TPWODL

CORRIGENDUM-I

Ref: Tender Enquiry No.: **TPWODL/RB/O/SER/078/CORRIGENDUM/001**, Date: 21.01.2022. Inviting reference to the above, the prospective bidders may note the following changes / modifications to relevant provisions of our Tender Notice & Tender Specifications.

1. **Modification to Annexure-II in technical Specification** :- Technical Specification for Internal Firewall is being attached .

SI. No	Specification Required	Complian ceYes / No	Remarks
	Technical Specifications for Internal Firewall		
1	Firewall must be a purpose build hardware delivering 50 Gbps of Firewall throughput and 9 Gbps of Threat Prevention Throughput. The devices should be quoted in HA		
2	Device must have 16 x 1 Gbe Ethernet Ports along with 4 x 10G ports from day-1 excluding Management and HA interface. Firewall device must have interface scalability for minimum 4 x 10G, 2 x 40G ports in future within the same appliances. Single Mode SFP (Fiber/Copper) for all ports needs to be provide		
3	The vendor must have a security gateway solution that can support the enablement of all next generation firewall security applications, including intrusion protection, application control, URL filtering, Anti-Bot, Anti-Virus.		
4	Appliance must be rack mountable.		
5	Firewall must have hot swappable dual power supply		
6	The device should support maximum concurrent sessions up to 12 Million and support 700K New Sessions/sec.		
7	Firewall vendor must be Leaders in Gartner magic quadrant for Enterprise Firewall for minimum 3 years.		
8	Integrated IPS must have 10,000+ up-to-date signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic pull or push signature update, threat encyclopedia integration.		
9	Solution must have DOS protection with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ ICMP session flooding (source/destination).		
10	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services: HTTP, HTTPS, SMTP, SMTPs, POP3, POP3s, IMAP, FTP etc.		
11	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.		
12	Solution must have Anti-bot capability using IP reputation DB to terminates botnet		

	communication to C&C servers.		
13	Solution should Inspect SSL encrypted traffic option for IPS, application control, antivirus and web filtering.		
14	Solution must Detect thousands of applications in different categories: Business, Cloud IT, Collaboration, Email, Game, General Interest, Mobile, Network Service, P2P, Proxy, Remote Access, social media, Storage/Backup, Update, Video/Audio, VoIP, Web Chat and Industrial.		
15	Custom application signature support must be available in Application control		
16	IPsec VPN: - Remote peer support: IPsec-compliant dialup clients, peers with static IP/dynamic DNS - Authentication method: Certificate, pre-shared key - IPsec Phase 1 mode: Aggressive and main (ID protection) mode - Peer acceptance options: Any ID, specific ID, ID in dialup user group - Supports IKEv1, IKEv2 (RFC 4306) - IKE mode configuration support (as server or client), DHCP over IPsec - Configurable IKE port - Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128. AES192, AES256, ARIA128, ARIA192, ARIA256, SEED - Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512 - Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14 to 21, 27 to 32 - Suite-B support: GCM128 and GCM256 - ChaCha20/Poly1305 PRF support: SHA1, SHA256, SHA384 and SHA512 - XAuth support as client or server mode - XAuth for dialup users: Server type option (PAP, CHAP, Auto), NAT Traversal option - Configurable IKE encryption key expiry, NAT traversal keepalive frequency		
17	Solution must support SSL VPN for thin remote clients equipped with a web browser only and support web application, such as HTTP/HTTPS Proxy, FTP, Telnet, SMB/CIFS, SSH. VNC, RDP, Citrix		
18	The Firewall should have integrated SSL VPN solution to cater to 300 SSL VPN concurrent users.		
19	IPv6 Support from day1- Management over IPv6, IPv6 routing protocols, IPv6 tunneling, firewall and UTM for IPv6 traffic, NAT46, NAT64, IPv6 IPsec VPN		
20	The proposed system shall have built-in high availability (HA) features without extra cost/license or hardware component		
21	The device shall support stateful session maintenance in the event of a fail-over to a standby unit.		
22	High Availability Configurations should support Active/Active or Active/ Passive		
23	Solution must ensure application availability and performance across multiple corporate WAN or across the internet to multi-cloud environments by leveraging WAN path failover, link aggregation, link remediation, and active path performance metrics. Solution should be capable enough to choose best link which meets performance expectations for a particular application and assigns packets or sessions to that WAN path.		
	The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route		

24	mode. Both modes can also be available concurrently using Virtual Contexts. Minimum 5 Virtual Firewall licenses to be provided with the solution and should be scalable to 10 Virtual Firewalls in future		
25	Proposed Solution must support category-based URL Filtering to control internet access for users, users must be displayed with customized block page when accessing restricted web category website.		
26	Proposed Solution should support working as Proxy for internet access to users.		
27	Security teams of TPWODL must be able to monitor and manage alerts and events from logs. Events should be processed and correlated in an easily readable format that analysts can understand for immediate response. Separate log server and Event Analysis Appliance must be provided.		
28	Virtual domain feature for partition of one physical firewall		
29	Centralized Logging and reporting solution must be proposed for internet and MPLS Firewall, supporting minimum 25 GB/day logging license. Software license can be proposed for Logging and reporting solution.		
30	Please mention Make, Model No. and Part Code		

2. Clause 1.3: Revised Calendar of Events shall be as mentioned below: -

Sr. No.	Calendar of Events	Existing Schedule	Revised schedule
1	Date by which interested and eligible vendors to pay tender fee and confirm participation in accordance with "Procedure /for participating in tender"	10.01.2022 Up to 15:00 Hrs	25.01.2022 Up to 15:00 Hrs
2	Last Date of receipt of pre-bid queries, if any	14.01.2022 up to 15:00 Hours	31.01.2022 up to 15:00 Hours
3	Last Date of Posting Consolidated replies to all the pre-bid queries as received	21.01.2022 up to 15:00 Hours	07.02.2022 up to 15:00 Hours
4	Last date and time of receipt of Bids	28.01.2022 up to 15:00 Hours	14.02.2022 up to 15:00 Hours

All other terms and conditions of the above tender will remain same.

By Order

Chief (Contracts & Store), TPWODL