Item No.	Description of Specifications	Complied / Not Complied	Remarks (if any)
	General Requirements		
1	Make (Please Specify)		
2	Model (Please Specify)		
3	Firewall shall be in “Leaders” quadrant as per the latest 3 years Gartner report for Network firewalls		
4	Firewall shall have ICSA certification for Antivirus, IPS, Firewall, IPSec and SSL VPN technologies		
5	Firewall shall be an appliance based hardware platform which is optimized and purpose-built for high performance with a security-hardened, purpose-built operating system		
6	Firewall shall have enterprise license for requested features. User/IP/Host/Bandwidth based licenses will not be accepted		
7	Should include two identical firewalls in HA cluster configuration.		
9	Firewall shall have redundant power supply units		
10	Shall be 19” rack mountable		
	Interface and Connectivity Requirements		
11	Firewall shall have USB interfaces for backing up/ restoring configuration, upgrading software images		
12	Minimum 4 x 10Gbps SFP+ Interfaces		
13	Minimum 8 x 1Gbps SFP Interfaces		
14	Minimum 16 x 1Gbps RJ-45 Copper Interfaces		
15	Dedicated RJ-45 MGMT interface		
16	Dedicated RJ-45 HA interface		
	Performance Requirements		
17	Firewall shall support 3 million concurrent connections or higher		
18	Firewall shall support a minimum of 270,000 new sessions per second processing		
19	Firewall shall have following minimum performance for NGFW, IPS and Threat Prevention based on real-world Traffic Mix –		
20	NGFW Throughput - 3.5 Gbps		
21	IPS Throughput - 5 Gbps		
22	Threat Prevention Throughput - 3 Gbps		
23	SSL Inspection Throughput - 4Gbps		
	Network & Routing Requirements		
24	Shall support Static Routing		
25	Shall support Policy-based Routing		
26	Shall support Dynamic Routing (RIP, OSPF, BGP &IS-IS) for both IPv4 and IPv6		
27	Shall support Multicast Routing		
28	Shall support Net Flow or sFlow		
29	Shall be USGv6/IPv6 certified		

	Firewall Features Requirements		
30	Firewall shall be able to operate in standard NAT mode, bridge mode or transparent mode		
31	Proposed firewall shall provide NAT functionality, including PAT		
32	Firewall shall support Policy-based NAT		
33	Firewall shall support User-Group based Authentication (Identity based firewalling)		
34	Firewall shall have IPv6 support for both NAT and Transparent Mode		
35	Firewall should support the creation of up to 10 virtual firewalls on the device itself. Any required licenses should be included.		
36	Firewall should include a pre-defined database of internet services which can be referenced in the firewall policy		
	Authentication Requirements		
37	Firewall shall have support for user authentication (Local and Remote)		
38	Firewall shall have support for external RADIUS, LDAP and TACACS + integration for User and Administrator Authentication		
39	Firewall shall support for Native Windows Active Directory Integration		
40	Support PKI/Digital Certificate based two-factor Authentication for Firewall Administrators		
	Administration & Management Requirements		
41	Firewall shall support WebUI (HTTP/HTTPS) and CLI (Telnet/ SSH) based management		
42	Firewall shall have configurable options to define remote access to the firewall on any interface and restrict the same to a specific IP/Subnet (i.e. Trusted Hosts for Management)		
43	Firewall shall support connecting directly to the firewall through a console connection (RJ45 or DB9)		
44	Firewall shall have SNMPv2c and SNMPv3 support		
45	Firewall shall have provision to generate automatic notification of events via mails/syslog		
46	Firewall shall have provision to send alerts to multiple email recipients		
47	Firewall shall support for role based administration of firewall		
48	Firewall shall support simultaneous login of multiple Administrators		
49	Firewall shall have provision to customize the dashboard by selecting suitable Widgets etc		

