Technical Specifications:

(To be submitted on the bidder's company letterhead along with the technical bid)

Sr. No.	Feature	Description	Complied (Yes/No)	Remarks
1	Make	Sophos [Sophos XGS 3300]		
2	Form Factor (RU)	1U Rack Mount		
3	Features	Layer 3–Layer 4 Firewall, NAT, VPN, Application Visibility and Control (AVC), User Identity, Next Generation Intrusion Prevention System (IPS), Zero-Day / Advanced Malware Protection, Web Security Essentials / URL Filtering		
4	Traffic Handled	TCP, UDP, HTTP, HTTPS, TCP/UDP-based applications		
5	Hardware Architecture & Performance	Multicore CPU architecture with hardened 64-bit operating system, minimum 16 GB RAM and dedicated co-processor with minimum 4 GB RAM for hardware acceleration. Appliance should support NG Protection, Application Control, IPS, DoS, SSL/TLS Inspection and Zero-Day Protection in a single platform. SSL/TLS inspection throughput should be 3000 Mbps or higher. Security Heartbeat should be able to restrict or isolate compromised systems until cleaned.		
6	NGFW Throughput	12000 Mbps or higher (Firewall, IPS and Application Control enabled)		
7	Threat Protection Throughput	10000 Mbps or higher (Firewall, IPS, Application Control and Malware Prevention enabled)		
8	Concurrent Sessions / Connections	13 million or higher		

Sr. No.	Feature	Description	Complied (Yes/No)	Remarks
9	New Sessions per Second	250,000 or higher		
10	General Management	Application acceleration support. XDR-ready with endpoint and server protection from the same OEM. Single management console for Firewall, Endpoint, Server, Email and Cloud Security. AI-driven static and dynamic file analysis using cloud sandboxing. Flexible user and group-based policies. Transparent proxy for anti-malware and web filtering. IPsec and SSL VPN support for Android and iOS with MFA. Minimum 1000 IPsec and 1000 SSL VPN users from day one. TLS 1.3 inspection support.		
11	Advanced Security Features	Advanced Threat Protection to detect and block C&C communication using multi-layer DNS and firewall inspection. Security Heartbeat for instant identification of compromised endpoints. Advanced web malware protection with emulation and real-time cloud threat intelligence. URL filtering database with millions of sites across 90+ categories backed by OEM labs.		
12	Type of Interface	GE Copper, SFP, SFP+		
13	1 GbE RJ45 Interfaces (from Day 1)	8 or more		
14	1/10 GbE SFP+ Interfaces (from Day 1)	4 or more (populated with 3 × 1 GbE Single Mode LC transceivers)		
15	Future SFP Interface Slots	6 or more		
16	Future 1/10 GbE	2 or more		

Sr. No.	Feature	Description	Complied (Yes/No)	Remarks
	SFP+ Slots			
17	IPsec VPN Peers (Site-to-Site)	1000 or higher		
18	IPsec VPN Peers (Client-to-Site)	1000 or higher		
19	SSL VPN Peers (Client-to-Site)	1000 or higher		
20	Storage Type	SSD		
21	Storage Capacity	200 GB or higher		
22	Power Supply	Single		
23	Processor Type	x86		
24	High Availability Support	Yes – Active-Passive HA with stateful failover		
25	Interface Expansion Slots	1 or more		
26	Firewall Policies License	Included		
27	Firewall License Features	Web Security Essentials / URL Filtering, IPS, Application Visibility, APT, Anti-Malware, C&C Protection, Geo-IP Protection, Zero-Day Threat Protection (from Day 1)		
28	IPS Signatures Supported	5000 or higher		
29	Security Intelligence	IP, URL, Domain, Geo-IP		
30	Certifications	ICSA / EAL4+ Certified, MTCTE from TEC India. Proposed NGFW must be listed in the Gartner Magic Quadrant (Network Firewall). Certificates		

Sr. No.	Feature	Description	Complied (Yes/No)	Remarks
		to be enclosed.		
31	Installation & Commissioning	Ability to restore existing firewall policies and configurations without third-party tools. The bidder must configure the firewall as per the scope of work.		
32	Documentation	Datasheet, technical specification sheet, administration guide and all supporting documents must be enclosed.		
33	OEM Warranty & Support	3 Years OEM License, Subscription and 24×7 TAC Support, including hardware warranty, firmware and security updates.		
34	Training	Moderate-level administrator training for the IT team covering firewall policies, VPN, HA management, monitoring and troubleshooting.		
35	Training Mode & Duration	On-site or remote training for a minimum of 1–2 working days with knowledge transfer and a Q&A session.		
36	Enhancement & Compliance	Any regulatory or compliance upgrades during the license period shall be supported without additional or hidden charges.		

Authorized Signatory (Bidder)

Name:
Designation:
Company Seal & Signature
Date: