Surat Smart City Development Limited (SSCDL)
ADDENDUM AND CORRIGENDUM-1
Name of the work: - Bid for Supply, Installation, Configuration and Integration of Networking Equipments for DC [SSCDL-Network-01-2018]

The Bidders are requested to take note of the following changes made in the bid documents, which are to be taken in to account while submitting the bid. They shall be presumed to have done so and submitted the bid accordingly.

- This Addendum and Corrigendum-1 shall be the part of the bid documents.
- All items specified in this Addendum and Corrigendum-1 supersede relevant items to that effect as provided in the original bid documents. All other specifications, terms and conditions of the original bid document shall remain unchanged.
- The queries raised and given by bidders, but the clarifications are not made in this Addendum and Corrigendum-1 shall be considered to remain unchanged as per the terms and conditions mentioned in the original bid documents.
- **The bidders who have already submitted Technical and/or Price bid need to resubmit them.**

Highlighted Colour	What does it indicate?
No highlight	Indicates content as per original RFP document
Highlighted in Green	Indicates amendment as per this Addendum and Corrigendum

Bidders shall read and consider following points, which shall be a part of the bid documents.

Sr. No.	Tender Reference	Existing Clause	Amended / New Clause
1.	Page No.27, Section-6, Technical Specification, Item 2A & 2B	**Appliance Throughput**	**Appliance Throughput**
		Minimum 4.5 Gbps or higher Antivirus/Threat Protection Throughput	Minimum 4.5 Gbps or higher Threat Protection/Prevention Throughput with Firewall/Web Filtering+ Application Control+ IPS+ Malware/Antivirus Protection enabled in real world/Enterprise/Production traffic scenario.
		Minimum 4.5 Gbps or higher IPS Throughput	Minimum 4.5 Gbps or higher IPS Throughput in real world/Enterprise/Production traffic scenario.
		Minimum 4.5 Gbps or higher NGFW/UTM Throughput	Minimum 4.5 Gbps or higher NGFW Throughput with Firewall/Web Filtering + Application Control+ IPS enabled in real world/Enterprise/Production traffic scenario.

Note: Throughput Values must be mentioned in the OEM authorized Datasheet.

Bidder is required to submit the Technical Compliance for Item 2A & 2B as per below.

6. Technical (minimum) Specification

- The Bidder may participate in the bid by quoting for one, more or all the items depending on his techno-commercial capability to supply & support that range of products. Bidders are required to mention Make & Model of the product.
- The bidder can quote only one option (i.e. only one product can be quoted) against each item meeting or exceeding the below mentioned minimum specification.
- The bidder must clearly specify the features of the offered product vis-à-vis specification and deviation if any in the Column-C and Column-D of Table-I respectively.
- The exact make and model of the product offered must be specified in the Table-II provided.
- The technical spec sheet and the product brochure of the product offered should also be submitted along with technical bid.
- In case the space provided is not sufficient then a separate paper as per the format below can be annexed to the bid. The same must be duly signed and stamped.
- **The Technical Specification Sheet must be submitted separately on OEM's letter head as well as on Bidder's letter head (for all items). The same must be duly signed and stamped by authorized person of respective entity.**

Table-I			
#	**Description and Minimum Specification**	**Compliance /[Yes/No]**	**Deviation from Specification /Remarks if Any**
A	**B**	**C**	**D**
2A & 2B	**Enterprise Next Generation Firewall/Unified Threat Management [Required Quantity- 2 (1+1 in HA)]**		

