Amendment-2 to "RFP ITW/05/2018-19 dated 25/01/2019 for Supply, Installation, Integration & Maintenance of FIREWALL & WEB SECURITY Solution in Canara Bank".

It is decided to amend the following in respect of the above RFP:

Bid Schedule (Page No. 2)

Events	Existing	Amended
	Time & Date	Time & Date
Last Date of Submission of Bids	02/03/2019, Saturday up to 3:00 PM	16/03/2019, Saturday up to 3:00 PM
Date and time of Opening of Part A- Conformity to Eligibility Criteria.	02/03/2019, Saturday up to 3:30 PM	16/03/2019, Saturday up to 3:30 PM

Sr No	Page No	Clause No	Existing clause	Amended Clause
1.	46	Annexure- 2	Eligibility Criteria Declaration	Amended Eligibility Criteria Declaration is attached
2.	9	10.2	At present, there is no network segregation for Internal & External traffic. Bank needs network segregation using virtual firewall technology and proposes the segregation of the traffic in 4 different zones i.e. ▪ Internal Inside (All servers accessed by branches/ Treasury wing), ▪ Internal Outside (Will be connected to MPLS Cloud) ▪ External Inside (All External/ Third Party facing servers) ▪ External Outside (All External/ Third Party connectivity's)	At present, there is no network segregation for Internal & External traffic. Bank needs network segregation using virtual firewall technology and proposes the segregation of the traffic in 2 Virtual firewalls in one box (Internal Firewall & External Firewall) i.e. ▪ Internal Inside (All servers accessed by branches/ Treasury wing) ▪ Internal Outside (Will be connected to MPLS Cloud) ▪ External Inside (All External/ Third Party facing servers) ▪ External Outside (All External/ Third Party connectivity's)
3.	53	Annexure- 7	Technical Specifications	Amended Technical Specifications is attached.

All the other Instructions and Terms & Conditions of the above RFP remain unchanged.

Please take note of the above Amendments while submitting your response to the subject RFP.

Date: 01/03/2019
Place: Mumbai

General Manager

Annexure-7
Amended Technical Specifications of Firewall & Web Security Solution

[Note: These details should be on the letter head of Bidder and should be signed by an Authorized Signatory with Name and Seal of the Company]

SUB: RFP for Supply, Installation, Integration and Maintenance of Firewall & Web Security Solution.
Ref: Your RFP ITW/05/2018-19 dated 25/01/2019

Note:

i. If the Bidder feels that certain features offered are superior to what has been specified by the Bank, it shall be highlighted separately. Information regarding any modification required in the proposed solution to meet the intent of the specifications and state-of-the-art technology shall be provided. However, the Bank reserves the right to adopt the modifications/ superior features suggested/ offered.

ii. The Bidder shall provide all other required equipments and/or services, whether or not explicitly mentioned in this RFP, to ensure the intent of specification, completeness, operability, maintainability and upgradeability.

iii. The selected bidder shall own the responsibility to demonstrate that the services offered are as per the specification/performance stipulated in this RFP and as committed by the bidder either at site or in bidder's work site without any extra cost to the Bank.

A. Technical Specification for Firewall & Web Security Solution

Sr No	Specification	Bidders Response (Yes/ No)
1	**General**	
1.1	The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operating system that eliminates the security risks associated with general-purpose operating systems.	
1.2	The firewall appliance should support Integrated IPS, Application control, Anti Virus and URL Filtering functionalities.	
1.3	The Licensing for all the components forming the solution should be per device and not user/ IP based.	
1.4	All devices as part of the solution must be from single OEM to avoid future support complexity.	
1.5	The security solution should be supported by OEM on 24x7x365 basis through a global Technical Assistance Center (TAC).	
1.6	The Support should be provided direct from OEM and not through any intermediate.	
1.7	The OEM should have published all the performance requirement on the corporate public website.	
1.8	During tenure all the Software/ Patch/ OS up gradation & Quarterly VAPT Remarks resolution should be done by the bidder/OEM with no cost to bank.	
1.9	All the licenses part should be applied to solution through central controller/ manager and not from cloud.	
2	**Firewall Performance & Features requirements**	
2.1	Security appliance should have a minimum 3.90 Gbps of Threat Protection/ Prevention Throughput with functions like Firewall, IPS, VPN, Antivirus and logging enabled (Enterprise Mix/ Real World Traffic).	
2.2	Appliance should have minimum 1,00,000 new sessions per second and minimum 3,00,000 concurrent sessions instead of 1,20,000 new sessions.	
2.3	Firmware/ Software/ Licenses Warranty Subscription: The above product should be covered under 6 years complete/ comprehensive warranty that includes firmware and software upgrades and all signature updates for all the	

CANARA BANK T.M. SECTION, TREASURY WING, BKC Mumbai-51.

