interface and restrict the same to a specific IP/Subnet (ie Trusted Hosts for Management)		
58	There must be a means of connecting directly to the firewall through a console connection (RJ45 or DB9)		

59	The device should have SNMPv2c and SNMPv3 support (for sending alerts to NMS in case of threats and system failures).		
60	Provision to generate automatic notification of events via mails / syslog		
61	Provision to send alerts to multiple email recipients		
62	Support for role based administration of firewall		
63	Should support simultaneous login of Multiple Administrators.		
64	Should have provision to customize the dashboard (eg: by selecting suitable Widgets)		
65	The Firewall must provide a means for exporting the firewall rules set and configuration to a text file via Web or TFTP		
66	Support for Image upgrade via FTP, TFTP and WebUI		
67	Should support system software rollback to the previous version during upgrade		
68	Should have a built-in Signature and Anomaly based IPS engine on the same unit		
69	Able to prevent denial of service and Distributed Denial of Service attacks.		
70	Should Identify and control applications (ie Application control feature)		
71	Should perform Traffic Shaping of popular P2P applications like KaZaa, Gnutella, BitTorrent, WinNY, eDonkey etc		
72	Should control popular IM/P2P applications regardless of port/protocol like Yahoo, MSN, Skype, AOL, ICQ etc		
73	Should support out of the box centralized real time and on demand reporting without firewall performance degradation		
74	Minimum One engineer should certified in high level for the product supplied. Please attach the certificate of the engineer.		
75	Vendor should operate 24/7/365 global Technical Assistance Center (TAC) with phone and e-mail support		
76	Vendor should have a customer portal which provides a knowledge base, maintenance versions, documentation, and hot fixes		
77	Vendor should provide escalation process through 24/7/365 staffed TAC		
78	Vendor should provide RMA for all hardware platform globally		
79	Vendor's RMA process should include next business day onsite replacement		
80	Comprehensive warranty for 1 years and Original Equipment Manufacture should have a local parts depot in Sri Lanka.		

Design ,Implementation and Support Services Requirements:

Sr. No.	Requirements	Compliance	Comments
1	Design should be categorized and completed in different levels and We should be able to add, edit or remove the requirements until the design document's sign off.		
2	The Implementation plan / Migration plan should have clearly defined roll-back plans to earlier working stage in any level to minimize any unplanned network outage.		
3	An offsite vender dependent training needs to be offered to minimum 1 technical staff to excel the administration of the product.		
4	The Managed Support Service Provider should be able to provide 24*7 support remotely and provide On-site support if required within 4-6 hours.		
5	The Managed Support Service Provider should provide the consultancy services for any solutions related requirements.		
6	24*7 Remote Support Services should be included for 3 Years.		
7	All the renewal agreements for consecative 3 years should be quoted (after the free remote support period)		