Table-I			
#	Description and Minimum Specification	Compliance /[Yes/No]	Deviation from Specification /Remarks if Any
	Basic Criteria		
	• OEM should have support Centre in India.		
	• Appliance must be ICSA Labs certified for Firewall		
	Minimum Hardware Specification		
	• Minimum 2 x 10GbE SFP+ Ports form day 1 with 2 x 10G SFP+ Transceivers provided/included with product from day 1		
	• Minimum 8 x 1GbE SFP Ports from day 1 with 2 x 1G SFP Transceivers provided/included with product from day 1		
	• Minimum 8 x 1GbE RJ45/Copper Ports from day 1		
	• Minimum 2 x USB Port		
	• 2 x Integrated AC input Power Supply		
	• Minimum 1x Console Management Ports (RJ45) & should provide http, https, SSH, Telnet, SNMP based management console for managing and configuring		
	• Ports can be configurable for LAN/ WAN/DMZ		
	Appliance Throughput		
	• Minimum Firewall throughput of 35 Gbps or higher		
	• Minimum 2,50,000 New Sessions/sec		
	• Minimum 75,00,000 Concurrent sessions		
	• Minimum 4.5 Gbps or higher SSL VPN throughput		
	• Minimum 4.5 Gbps or higher Threat Protection/Prevention Throughput with Firewall/Web Filtering+ Application Control+ IPS+ Malware/Antivirus Protection enabled in real world/Enterprise/Production traffic scenario.		

Table-I			
#	**Description and Minimum Specification**	**Compliance /[Yes/No]**	**Deviation from Specification /Remarks if Any**
	• Minimum 4.5 Gbps or higher IPS Throughput in real world/Enterprise/Production traffic scenario.		
	• Minimum 4.5 Gbps or higher NGFW Throughput with Firewall/Web Filtering + Application Control+ IPS enabled in real world/Enterprise/Production traffic scenario.		
	General Features		
	• Should be appliance based and rack mountable.		
	• The Firewall should support "Route Mode" or "Transparent Mode" and support web proxy/ssl proxy		
	• Device in built DNS server for prevention of phishing and pharming scams involving DNS poisoning while reducing time taken for DNS mapping.		
	• Intrusion Prevention System		
	• Gateway Anti-virus		
	• Gateway Anti-spam with DLP functionality		
	• Web Content & Application Filtering		
	• Application Control		
	• Cloud Sandbox/Zero day prevention		
	• Botnet Blocking/Prevention		
	• Bandwidth Management/Traffic Shaping capable of setting guarantee bandwidth and maximum bandwidth per firewall policy		

Table-I			
#	**Description and Minimum Specification**	**Compliance /[Yes/No]**	**Deviation from Specification /Remarks if Any**
	• High Availability with Active-Active & Active-Passive mode support		
	• The High Availability should be supported in the Firewall from the day one and without any extra license.		
	• The Firewall should support Static, Policy Base, Identity based, Multicast routing and dynamic routing for RIP1 & 2, OSPF, OSPFv3, BGP4, RIPing, Server Load Balancing.		
	• The Firewall should belong to a family of products that attains industry standard Approved Certification and attains IPv6 Ready Phase 2 & IPv6 Certification		
	• Should support IPv6 ACL to implement security Policy for IPv6 traffic.		
	• Support for user authentication over SMS and in built two factor authentication without any additional cost.		
	• The proposed solution should support integration with Windows NTLM, Active Directory, LDAP, Radius, or Local Database for user authentication.		
	• Country Based Blocking, FQDN support and should support MIX mode deployment		
	• Should have an integrated wireless controller and should be able to manage multiple wireless access points centrally from web admin console.		
	• Should have feature/provision for Virtual System/Appliance/Domain or equivalent feature which splits the physical Appliance/domain into virtual by configuration/Software. (Optional).		
	• Should have Feature/module for Device Logging & Reporting and support for appliance/Hardware based Centralized Logging & Reporting Solution deployed additionally.		
	Gateway Antivirus, Anti-Spyware and Anti-Spam		

Table-I			
#	Description and Minimum Specification	Compliance /[Yes/No]	Deviation from Specification /Remarks if Any
	• Firewall must be able to scan http, https, IMAP, IMAPs, FTP, FTPs, POP, POPs, SMTP, SMTPs & MAPI protocols with AV signatures		
	• Virus, Worm, Trojan Detection and Removal, Automatic Virus signature database update, Real-Time blacklist, Redirect spam mails to dedicated email address, image-spam filter, Spam Notification, Zero hour Virus outbreak protection.		
	Web and Application Filtering		
	• The proposed solution should be able to enable or disable Web Filter per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS		
	• Should blocks web plug-ins such as ActiveX, Java Applet, and Cookies & Shall include Web URL block, Web keyword block, Web Exempt List		
	• The proposed solution must work as a HTTP proxy server with integrated Firewall, Anti-Virus, Anti-Spam, Content filtering, IPS.		
	• The proposed solution should be able to enable or disable Web Filter per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS		
	• The solution shall allow administrators to create multiple new local URL filtering categories besides dynamic categories		
	• Application Control Solution must provide option to create custom signature for applications & it should able to understand		
	• Well-known application like P2P, Voice, etc. without any dependency on the ports		
	Wireless Security and Control		
	• Should act as a wireless controller, Simple plug-and-play deployment of wireless access points (APs) - automatically appear on the firewall control centre, Central monitor and manage all APs and wireless clients through the built-in wireless		