	components supplied in the device.	
2.4	**Hardware Warranty : The above Hardware product should be covered under 3 years complete/ comprehensive warranty and & AMC period of 3 Years (If Contracted) that includes Hardware replacement within 4 hours in case of Hardware Device Failure.**	
2.5	The firewall should do stateful inspection & must also support asymmetric routing if required.	
2.6	Should support Policy based routing, Static Routing, OSPFv2, OSPFv3 & BGP routing protocols.	
2.7	Multicasting must be supported in device	
2.8	It should load balance & support automated Failover for 3 ISP's or more.	
2.9	Security solution must support IP, User & Device based policies.	
2.10	Security solution must integrate with Open LDAP, Radius, AD for user based policy & SIEM Solution.	
2.11	**Security solution should support at least 6 Virtual Systems/ Domains per box for Firewall virtualization & 4 Virtual Systems licenses per box from day one.**	
2.12	Should support Active-Active & Active-standby when deployed in HA.	
2.13	Should support IPv6 traffic & other IPV6 features required for future IPV6 migration from day one	
2.14	The Firewall must provide NAT functionality including Dynamic and Static NAT translations. It should be able to support Port Forwarding, PAT and DNS Translation.	
2.15	Solution should support IPv4 to IPv6 & IPv6 to IPv4 NAT functionality	
2.16	The Proposed system should support NTP, SNMP v2c and v3.	
2.17	Security solution should support integration with Firewall Analyzer like Algosec etc & NCCM like Everest etc.	
3	**Hardware Architecture**	
3.1	**The platform must be capable of supporting a minimum of 16 interfaces *10/100/1000 Base Copper interfaces (If any bidder is providing interfaces with SFP then bidder has to provide same number of RJ45 Copper Transreceivers) & 2* 10G SFP+ from day one (with 2*10G SFP+ Transreceivers) and Management, HA/ Sync etc ports must be additional.**	
3.2	Security solution must have local console port RJ45 and 1xUSB Port.	
3.3	Appliance should have minimum 8 Physical cores.	
3.4	Appliance should have minimum 32 GB of RAM.	
3.5	**Security solution must have either inbuilt integrated minimum 240 GB SSD storage in case external management server is available in proposed solution else should have integrated minimum 2x240GB SSD RAID1 of storage in case the proposed solution is not having Management server.**	
3.6	**Should support Hot Swappable Redundant Power Supplies & Fans.**	
3.7	**Mounting:** Product should be 1U or 2U Rack Mountable Chassis (Mounting kit, brackets to be supplied and fixed).	
3.8	**Bundling:** All the necessary connectors, external software media, manuals, Console Cable, India Standard Power Cable or any other hardware and software should be bundled and included for all operations listed above.	
3.9	**End of Support should not be within 6 Years from date of BID opening.**	
4	**VPN**	
4.1	Security solution must have minimum VPN throughput of 2 Gbps or more.	
4.2	Security solution must support IPSec & SSL VPN with default functionalities from day one.	
4.3	Should support the following IPSEC VPN deployment modes: Gateway-to-gateway, hub-and-spoke, redundant-tunnel, VPN termination in transparent mode.	
4.4	Security Solution must support following OS (MAC OS X, Microsoft Windows and 64 Bit Operating System) while connecting to Office using SSL VPN.	

5	Anti-Virus	
5.1	Security solution must have Gateway Antivirus features in it which must support scanning for protocols such as SMTP, POP, HTTP, HTTPs, FTP, SFTP.	
5.2	It should be capable to detect & prevent virus such as Trojan, Malwares, Malicious data etc at gateway level.	
5.3	Security solution should have capability for virus outbreak Detection and prevention using checksums to filter files.	
6	IPS	
6.1	It should support at least 5000+ signature Data Base for IPS & Subscription for new signatures download as and when required without any extra cost to bank.	
6.2	Security solution must have provision to create custom signatures for IPS & enter exception to exclude Advisory recommendation.	
6.3	Security solution must have the following minimum IPS controls for detection and prevention of drive-by exploits detection, Replacement message, fail-open, protocol decoders, signature rate count threshold and geography location filters.	
6.4	IPS must have capability to define filters based on Severity, target, OS, application, and/or protocol	
7	Management & Reporting	
7.1	Security solution must be centralized management framework. fully managed by Web browser or via client with full options to configure Routing, Policies, address object & UTM profiles	
7.2	The Firewall should support authentication protocols like LDAP, RADIUS and have support for firewall passwords, token-based products like RSA SecurID, RADIUS or TACACS+ authentication servers and digital certificates.	
7.3	The Proposed system should provide facility for Web based & Secure console based remote administration.	
7.4	Provision to generate automatic alerts via E-mails / Syslog.	
7.5	Support for Image upgrade & Backup via WebUI or TFTP.	
7.6	Analyzing network traffic with real time dashboard must be available within Security solution/ management itself.	
7.7	Security solution must support HTTPS, SSH, TELNET, SNMP based management	
7.8	Security solution should provide a holistic view into devices, traffic, applications, and events and the ability to stop a threat anywhere along its attack chain	
7.9	Centralized management and reporting framework should be supplied as Hardware Appliance/ Physical/ Virtual Server.	
7.10	Centralized management and reporting and appliance should have usable capacity of 2 TB after installing RAID 1 with provision for future expansion and should support 2GB logs per day capacity.	
7.11	Firewall must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes.	
7.12	The Firewall administration station must provide a means for exporting the firewall rules set and configuration.	
7.13	Role based administration with multiple administrators should be supported.	
7.14	Management should provide detailed Event Analysis for Firewall, IPS, VPN and Antivirus with reporting of all components.	
7.15	Detailed Event analysis including Source IP, Destination IP, Port, Type of Threat, CVE ID, Advisory Recommendations) for Threat Prevention Controls Anti-Malware, IPS, Application Control etc need to be provided with Real-Time and Historical reporting all the components.	

