Technical Specification for Next Gen Firewall

Sl.No.	Technical Specification
1. General	
a.	The appliance-based security platform should provide firewall, AVC, Anti malware, Anti-Bot, Ant-Spyware, URL and IPS functionality in a single appliance from day one.
b.	Proposed appliance shall have minimum 240 GB SSD drive;
c.	Multicore CPU architecture with a hardened 64-bit operating system to support higher memory with min 4 physical CPU cores on device and minimum 8 GB RAM on device or higher.
d.	Firewall should have option of redundant power supply for future requirement.
e.	
2. Sizing Parameters:	
a.	Should have 3 Gbps or more throughput with all features enabled Under Test Condition, 5 Gbps or more throughput in Real World/Prod Performance Under Test Condition and 3 Gbps or more Threat prevention throughput with enabling Application-ID/AVC, NGIPS, Anti-Virus, Anti-Spyware, Anti Malware, Anti-Bot, Zero- day attacks.
b.	Firewall should have at least 2 Gbps of VPN throughput.
c.	Firewall should support at least 20K new connections per second or more and shall support at-least 1 Million concurrent session/connection with all application control enabled.
d.	Proposed solution should support minimum 3 Gbps IPS throughput
e.	Proposed solution should support minimum 500 Mbps of TLS/SSL inspection and decryption throughput
f.	Proposed solution should support minimum 500K Deep packet inspection connection
g.	Proposed solution should support minimum 70K SSL Deep packet inspection connection
h.	No of VLANs - 200
i.	Minimum IPSec VPN peers - 500
3. NG Firewall Features:	
a.	Should support manual NAT and Auto-NAT, Static NAT, Dynamic NAT, Dynamic PAT.
b.	The firewall have the capability of identifying the network traffic of network hosts from both virtual and physical machines and their activities.
c.	Should be capable of detecting and blocking IPv4 and IPv6 attacks including capabilities like DNS security / equivalent.
d.	Solution should support capability to detect threats emerging from inside the network.
e.	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor.
f.	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).
g.	The proposed firewall shall perform application-based signature matching beyond the traditional hash base signatures for AVC.
h.	The proposed firewall shall be able restrict application traffic to its default ports to prevent evasive applications from running on non-standard ports.
i.	The proposed firewall shall be able to protect the user from the malicious content upload or download by application/protocol by enforcing the total threat protection for known and unknown malicious content such as virus, malware or a bad URL.
j.	Support NAT, PAT & Policy based NAT/PAT, Mapped IP (MIP) & Virtual IP(VIP).
k.	IPSec and SSL VPN Tunnelling
4	Data encryption support DES, 3DES, AES 128-, 256-bit
5	Support stateful HA in Active-Active or Active-Passive Mode

6	Tunnelling functionality Nat66 (IPv6-to-IPv6) & Nat 64 (IPv6-to-IPv4).
7	IP address assignment features PPPoE, DHCP
8	The proposed firewall should support Bi-directional raw TCP inspection that scans raw TCP streams on any port .
9	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.
10	Firewall must support Cloud based / On Prem Advanced Threat Protection solution from day one and both the solution should from same OEM.
11	The firewall should have ability to prevent potentially malicious files from entering the network and those files sent to the sandbox for analysis to be held at the gateway until a verdict is determined.
12	IPv6 features Syn Cookie, Syn-proxy DoS attack detection, SIP, RTSP, ALG's, BGP4, DHCPv6 Relay, GRE IPv4 to IPv6 tunnelling.
13	System management and configuration Using web GUI/client based (without any limitation in number of clients), Command Line interface (console/SSH).
14	Supporting Protocols FTP, SMTP, HTTP, HTTPS, SNMP, UDP, ICMP, RPC, DNS, DHCP, ARP, TCP, POP3, IGMP, PIM.
15	Authentication protocols RADIUS, LDAP methods
16	Routing protocols Static, RIP, OSPF, OSPFv3 and BGP, BGPv6.
17	content filtering JAVA & ActiveX blocking
18	Proposed FW shall also support:
a.	DoS & DDoS prevention
b.	TCP reassemble for fragmented packet protection
c.	Brute Force attack mitigation
d.	SYN cookie protection
e.	Zone / Interface based IP spoofing
f.	Malformed packet protection
g.	Stateful packet inspection
h.	Detail logging and packet capture
19	Filtering of packets based on Source address, destination address, protocol type, user, port number, URL.
20	The Appliance OEM must have its own threat intelligence analysis centre and should also use the global footprint of security deployments for more comprehensive network protection
21	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location.
22	Solution should have the capability to integrate with other security solution like Network Admission Control (NAC) & SIEM. If additional license required for integration, then all required license should be available from day-1.
23	The Firewall Solution must have option of dedicated centralized analytics, logging & reporting from same OEM for future requirement. The solution should support customized reporting with the capability to create scheduled reports. The reporting platform must be accessible via a web-based interface / client-based GUI (without any limitation in number of client).
24	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools. All licenses required for above mentioned security solution must be activated from day one.
25	Interface Requirement:
a.	Minimum number of 1 Gbps Copper ports: 12 or more

b.	Minimum number of 10 Gbps SFP+ ports - 2 or More
26	License
a.	Warranty - 3 year comprehensive onsite warranty including 24x7 telephone, email and web-based technical support and should be extended to another 2 years
b.	Manufacturer's warranty should be mentioned minimum 05 (Five) years warranty including all services like GAV, IPS, Antispyware or antimalware, CFS, Application control, BoT protection , Advance Threat Protection, Patch & Firmware upgrade and Hardware.
c.	OEM should have scored minimum 97% in Exploit Block rate in the last NSS Lab report for NGFW (2019) and must be EAL4+/ICSA Lab certified for Network Firewall, Anti-virus and ATD
d.	The Firewall OEM must be ICSA Lab certified for Network Firewall, Anti-virus and ATD and should have detection rate of 99% or higher.
e.	The proposed appliance should come from firewall appliance family which has ICSA labs certification/NSS/NDP/ Indian Standard, IC3S/Common Criteria.
f.	The proposed appliance solution shall support cloud based Sandboxing technology for preventing zero-day threats with detecting 99.99% of previously unknown threats. Latest published report must be available in publicly.
g.	OEM should have TAC and R&D centre in INDIA with a Tollfree number.
h.	Supply, Installation, Integration, testing commissioning and training as per site requirements shall be done by the bidder.
i.	The bidder should have their registered office in Odisha Region to ensure immediate support during downtime.