Implementation of Hardware firewall for CIPM Head Office Technical Specification

Product: Fortinet
Make: FortiGate
Model: FG400E

Technical and Functional Specifications			
S.No	**Specification**	**Compliance (Y/N)**	**Remarks**
Physical attributes			
1	The proposed vendor must have a track record of continuous improvement in threat detection (IPS) and must have successfully completed NSS Labs' NGFW Methodology v6.0 testing with a minimum exploit blocking rate of 99%		
2	Network security appliance should support "Stateful" policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc.		
Interfaces			
3	16 x GE RJ45, 16 x Gigabit Fiber (SFP) inbuilt interfaces from day one		
4	The Appliance should have atleast 1xUSB and 1xConsole Ports and 2 X management ports		
Performance and Availability			
5	Minimum 30 Gbps Firewall throughput, 2,000,000 concurrent sessions, and 400,000 new sessions per second support from day one		
6	Minimum IPS throughput of 6 Gbps & NGFW (Includes Firewall, Application Control and IPS) Throughput of 4 Gbps from day one on Enterprise Mix traffic		
7	Appliance should have minimum 4 Gbps of Threat prevention throughput		
8	IPsec VPN throughput: minimum 18 Gbps		
9	Minimum of 10000 firewall policies support		
10	Simultaneous IPsec VPN tunnels: 300		
11	Should have 200 SSL VPN peer support from day one		
12	The solution should have minimum 8GB of RAM and 4 Core CPU from day one		
Routing Protocols			
14	Should support Static Routes & Policy Based Routing		
15	Should support dynamic routing protocol like RIP, OSPF, BGP		
16	NGFW must support Secure SD - WAN feature along with advance routing protocols such as BGP		

17	Build-in SDWAN must be able to do load balancing of various links based on source address, User group, protocol and/or applications		
18	SLA for SDWAN must be defined based on packet loss or latency or jitter. Even combination of all 3 option must be possible		
Protocols			
19	IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP		
20	Allows secure deployment of next-generation IPv6 networks, as well as hybrid environments that require simultaneous, dual stack support of IPv4 and IPv6		
Other support			
21	Network Address Translation (NAT) shall be configurable as 1:1, 1: many, many: 1, many: many, flexible NAT (overlapping IPs). Reverse NAT shall be supported.		
22	The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should have at least 200 million rated websites and 75+ categories without external solution, devices or hardware modules.		
23	Should support features like Anti-Virus, APT Cloud, IPS,Web-Filtering, Application-Control, Gateway DLP from day one		
24	The product must support Layer-7 based UTM/Firewall virtualization, and all UTM features should be supported in each virtual Firewall like IPS, Web filter, Application Control, Threat Prevention, Content Filtering etc.		
25	Should support LDAP, RADIUS, Windows AD, PKI based Authentication & should have integrated two factor authentication server support from day one		
26	Should have a built-in Signature and Anomaly based IPS engine with minimum 7000+ IPS Signature support from day one on the same unit & also the IPS should have DDoS and DoS anomaly detection and protection mechanism with threshold configuration.		
27	Should have integrated Application control solution & Should have identification support for at least 3000+ applications and the identification should be regardless of ports. The applications need to be predefined on the box.		
28	Should include the Antivirus, Anti Botnet, IP Reputation, Advance Threat Protection Functionalities.		
29	Should include the File disarm and reconstruction feature		
30	Should support real-time checksums DB of newly detected threats before AV signatures are available		

31	The solution should have inbuilt server load balancing functionality from day one		
32	The Firewall should have integrated solution for VPN and there should be no user based licensing for SSL VPN & IPsec VPN as well		
33	The solution should have the flexibility to write security policies based on IP Address & User Name & Endpoint Operating System		
QoS			
34	QoS features like traffic prioritization, differentiated services, should support for QoS features for defining the QoS policies.		
35	Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI, SSH, Console Port etc.		
36	Should support SNMPv1, SNMPv2, SNMPv3		
37	Should capable to provide a convenient method for alerting administrators when critical events are encountered, by sending e-mail alert messages to administrator defined e-mail addresses		
Reports			
38	Traffic Log(Forward Traffic, Local traffic and Sniffer traffic), Event Log (System, Router,VPN, SDWAN, User, EndPoint, HA), Security Log (Antivirus, Webfilter, Application control, Data leak prevention), Forticloud Summary reports, Email Sendig Reports Automatically.		
Certification			
39	Appliance shall be ICSA certified for Firewall, IPsec VPN functionalities		
40	Product OEM should have its own Technical assistance center (should not be outsourced) in India		
41	OEM should be in Leaders quadrant of Gartner's – in Latest Network Firewalls and UTM Magic Quadrant for the last five years.		
Support and Return merchandise authorization			
42	Vendor should operate 24/7/365 local & global Technical Assistance Center (TAC) with phone and e-mail support. During office hours, local language support center would be an advantage		
43	Vendor should be able to provide escalation process through 24/7/365 locally staffed TAC		
44	Vendor's RMA process should include next business day onsite 1-to-1 replacement		
45	User Training should be facilitated		
46	Manufacture authorization letter should be provided ***(Documentary proof must be attached)***		

Vendor Eligibility			
47	Firewall unit brand should be produced under the same brand for at least for last 05 years		
48	Should have at least 3 vendor certified Engineers who should have 3 or more years of experience with the same brand		
POC - Shortlisted Supplier			
49	POC for 1 month period with required features		
Financial Proposal of the product			
Item with Description		**Price (LKR)**	
1	Cost of FortiGate Firewall with 01 years comprehensive Unified Threat management		
2	Installation and initiation charges		
Support option			
1	24/7 Support for 1 year period		
2	8 to 5 Support for 1 year period		