Date

Signature with seal:
Name :
Designation :

Annexure-2
Amended Eligibility Criteria Declaration

[Note: These details should be on the letter head of Bidder and should be signed by an Authorized Signatory with Name and Seal of the Company]

The Deputy General Manager
Canara Bank,
Technology Management Section,
Integrated Treasury Wing, 5th Floor, B Wing,
C 14 G Block, Bandra Kurla Complex,
Bandra East Mumbai 400 051Maharashtra

SUB: RFP for Supply, Installation, Integration and Maintenance of Firewall & Web Security Solution.
Ref: Your RFP ITW/05/2018-19 dated 25/01/2019

We have carefully gone through the contents of the above referred RFP and furnish the following information relating to Eligibility Criteria.

	Sr No	Eligibility Criteria	Documents to be submitted with Part A - Conformity to Eligibility Criteria	Bidder's Response and Documents Submitted
CONSTITUTION	a)	The Bidder should be a registered Company in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013.	Copy of Certificate of Incorporation and Certificate of Commencement of business in case of Public Limited Company OR Certificate of Incorporation in case of Private Limited Company, issued by the Registrar of Companies.	
OEM	b)	Bidders shall be the Original Equipment Manufacturers (OEM) of Solution (OR) An authorized dealer	If the applicant is a OEM, an Undertaking Letter has to submitted in this effect. OR If the bidder is an Authorized Dealer, an Authorization letter from their OEM to deal/market their product in India and it should be valid for a minimum period of 5 years from the date of submission of the Bid.	
FINANCIALS	c)	The Turnover of the Bidder should be minimum Rs. 10 Crores each year during last 3 years (i.e. 2015-2016, 2016-17 and 2017-18). The turnover must be individual company's turnover and not that of any group of companies.	Bidder has to submit Audited Balance Sheet for last 3 Years (i.e. 2015-16, 2016-17 and 2017-18).	
	d)	The Bidder should have Positive Net Worth as on 31/03/2018.	The Bidder must produce a certificate from the Company's Chartered Accountant to this effect.	

BIDDER EXPERIENCE	e)	The bidder should have supplied at least 15 Firewall & Web-Security Solution to Scheduled Commercial Banks, Govt Undertakings/ Depts, PSUs, NBFC, Stock Exchanges in India in last Three years (i.e. from 01/01/2016 to 31/12/2018).	Bidder has to submit Purchase Order Copies or Letters confirming the delivery/ Supply of the Firewall & Web-Security Solution from the Customers to this effect are to be enclosed.	
	f)	The Bidder should have their Own/ Franchise Service / Support Office in Mumbai & Bengaluru as mentioned in Annexure-4 of the RFP.	The Bidder has to submit the details viz., Address, phone no., email id and contact person Name & Mobile no. etc. as per Annexure-4.	
SOLUTION EXPERIENCE	g)	Minimum 5 Nos. of the Make of Firewall & Web-Security Solution (not necessarily the model) offered to Bank in this RFP should have been supplied to Scheduled Commercial Banks, Govt Undertakings/ Depts, PSUs, NBFC, Stock Exchanges in India in last Three years (i.e. from 01/01/2016 to 31/12/2018) (not necessarily by the bidder).	Bidder has to submit Purchase Order Copies or Letters confirming the delivery/ Supply from the Customers duly mentioning the make of the Firewall & Web-Security Solution to this effect are to be enclosed.	
DECLARATION	h)	The Bidder should not be a blacklisted/ debarred company as on date of submission of RFP by any Government entity, Bank or Financial Institutions.	Bidder should submit an undertaking letter to this effect in Letter Head stating.	

We confirm that the information furnished above is true and correct. We also note that, if there are any inconsistencies in the information furnished above, the bid is liable for rejection.

Date

Signature with seal
Name :
Designation :

केनरा बैंक CANARA BANK Mumbai-51. T.M. SECTION, TREASURY WING, BKC