Table-I			
#	Description and Minimum Specification	Compliance /[Yes/No]	Deviation from Specification /Remarks if Any
	controller, Support for IEEE 802.1X (RADIUS authentication), Wireless repeating with supported Aps.		
	Intrusion Prevention System (IPS)		
	• For different attacks like Mail Attack, FTP Attack, HTTP Attack, DNS Attack, ICPM Attack, TCP/IP Attack, DOS and DDOS Attack, Telnet Attack.		
	• Signatures: Custom, IPS Policies: Multiple, Custom, User-based policy creation, Automatic real-time updates.		
	• Should have a built-in Signature and Anomaly based IPS engine on the same unit and Anomaly based detection should be based on thresholds.		
	• Able to prevent denial of service and Distributed Denial of Service attacks on signature.		
	• Administrator shall be able to configure DoS policies that are used to associate DoS settings with traffic that reaches an interface based on defined services, source and destinations IP/Range.		
	Advance Threat Protection		
	• Advanced Threat Protection (Detect and block network traffic attempting to contact command and control servers).		
	• It must have facility to block Bot/Botnet attacks from day 1 & also should scan Mobile devices security from day 1.		
	Cloud based Zero day prevention or Sandboxing		
	• Solution should have support to inspect executables and documents containing executable content including .exe, .com, .dll, .docx, rtx, etc , and malware behaviour analysis and should support cloud based Zero day prevention or Sandboxing.		

Table-I			
#	Description and Minimum Specification	Compliance /[Yes/No]	Deviation from Specification /Remarks if Any
	VPN		
	• L2TP, PPTP, IPsec and SSL must be a part of Basic Appliance.		
	• The SSL VPN should be integrated solution and there should be no user based licensing for SSL VPN with SSL encryption/decryption.		
	• Firewall must have at least 400 SSL VPN client in Route mode from the day 1.		
	• The system shall support IPSEC site-to-site VPN and remote user VPN in transparent mode without any additional cost for VPN clients.		
	Load Balance		
	• For Automated Failover/Failback, Multi-WAN failover, High availability: Active-Active. QoS, OSPF, RIPv2, BGP, Policy routing based on Application and User support Round Robin Load Balancing		
	Bandwidth Management		
	• Application and user bandwidth management, Multi WAN bandwidth reporting, guaranteed bandwidth policy. Bandwidth for User, Group, Firewall Rule, URL and Applications.		
	Mobile application control and mobile malware protection		
	• Device should have feature to provide Security for Mobile devices protection for Apple IOS and Android environments which includes mobile application control and mobile malware		
	Monitoring and Reporting System		
	• Reports should be accessible through HTTP/HTTPS/Client based.		

Table-I			
#	**Description and Minimum Specification**	**Compliance /[Yes/No]**	**Deviation from Specification /Remarks if Any**
	• Should provide reports in Graphical/CSV/Excel/PDF format or cloud based.		
	License for UTM/NGFW		
	• The proposed solution must be licensed per unit for **5 years** with Full UTM/Enterprise subscription for IPS , Gateway Antivirus, Anti-Spyware, and Content/Web Filtering System, Applications Control, Cloud based zero day prevention/sandboxing, Mobile security, Botnet Prevention/blocking, Analysis & Management along with Logging & Reporting Solution. • Out of two devices one device is required **with 24x7 support** while other is required **With 8x5 support**.		

Place

Date :

Company stamp :

Signature of Authorized Person

Designation :

Name :