Corrigendum

Reference No: OCAC-NEGP-INFRA-0009-2017/17040

S.L. NO	Clause No.	Existing Clause	Amended/Modified Clause
1	Section I : 1.1 Scope of Work (B) Eligibility Criteria Sl No. 5	The bidder must have successfully undertaken at least the following numbers of systems implementation engagement(s) of value specified herein : - One project of similar nature(in system integration) not less than the amount Rs. 4,00,00,000/- (Four Crore Only) OR - Two projects of similar nature(in system integration) not less than the amount equal Rs. 2,25,00,000/- (Two crore twenty five lakh Only) each; OR - Three projects of similar nature(in system integration) not less than the amount equal Rs. 1,80,00,000/- (One Crore eighty lakh Only) each	The bidder must have successfully undertaken at least the following numbers of systems implementation engagement(s) of value specified herein : - One project of similar nature(in system integration) not less than the amount Rs. 4,00,00,000/- (Four Crore Only) OR - Two projects of similar nature(in system integration) not less than the amount equal Rs. 2,25,00,000/- (Two crore twenty five lakh Only) each; OR - Three projects of similar nature(in system integration) not less than the amount equal Rs. 1,80,00,000/- (One Crore eighty lakh Only) each Similar nature means "Supply, Installation and maintenance of Network & Security Equipments for Government / Public Sector Enterprises/BFSI in India in last three Years".
2	Section I : 1.1 Scope of Work (B) Eligibility Criteria Sl No. 7	Relevant documentary evidences like Authorization letters (MAF (Manufacturers authorization Form) from all OEMs whose products are being quoted by the Bidder need to be attached in the proposal)	Relevant documentary evidences like Authorization letters [MAF from all OEMs] to be submitted within 15 days after award of contract/purchase order whose products will be supplied.
3	Section IV: Technical Specifications 4.1 Technical specifications for Firewall, sl. No. 5	The appliance should support atleast 16* 10G ports and 4 * 40 G ports from Day one(all ports should be populated with required SFP modules).	The appliance should fitted with 16 x 10G ports and 4 x 40 G ports populated with required SFP modules.
4	Section IV: Technical Specifications 4.1 Technical specifications for Firewall, sl. No. 11	Solution should support both client and clientless SSL based VPN(MAC and IP binding), out of which 10 nos should work with client and 40nos with clientless VPN.	Solution should support both client and clientless SSL based VPN(MAC and IP binding).
5	Section IV: Technical Specifications 4.1 Technical specifications for Firewall, sl. No. 32	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality	Firewall should be IPV6 ready from day1. Firewall should support Nat66 (IPv6-to-IPv6) & Nat 64 (IPv6-to-IPv4) functionality.
6	Section IV: Technical Specifications 4.1 Technical specifications for Firewall, sl. No. 40	Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.	Solution should support network analysis capability to detect threats emerging from inside the network. This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.
7	Section IV: Technical Specifications 4.1 Technical specifications for Firewall, sl. No. 44	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 280 million of URLs in more than 80 categories	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than millions of URLs in more than 60 categories
8	Section IV: Technical Specifications 4.1 Technical specifications for Firewall, sl. No. 55	Firewall should provide application inspection for DNS, FTP, HTTP, SMTP,ESMTP,LDAP, VXLAN, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP with policy based.	Firewall should provide application inspection for DNS, FTP, HTTP, SMTP,LDAP, VXLAN, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP with policy based.
9	Section IV: Technical Specifications 4.1 Technical specifications for Firewall, sl. No. 56	Should support Remotely Triggered Black Hole for Border Gateway protocol security	Dropped

