# WEBEL TECHNOLOGY LIMITED

## CORRIGENDUM - I

## Tender No. WTL/SCRB/CCTNS/20-21/004 dated 27.07.2020

1. **Changes in Section –I, TECHNICAL SPECIFICATION WITH COMPLIANCE STATEMENT. Revise Section – I is enclosed.**

# WEBEL TECHNOLOGY LIMITED

## SECTION - I

## TECHNICAL SPECIFICATION WITH COMPLIANCE STATEMENT

(Tender No. WTL/SCRB/CCTNS/20-21/004)

- Bidder should submit all relevant data sheet/brochure of all quoted items and should also available in respective OEM's official website.
- Bidder should indicate items mentioned in the OEM data sheet / brochure by marketing as mentioned in minimum specification in the RFP

### 1. Minimum specifications for Next Generation Firewall

| | |
|---|---|
| **Quantity** | **02** |
| **Make** | |
| **Model** | |

| SL # | Minimum Specification | Specifications (Quoted / applicable by the bidder) | Compliance |
|---|---|---|---|
| 1 | The Firewall appliance should be a purpose-built appliance for multi-layered architecture with integrated next generation security functions like Firewall, IPS, Anti-virus, Anti-BOT, Zero-day protection and Application awareness. The product licensing should be device based and not user/IP based (should support unlimited users except for VPN). The Proposed solution must be considered amongst the industry leaders in the category of enterprise firewalls and must have achieved at least 97% of blocking rate for live exploits in last 1 year. The bidder must provide substantial reports from 3rd party independent industry analysts like Gartner and NSS Labs. | | |
| 2 | Throughput capacity of firewall should not be less than 40 Gbps and after enabling all the integrated functions, the appliance should be able to provide at least 10 Gbps of throughput under real-world enterprise condition. The solution should be able to provide a multi-layered scalable security for at least 10,000,000 scalable to 25,000,000 concurrent sessions. Appliance should support up to 300,000 new connections per second. Solution should be based on multi core processors and not on proprietary hardware platforms like ASICs. Should have minimum 32 GB memory with option of upgradable up to 64 GB. Hardware should have field upgradable capabilities for upgrading components like network cards, RAM, power supplies., etc. and should be provided with redundant power supply and fans | | |
| 3 | Solution should have following deployment modes mandatory: a) L3 Mode, b) L2/Transparent Mode. The solution should be deployed in High Availability. The appliance should have inbuilt storage of at least 1 TB configured in RAID. | | |

| | | | |
|---|---|---|---|
| 4 | Interface Requirement: 8 x 10/100/1000Base-T Copper Ports, 2 x 10G SFP+ ports from day 1 and support for addition of another 4 X 10G SFP+ or 2 x 40G QSFP ports. Dedicated Management and Sync Ports is required | | |
| 5 | Firewall Feature: solution should be based on "stateful inspection" technology and must support protection against SQL Injections, Cross-site Scripting, Session Hijacking, URL Tampering, Cookie Poisoning etc. Must allow security rules to be enforced within time intervals to be configured with an expiry date/time. The communication between the management servers and the security gateways must be encrypted and authenticated with PKI Certificates. The operating system of the proposed solution must not have any back-door vulnerability in last one year. | | |
| 6 | Solution must support IPv6 traffic handling on IPS and APP module, Firewall, Identity Awareness, URL Filtering, Antivirus and Anti-Bot. The solution must support dual-stack i.e., any host should be able to be configured with both IPv4 and IPv6 addresses simultaneously. All offered components (hardware and software) must be from single vendor. The Operating system should be hardened, purpose built and secured and must not have any backdoor vulnerability released in last one year | | |
| 7 | Solution must support gateway high availability and load sharing with state synchronization. Solution must support Configuration of dual stack gateway on a bond interface, OR on a sub-interface of a bond interface. Solution must Support 6 to 4 NAT, or 6 to 4 tunnels. | | |
| 8 | User Identity / Awareness: Must be able to acquire user identity from Microsoft Active Directory without any type of agent installed on the domain controllers. Must support Kerberos transparent authentication for single sign on. Must support the use of LDAP nested groups. Must be able to create rules and policies based on identity roles to be used across all security applications. The solution should have the inherent ability to detect multi-stage attacks. For the purpose of detecting multi stage attacks the solution should include static analysis technologies like antivirus, anti-malware/anti bot however in an integrate mode with the solution. The bidder or SI may use additional appliances (at max 2) for the solution but should be provided by the same OEM in the solution. | | |

| | | | |
|---|---|---|---|
| 9 | The solution should inspect the web sessions (HTTP and HTTPS both) to detect and notify the malicious web activity including malicious file downloads through the internet. Third Party/Separate appliance for SSL offloading will not be accepted. The proposed solution should dynamically generate real-time malware intelligence for immediate local protection via integration with the separate Automated Management and Event Correlation System. This Automated Management and Event Correlation solution must be from the same OEM. Solution should have an ability to remove all the active content and macros sending only a clean document to the end user. Solution should be able to detect & Prevent the Bot communication with C&C. | | |
| 10 | Solution should have an Multi-tier engine to i.e. detect & Prevent Command and Control IP/URL and DNS. Solution should be able to detect & Prevent Unique communication patterns used by BOTs i.e. Information about Botnet family. Solution should be able to detect & Prevent attack types i.e., such as spam sending click fraud or self-distribution, that are associated with Bots. Solution should be able to block traffic between infected Host and Remote Operator and not to legitimate destination. Solution should be able to provide with Forensic tools which give details like Infected Users/Device, Malware type, Malware action etc. | | |
| 11 | Security Management: A separate centralized management appliance needs to be provided for management and logging of NGFW appliance. In case other security components like APT solution etc. are from the same OEM then a single centralized management, logging (and not multiple management system) should manage all such security devices. | | |
| 12 | Security management application must support role based administrator accounts. Management must provide functionality to automatically save current state of Policy each time when any configuration changes in Security policy is enforced, and should have option to revert back to previous state stored state. It must be capable of storing at least last 5 policies. Management Solution must include a Certificate-based encrypted secure communications channel among all vendor distributed components belonging to a single management domain. The management must provide a security rule hit counter in the security policy. Solution must include a search option to be able to easily query which network object contain a specific IP or part of it. Solution must have a security policy verification mechanism prior to policy installation. | | |
| 13 | The Log Viewer should have the ability view all of the security logs of all functions managed by the solution in one view pane (helpful when troubleshooting connectivity problem for one IP address) | | |