50	Firewall shall provide a means for exporting the firewall rule set and configuration to a text file via Web or TFTP		
51	Firewall shall support for image upgrade via FTP/TFTP or WebUI		
52	Firewall shall support system software rollback to the previous version during upgrade		
53	Firewall should include one or more Two Factor Authentication (2FA) mobile soft tokens, that can be assigned to admin users. This should be expandable to other users by purchasing more tokens in the future, if required.		
	IPS and Application Control Requirements		
54	Firewall shall have built-in Signature and Anomaly based IPS engine on the same unit		
55	Firewall shall be able to mitigate denial of service attacks		
56	Firewall shall be able to mitigate buffer overflow attacks		
57	Firewall shall be a Certified IPS by an independent certification/testing body such as NSS Labs and ICSA		
58	Firewall shall identify and control applications		
59	Firewall shall control popular IM/P2P, social media, malware, applications regardless of port/protocol		
60	Firewall shall be able to control access to cloud-based applications and should able to route the specific apps via different WAN links based on the jitter and latency on the link		
	Gateway Antivirus		
61	Firewall shall facilitate embedded gateway antivirus support		
62	Firewall shall include anti-spyware and worm prevention		
63	Gateway antivirus shall support real-time detection of viruses and malicious code for HTTP,HTTPS, FTP,SMTP, SMTPS,POP3 and IMAP protocols		
64	Firewall shall have configurable policy options to select what traffic to scan for viruses		
65	Firewall shall have options to prevent user downloads based on file extension as well as file type		
66	Firewall shall have the ability of antivirus scanning for IPv6 traffic		
	Web Content Filtering Requirements		
67	Firewall shall facilitate embedded web content filtering feature		

68	Web content filtering shall work independently without the need to integrate with an external proxy server		
69	Web content filtering shall have the facility to block URLs based on categories		
70	Web content filtering shall support HTTP and HTTPS traffic		
71	Firewall shall be able to block URLs hosting spywares/adware etc		
72	Firewall shall be able to block different categories/sites based on User Authentication		
73	Firewall shall have options to customize the “Blocked Webpage Message” information displayed to end users		
74	Firewall shall be able to detect DNS-based spoofing attacks		
75	Firewall shall include DNS filtering feature to block DNS requests to known botnet C&C domains		
76	Firewall shall support category based DNS filtering		
77	Firewall shall support YouTube video filtering based on pre-defined categories and based on YouTube channel IDs.		
	Encryption & VPN Requirements		
78	Firewall shall have integrated VPN that support the following protocols DES, 3DES,MD5,SHA-1, SHA-256, MD5, Diffie-Hellman Group1, Group2,Group 5, IKE v1/2, AES 128/192/256		
79	Firewall shall support Hub and Spoke VPN topology		
80	Firewall shall have integrated client and portal based SSL VPN with no user license slab restriction.		
81	Firewall shall support SSL two-factor authentication with Digital Certificates or Hardware/Mobile tokens		
82	Firewall shall support Single Sign-On Bookmarks for SSL Web VPN		
83	Firewall shall support Windows, Linux and MAC OS for SSL-VPN.		
84	Firewall shall support NAT within IPSec/SSL VPN tunnels		
85	Firewall shall support L2TP and VXLAN protocols over IPSec VPN tunnels.		
	Other Requirements		
86	Firewall shall have option to configure traffic shaping. It shall have provision to define guaranteed bandwidth and maximum bandwidth		
87	Firewall shall support Gateway Data Loss Prevention (DLP) feature for popular protocols like HTTP, HTTPS,FTP,POP3,IMAP, SMTP, POP3S, IMAPS, SMTPS etc		