10	Section IV: Technical Specifications 4.1 Technical specifications for Firewall, sl. No. 61	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and tuning workflows
11	Section IV: Technical Specifications 4.1 Technical specifications for Firewall	New clause added	Management and advanced reporting (minimum 1 TB storage space for historical logs) functionalities with complete feature parity on firewall administration must be provided from day1.
12	Section IV: Technical Specifications 4.2 Technical specifications for NIPS, sl. No. 2	NIPS should be from different manufacturer as of Networking (Router-Switch) & Firewall OEM	NIPS should be from different manufacturer as of Firewall OEM
13	Section IV: Technical Specifications 4.2 Technical specifications for NIPS, sl. No. 5	Solution should provide stateful failover among devices for all components and should be completely automatic without any sort of manual intervention	Solution should support high availability.
14	Section IV: Technical Specifications 4.2 Technical specifications for NIPS, sl. No. 8	IPV6 Compliant: • Solution should be IPV6 ready. It should have IPV6 ready logo or similar certification from any other reputed third party. No extra cost will be borne for IPV6 implementation • Solution must support the complete STACK of IP V4 and IP V6 services	IPV6 Compliant: • Solution should be IPV6 ready from day1. No extra cost will be borne for IPV6 implementation • Solution must support the complete STACK of IP V4 and IP V6 attack services
15	Section IV: Technical Specifications 4.2 Technical specifications for NIPS, sl. No. 10	The IPS should be a dedicated purpose built hardware, not a part of Router, Firewall module and UTM solution with Real World Throughput 10 Gbps scalable upto 30 Gbps .All the signatures update subsrciption should be provided from Day1	The IPS should be a dedicated purpose built hardware with real World Throughput 10 Gbps scalable upto 30 Gbps .All the signatures update subscription should be provided from Day1
16	Section IV: Technical Specifications 4.2 Technical specifications for NIPS, sl. No. 13	Inspection Ports:16 x 10 GbE SFP+ , 4 x 40 GbE QSFP+ support. All ports should be configured with required transreceivers. Appliance should have additional ports for sinc, HA and other functionalities. -At least 8 Nos of ports should downgrade to 1Gb copper RJ45 Ethernet port through supplied transceivers. [8 No's Transcevicers are to be provide by the Bidder/ Supplier]. - Appliance should have supplied with Indian standard 3pin power cord. -Appliance should have supplied with necessary patchcord for HA, router, switch, firewall port for configuration. - Suppliers should ensured with flawless connectivity among devices like router, switch, NIPS, Firewall, server etc. - Device should be configured onsite by OEM with current SDC architechture and HP ArcSight SIEM solution as best practice.	Inspection Ports: Appliance should fitted with 16 x 10 GbE SFP+ support. All ports should be configured with required transreceivers. Appliance should have additional ports for sinc, HA and other functionalities. -At least 8 Nos of ports should downgrade to 1Gb copper RJ45 Ethernet port through supplied transceivers. [8 No's Transcevicers are to be provide by the Bidder/ Supplier]. - Appliance should have supplied with Indian standard 3pin power cord. -Appliance should have supplied with necessary patchcord for HA, router, switch, firewall port for configuration. - Suppliers should ensured with flawless connectivity among devices like router, switch, NIPS, Firewall, server etc. - Device should be configured onsite by OEM with current SDC architechture and HP ArcSight SIEM solution as best practice.
17	Section IV: Technical Specifications 4.2 Technical specifications for NIPS, sl. No. 17	Each appliance in the Solution should support and not limited to: • NIPS should be deployed in High Availability. It should support stateful high availability such that state information is shared between the HA appliance. In case one of the appliances fails state is maintained. • Active- Failover: The NIPS must support Stateful Active-Failover architecture for NIPS and high availability for redundancy with out using any third party or additional software or hardware	Solution should support high availability.