| | | | |
|---|---|---|---|
| 14 | The Log Viewer should have the ability in the log viewer to create filter using the predefined objects (hosts, network, groups, users...). All the solution components should be provided 5 years comprehensive warranty and support from the OEM. | | |
| 15 | The bidders are requested quote for at least 1500 SSL VPN users' licenses from day 1 and can be scalable in future to support upto 5000 without any additional cost. The users should be able to authenticate locally from the Next Generation firewall and can also be integrated with Active Directory | | |

**2. Minimum Specifications for Layer 2 Switch**

| **Quantity** | **04** |
|---|---|
| **Make** | |
| **Model** | |

| **SL #** | **Minimum Specification** | **Specifications (Quoted / applicable by the bidder)** | **Compliance** |
|---|---|---|---|
| | Architecture | | |
| 1 | Shall be 19" Rack Mountable | | |
| 2 | 24 RJ-45 autosensing 10/100/1000 ports and 4 x1/10G SFP+ ports. The switch should have one console port. | | |
| 3 | Should have minimum 1GB SDRAM and minimum 12 MB Packet buffer size | | |
| 4 | Shall have switching capacity of 128 Gbps | | |
| 5 | Shall have up to 95 mpps switching throughput | | |
| 6 | The Switch should support minimum 32000 MAC address | | |
| 7 | The switch should support Traffic prioritization (IEEE 802.1p) to allows real-time traffic classification into eight priority levels mapped to eight queues | | |
| 8 | The switch should support Layer 4 prioritization to enable prioritization based on TCP/UDP port numbers | | |
| 9 | The switch should support Class of Service (CoS) to sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ | | |
| 10 | The switch should support Rate limiting to sets per-port ingress enforced maximums and per-port, per-queue minimums | | |
| 11 | The switch should Provide graceful congestion management | | |
| 12 | The switch should support Dual stack (IPV4 and IPV6) to transition from IPv4 to IPv6, supporting connectivity for both protocols | | |
| 13 | The switch should support MLD snooping to forward IPv6 multicast traffic to the appropriate interface | | |

| | | | |
|---|---|---|---|
| 14 | The switch should support ACL and QoS for IPv6 network traffic | | |
| 15 | The switch should support Access control lists (ACLs) - Minimum 2K ACLs to be supported | | |
| 16 | The switch should support RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping | | |
| 17 | The switch should support IP multicast snooping and data-driven IGMP.Should support PIM SM and DM. | | |
| 18 | The switch should support static routing, and policy based routing | | |
| 19 | The switch should support LLDP-MED (Media Endpoint Discovery) | | |
| 20 | The switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) | | |
| 21 | The Switch should support resilient stacking of minimum 8 switch spread across the building or campus. | | |
| 22 | The switch should support IEEE 802.1s Multiple Spanning Tree | | |
| 23 | The switch should support IEEE 802.3ad link-aggregation-control protocol (LACP) and port trunking | | |
| 24 | Should support encapsulation(tunneling) protocol for overlay network that enables a more scalable virtual network deployment | | |
| 25 | The switch should support SNMPv1, v2, and v3 | | |
| 26 | The switch should support Dual flash images | | |
| 27 | The switch should allow multiple configuration files to be stored to a flash image | | |
| 28 | The switch should support sFlow/equivalent | | |
| 29 | The switch should support Unidirectional link detection (UDLD) | | |
| 30 | The switch should support IEEE 802.1Q (4094 VLAN IDs) and minimum 2K active VLANs simultaneously | | |
| 31 | The switch should support Rapid Per-VLAN Spanning Tree (RPVST+) | | |
| 32 | The switch should support GVRP and MVRP/equivalent | | |
| 33 | The switch should support DHCP server. | | |
| 34 | The switch should support IEEE 802.1X | | |
| 35 | The switch should support Web-based authentication | | |
| 36 | The switch should support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per port | | |
| 37 | The switch should support Access control lists (ACLs) | | |
| 38 | The switch should support Source-port filtering | | |
| 39 | Shall support IEEE 802.3az Energy- efficient Ethernet (EEE) to reduce power consumption | | |
| 40 | Operating temperature of 0°C to 45°C | | |

| | | | |
|---|---|---|---|
| 41 | Safety and Emission standards including EN 60950; IEC 60950; VCCI Class A; FCC Class A | | |
| 42 | OEM should be leaders in Gartner magic quadrant report since last three years (wired and wireless) | | |
| 43 | Warranty - 5 years OEM | | |

Authorized Signatory (Signature In full): _____

Name and title of Signatory: _____

Stamp of the Company: _____