88	Gateway Data Loss Prevention feature shall support popular file types like MS-Word, MS- Excel, MS-PowerPoint and PDF		
89	Firewall shall support packet capture/sniffer to capture and examine the contents of individual data packets that traverse the firewall		
90	Firewall shall include automation capabilites in order to take automated action based on defined triggers.		
91	The automation feature should be able to trigger actions based on specific log events, CPU/Memory high incidents, license expiry, compromised host detection and HA failover.		
92	Firewall shall include Content disarm and reconstruction (CDR) capabilities to sanitize Microsoft Office documents and PDF files by removing active content, such as hyperlinks, embedded media, JavaScript and macros from the files without affecting the integrity of its textual content.		
93	Firewall should include email filtering capabilities with the ability detect spam based on IP address, URL and email checksums.		
94	Firewall should provide protection against the latest botnets by preventing communication with external command & control (C&C) servers.		
95	Firewall should provide protection against zero day attacks through sandboxing capabilities and virus outbreak protection services against latest emerging threats.		
96	Firewall shall include in-built SD-WAN feature set without the need for any additional licenses. Should be mentioned as a “Leader” as per the latest 3 years Gartner report for WAN edge infrastructure.		
	High Availability Requirements		
97	Proposed firewall shall support Active-Active as well as Active-Passive redundancy by use of 02Nos. of independent Firewall appliances.		
98	Proposed firewall shall support stateful failover for firewall sessions		
99	High Availability Architecture shall have the ability for Device Failure Detection and Notification as well as Link Status Monitor		
100	All required licenses and subscriptions should be included for firewall devices in HA configuration.		
	Cloud analyzer		
101	Solution should be proposed with a dedicated logging and reporting solution		

102	Logging and Reporting solution should support to integrate all NGFW devices included in the solution		
103	Logging and reporting solution should be cloud-based (SAAS)		
104	Proposed solution should be capable of handling minimum 7GB/day of logs per day.		
105	The solution should support adding more GB/day log capacity in the future by purchasing additional licenses		
106	The solution should be able to receive all logs from the proposed firewalls and should be able to retain the logs and generate historical reports.		
107	The solution should include a daily updated threat feed of bad IPs, URLs and domains which will be used to analyze the receved logs for any indicators of compromise.		
108	The solution should include the capabilty to create SOC playbooks for automating incident handling.		
109	Proposed solution should provide log storage for a period of 1 year.		
110	Should support out of the box Management reports for NGFW and should be able to create Custom report based on the custom database quarries.		
111	Should able view the current session details from the dashboard, including, Source, Destination, Country, Application, etc..		
112	Should support to generate the following customized reports for daily, weekly, monthly, yearly etc., and but not limited to link bandwidth utilization, device health monitors, security enforcements, system logins etc.		
113	Solution should provide the ability to schedule reports to run at non-peak hours or run-on demand and should be able to send the reports to intended recipients via email		
114	All reports must be exportable in PDF, HTML and CSV formats.		
	Vendor/Supplier Eligibilities		
115	Vendor shall operate 24/7/365 global Technical Assistance Center (TAC) with telephone and e-mail support.		
116	Original Equipment Manufacturer (OEM) of the proposed firewall shall have a local parts depot in Sri Lanka		
117	Vender's RMA (Return Material Authorization) process shall include next business day onsite replacement(With In one day)		

118	Bidder should have minimum of 03 certified engineers from the quoted brand.		
119	Vendor should have 5 years past experince in selling and maintaining proposed same brand in Sri Lanka. Documentary evidence should be provided.		
120	Bidder shall submit the Original Manufacture’s Authorization Certificate along with the bid		
	Warranty & Subscriptions		
121	Firewall shall have OEM authorized warranty / support services (TAC) for 24x7 for One (01) year		
122	Firewall shall have security subscription licenses from OEM for One (01) year. Bidder shall clearly provide the details on provided licenses.		
	Other		
123	Vendor should have 5 years past experince in selling and maintaining proposed same brand in Sri Lanka. Documentary evidence should be provided.		
124	Details of three recent clients using proposed brand should be provided with contact details		
125	Supply, install, commission, maintain, and connect to the existing core network in DMC, fulfilling the requirements specified by DMC.		