18	Section IV: Technical Specifications 4.2 Technical specifications for NIPS, sl. No. 18	Solution should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc	Solution should have the capability of easy rollbacks during the version upgrades etc
19	Section IV: Technical Specifications 4.2 Technical specifications for NIPS, sl. No. 22	NIPS should protect against SSL based attacks. NIPS should have built-in SSL decryption Engine for SSL Traffic decryption to support prevention of encrypted attacks - which includes attacks over secured http channel without need to have additional appliances	NIPS should protect against SSL based attacks. NIPS should have built-in/ 3rd party SSL decryption Engine integration capability for SSL Traffic decryption to support prevention of encrypted attacks - which includes attacks over secured http channel without need to have additional appliances
20	Section IV: Technical Specifications 4.2 Technical specifications for NIPS, sl. No. 40	**Following Classification Parameters should be supported in the Network Protection Policy:** • SRC Network Input • SRC Network • DST Network Input • DST Network • Port Group • Direction • VLAN Tag Group • MPLS RD Group	**Following Classification Parameters should be supported in the Network Protection Policy:** • SRC Network Input • SRC Network • DST Network Input • DST Network • Port Group • Direction • VLAN Tag Group
21	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 1	OEM should be present in Gartner's LEADER magic quadrant in the latest application delivery controller(ADC) report (2016)	OEM should be present in Gartner's LEADER magic quadrant in the latest application delivery controller(ADC) report (2016) or top 3 in IDC report.
22	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 3	Minimum Traffic ports supported: 2x 10 GbE SFP+ 8 x 1GbE RJ45 Layer 4 connections per second: Minimum 600,000 CPS Maximum Layer 4 concurrent connections: 12 million connection Layer 7 requests per second: Minimum 850,000 RPS	Minimum Traffic ports supported: Appliance should fitted with 8x 10 GbE SFP+ Layer 4 connections per second: Minimum 600,000 CPS Layer 4 concurrent connections: Minimum 12 million connection Layer 7 requests per second: Minimum 850,000 RPS
23	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 6	Following Server Load Balancing Topologies should be supported: • **Virtual Matrix Architecture** • Client Network Address Translation (Proxy IP) • Mapping Ports • Direct Server Return • One Arm Topology Application • Direct Access Mode • Assigning Multiple IP Addresses • Immediate and Delayed Binding • **IP Address Ranges Using imask**	Following Server Load Balancing Topologies should be supported: • Client Network Address Translation (Proxy IP) • Mapping Ports • Direct Server Return • One Arm Topology Application • Direct Access Mode • Assigning Multiple IP Addresses • Immediate and Delayed Binding
24	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 10	The SLB should support the below metrics: — **Minimum Misses**, — Hash, — Persistent Hash, — **Tunable Hash**, — Weighted Hash, — Least Connections, — Least Connections Per Service, — Round-Robin, — Response Time, — Bandwidth,	The SLB should support the below metrics: — Hash, — Persistent Hash, — Weighted Hash, — Least Connections, — Least Connections Per Service, — Round-Robin, — Response Time, — Bandwidth,
25	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 12	**VIRTUALIZATION:** The proposed SLB should have ADC-VX/Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. The Hypervisor used to virtualize the SLB hardware should be a specialized purpose build hypervisor, not a commercially available hypervisor (like XEN, VmWare etc.) with smaller footprint. Each virtual ADC instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management. The proposed device should have 2 Virtual Instances from Day 1 and scalable upto 24 Virtual Instances.	**VIRTUALIZATION:** The proposed SLB should have ADC-VX/Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. The Hypervisor used to virtualize the SLB hardware should be a specialized purpose build hypervisor, not a commercially available hypervisor (like XEN, VmWare etc.) with smaller footprint. Each virtual ADC instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management. The proposed device should supplied with minimum 16 Virtual Instances from Day 1.

26	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 16	A framework for customizing application delivery should be provided using user-written scripts, that provides the flexibility to control application flows and fully meet business requirements in a fast and agile manner. The proposed framework should enables to: • **Extend Server Load Balancer Fabric services** with delivery of new applications • Quickly deploy new services • Mitigate application problems without changing the application • Preserve infrastructure investment by adding new capabilities without additional equipment investment	A framework for customizing application delivery should be provided using user-written scripts, that provides the flexibility to control application flows and fully meet business requirements in a fast and agile manner. The proposed framework should enables to: • Extend Server Load Balancer Fabric services/network function virtualization with delivery of new applications • Quickly deploy new services • Mitigate application problems without changing the application • Preserve infrastructure investment by adding new capabilities without additional equipment investment
27	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 17	Should support Web Performance Optimization feature that should employ different acceleration treatments for different application and browser scenarios: a) Simplifying large, complex web pages. b) Caching c) Accelerate entire web transaction d) Third-Party timing and SLAs e) **Content Minification** f) Acceleration for mobile devices--Mobile Caching, Image resizing, **Touchtoclick conversion**	Should support Web Performance Optimization feature that should employ different acceleration treatments for different application and browser scenarios: a) Simplifying large, complex web pages. b) Caching c) Accelerate entire web transaction d) Third-Party timing and SLAs e) **Content Minification/content optimization** f) Acceleration for mobile devices--Mobile Caching, Image resizing, **Touchtoclick conversion/dynamic detect**
28	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 19	***The Server Load balancer should support the Application Performance Monitoring feature and should support the following:*** 1) Real user monitoring for any client with no agent software. 2) Centralized monitoring of performance across Local and Datacenter. 3) Measurement of real users and their actual transactions including errors – eliminating manual scripting of synthetic transactions 4) Diagram allowing to visually see which transactions breach SLA 5) Breaking down the measurements by specific application, location or transaction 6) SLA is user-defined – allowing full control over application 7) Ability to see which transactions were not completed due to errors.	*The Server Load balancer should support the Application Performance Monitoring feature and should support the following (using integrated or out of box solution without any additional cost):* 1) Real user monitoring for any client with no agent software. 2) Centralized monitoring of performance across Local and Datacenter. 3) Measurement of real users and their actual transactions including errors – eliminating manual scripting of synthetic transactions 4) Diagram allowing to visually see which transactions breach SLA 5) Breaking down the measurements by specific application, location or transaction 6) SLA is user-defined – allowing full control over application 7) Ability to see which transactions were not completed due to errors.
29	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 27	Should Support SSL Offloading & Acceleration on same hardware to reduce number of equipment in Data center & save power / cooling requirement	• Should Support SSL Offloading & Acceleration on same hardware to reduce number of equipment in Data center & save power / cooling requirement. • SLB should have minimum 30,000 SSL transactions per second for 2048 key from day one
30	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 35	The proposed WAF can be a dedicated appliance or part of ADC solution with minimal latency. • If WAF is a dedicated appliance, it should compliance with the above architecture of SLB.	➢ Proposed WAF should have minimum 1 Gbps throughput ➢ The proposed WAF can be a dedicated appliance or part of ADC solution with minimal latency. • If WAF is a dedicated appliance, it should compliance with the above architecture of SLB.
31	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 44	• Known Types of Attack Protection - Rapid Mode	Known Types of Attack Protection - Rapid / protection mode

32	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 58	Manipulation of IT Infrastructure Vulnerabilities	Dropped
33	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 59	3rd Party Misconfiguration	Dropped
34	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 82	SafeReply Security Filter	safe reply or masking of sensitive information in HTTP response filters
35	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer	Device Fingerprint-based tracking	Device Fingerprint-based tracking OR module to detect and prevent HTTP requests from ROBOTS or web spiders filters
36	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 94	WAF should support Device Fingerprint technology by involving various tools and methodologies to gather IP agnostic information about the source.	WAF should support Device Fingerprint technology OR robots and web spider filters by involving various tools and methodologies to gather IP agnostic information about the source.
37	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 95	Fingerprint information should include the Client Operating System, browser, fonts, screen resolution, and plugins etc.	*Fingerprint information should include the Client Operating System, browser, fonts, screen resolution, and plugins etc. (applicable for Fingerprint technology) OR Solution should provide advanced bot detection and prevention mechanism based on smart combination of signature-based and heuristic analysis*
38	Section IV: Technical Specifications 4.3 Technical specifications of Server load balancer, sl. No. 96	It should support running JavaScript on the client side. Once a JavaScript is processed, an AJAX request is generated from the client side to the WAF with the fingerprint information.	*It should support running JavaScript on the client side. Once a JavaScript is processed, an AJAX request is generated from the client side to the WAF with the fingerprint information (applicable for Fingerprint technology)*
39	Section IV: Technical Specifications 4.4 Technical specifications of 48 port 10G/40G Layer 3 Switch, sl. No. 5	Switch should support the complete STACK of IP V4 and IP V6 services. Switch must have IPv6 phase 2 ready logo certification.	IPV6 Compliant: • Solution should be IPV6 ready from day1. No extra cost will be borne for IPV6 implementation • Switch should support the complete STACK of IP V4 and IP V6 services
40	Section IV: Technical Specifications 4.4 Technical specifications of 48 port 10G/40G Layer 3 Switch, sl. No. 10	Proposed solution supplied with LC-LC loaded Fibre patch panel with 15 Mtrs Patch cord (Maximum of three Nos.) from switch ports side to patch panel.	Each Switch should be supplied with 10 nos. of 15 Mtrs LC-LC patch cord. 10 nos. of 10 Mtrs LC-LC patch cord. 10 nos. of 10 Mtrs CAT6 RJ45 patch cord. 10 nos. of 15 Mtrs CAT6 RJ45 patch cord Patch cord should be from OEM (AMP/CommScope /Rosenberger) with 25 years replacement warranty against any manufacturer defect
41	Section IV: Technical Specifications 4.4 Technical specifications of 48 port 10G/40G Layer 3 Switch, sl. No. 11	Proposed solution should supplied with 48 Nos of 10Mtr LC-LC patch cord with separate 25 nos of 10 Mtrs CAT6 RJ45 patch cord for existing copper switch.	
42	Section IV: Technical Specifications 4.4 Technical specifications of 48 port 10G/40G Layer 3 Switch, sl. No. 12	Patch panel and patch cord should have supplied with OEM like Tyco, commscope with 25 years of replacement warranty against any manufacturer defect	

43	Section IV: Technical Specifications 4.4 Technical specifications of 48 port 10G/40G Layer 3 Switch, sl. No. 18	Switch should have the following interfaces:i. 48 x 10G Fiber ports with SR modules Loaded ii. 6 x 40GbE /100GbE QSFP ports with Short Range Module Loaded for 40G operations with patch cord	Switch should have the following interfaces:i. 48 x 10G Fiber ports with SR modules Loaded ii. 6 x 40GbE ports with Short Range Module Loaded for 40G operations with patch cord
44	Section IV: Technical Specifications 4.4 Technical specifications of 48 port 10G/40G Layer 3 Switch, sl. No. 25	Switch should support for different logical interface types like loopback, VLAN, SVI, Port Channel, multi chassis port channel/LAG etc	Switch should support for different logical interface types like loopback, VLAN, SVI/RVI, Port Channel, multi chassis port channel/LAG etc
45	Section IV: Technical Specifications 4.4 Technical specifications of 48 port 10G/40G Layer 3 Switch, sl. No. 29	Switch should support minimum 1000 VRF instances	Switch should support minimum 500 VRF instances
46	Section IV: Technical Specifications 4.4 Technical specifications of 48 port 10G/40G Layer 3 Switch, sl. No. 32	Switch should support minimum 2 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) including the services: a. Switching b. IP Routing (Static/Dynamic) c. IP Forwarding d. Policy Based Routing e. QoS f. ACL and Other IP Services g. IP V.6 host and IP V.6 routing	Switch should support minimum 1.4 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) including the services: a. Switching b. IP Routing (Static/Dynamic) c. IP Forwarding d. Policy Based Routing e. QoS f. ACL and Other IP Services g. IP V.6 host and IP V.6 routing
47	Section IV: Technical Specifications 4.4 Technical specifications of 48 port 10G/40G Layer 3 Switch, sl. No. 35	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.	Switch should support multi OEM hypervisor environment and should support features for programmable configuration change
48	Section IV: Technical Specifications 4.4 Technical specifications of 48 port 10G/40G Layer 3 Switch, sl. No. 37	Switch should support VLAN Trunking (802.1q) and should support 4096 VLAN	Switch should support VLAN Trunking (802.1q) and should support 3900 VLAN
49	Section IV: Technical Specifications 4.4 Technical specifications of 48 port 10G/40G Layer 3 Switch, sl. No. 39	Switch should support minimum 96,000 no. of MAC addresses	Switch should support minimum 90,000 no. of MAC addresses

Bid submission date is extended till 20/10/2017, 2:00 PM. Subsequently revised timings are as follows:

Opening of Pre-Qualification Bids (PQ)	20/10/2017, 3:30 PM
Opening of Technical Bids (TB)	20/10/2017, 4:30 PM
Opening of Commercial Bids (CB)	To be Informed.

Other than above no amendments in the RFP are made.