RFP for Supply, Installation, Commissioning and Post Warranty Maintenance of IT Network Equipment

(Replies to bidders' queries)

RFP No. T-11014/23/2017-Tech/Vol-I dated 15.03.2018

Sr. No	Clause No.	RFP Pg. No.	Existing Provision in the Clause	Clarification Sought by bidders	Replies from UIDAI
1	**1.2.1**	**12**	Bid Submission End Date	**Query from the bidder –** Extension of time at least 2 weeks more	No change.
2	**2.3.2 (a)**	**20**	The Bidder shall submit an EMD of Rs 67 Lakh as bid security fee in a sealed envelope. EMD in any form will not be accepted.	**Query from the bidder –** Estimated cost	No change
3	**2.18 (4)**	28	Bidder shall have an average annual turnover of at least INR 90 Crores in last 3 financial years (FY 2014-15, 2015-16, 2016-17) from IT goods and services	**Query from bidder-** Request you to please give relaxation on it and amend this clause as under: Bidder shall have an average annual turnover of at least INR 80 Crores in the last 3 financial years (FY 2014-15, 2015-16, 2016-17) from IT Goods and services.	No change.

4	**2.18 (5)**	28	Bidder Experience in India	**Query from the bidder –** Formation of Consortium	No change.
5	**2.32 (3)**	**37**	Performance Bank Guarantee will be for a total amount equivalent to 5% of total contract value. Multiple PBGs shall be submitted which are as below a) 5% of total CAPEX cost and having validity till T_0+3 years and 5 months. However, PBG should remain valid for 60 days beyond CAPEX obligations. b) 1.25% of total OPEX cost having validity till T_0 + 4 Year and 5 Months. However, PBG should remain valid for 60 days beyond 4th Year AMC period for which revised PBG at later stage may be submitted if required. c) 1.25% of total OPEX cost having validity till T_0+5 Year and 5 Months. However, PBG should remain valid for 60 days beyond 5th Year AMC period for which revised PBG at later stage may be submitted if required. d) 1.25% of total OPEX cost having validity till T_0+6 Year and 5 Months. However, PBG should remain valid for 60 days beyond 6th Year AMC period for which revised PBG at later stage may be submitted if required. e) 1.25% of total OPEX cost having validity till T_0+7 Year and 5 Months. However, PBG should remain valid for 60 days beyond 7th Year AMC period for which revised PBG at later stage may be submitted if required. (T_o is date of issue of LoI/NOA by UIDAI)	**Query from the bidder -** 1) Whether you require PBG Validity To+3 years+ 2 month require or To+3 years+ 7 month require. Please confirm. 2) Also allow to bidder provide the AMC PBG after expiry of Product PBG, but submitting 15 days before the expiry of product PBG. Also confirm AMC PBG is valid for 1 year + 5 month or 1 year + 2 month.	PBG Validity would hold for the periods as mentioned in the relevant clauses of the RFP. For further clarity, the following explanation may be referred – PBG validity - **T_0 + X + Y + 60 days.** Where, X denotes the time from acceptance of NOA/LoI by the bidder to commencement of warranty. Y denotes contractual obligation period like 3 years for warranty, 3+1 year for 4th year AMC & so on. **Also, please refer corrigendum**.

6	**3.6 (1)**	**44**	The Vendor shall be responsible for installation, commissioning, testing and post warranty maintenance of IT Network Equipment at Data Centre at Hebbal, Manesar and two upcoming DCs including integration of IT hardware being procured via this RFP, through OEMs for all equipments of the bid.	**Query from the bidder -** Whether you require completion project through back to back OEM or Bidders? Please confirm.	Clause is explicit enough. No further clarification is considered necessary. Hence, no change.
7	**3.10.2 (1)**	48	This contract for "Supply, Installation, Commissioning and Post Warranty Maintenance of IT Network Equipment" shall start from date of acceptance of Notification of award by bidder (as per clause 2.30 of section II of RFP) and shall last till completion of 4th year of AMC. This includes warranty period of 3 years (36 months) in respect of equipment, and comprehensive AMC support (after 3 years of warranty) for equipment upto 48 months. In case product/equipment is not End of Support after expiry of contract, the purchaser may extend the contract upto 2 years or till the equipment is End of Support, whichever is less (after completion of 7 years from date of commencement of warranty) on same terms and conditions of this contract at the sole discretion of the Purchaser. The rate for such extension of AMC will be 7th year AMC cost.	**Query from the bidder –** Request to extend the project with mutual agreement.	No change.

8	**3.11.1**	43-44	The payments of Capex cost for goods shall be as under: i) 50% against delivery of all equipment and accessories. ii) 30% against installation and commissioning of all Goods/ Services iii) 10% against submission of ATRR by the bidder iv) Balance 10% on commencement of warranty or completion of 30 days from the date of submission of ATRR , whichever is early, subject to submission of Bank Guarantee of Equivalent amount and having validity till 3 years and 3 months from date of commencement of warranty.	**Query from the bidder –** Request you to please amend this clause as under: 1) 90 % Payment of the project value will released within 30 days from the date of delivery. 2) Balance 10% Payment will release after successful installation and commissioning along with submission of PBG as per tender. **Query from the bidder –** 80%-10%-5%-5%	No change. No change.

9	**3.31**	58	Payments shall be subject to deductions of any amount, for which the Vendor is liable under the agreement against this Bid.	**Query from the bidder –** In tender, no TDS is deducted. So, please remove this clause.	No change.
10	**4.1.2**	69-70	Manufacturer Authorization Form	**Query from the bidder –** Juniper Networks operates & sell products in India through Resellers & Partners. We do not deal directly or bid for project without the partners. Hence request some changes in the MAF. Draft MAF with changes recommended is as attached.	No change.
11	**5.3 (5)**	79	The Bidder should ensure that there is a 24x7 comprehensive onsite support arrangement during the currency of the contract with all the OEMs for respective components.	**Query from the bidder –** The Bidder should ensure that there is a 24x7 comprehensive onsite support arrangement during the currency of the contract with all the OEMs / OEM Authorized Partners for respective components.	No change.

				Query from the bidder – In Page no. 83, clause no.5.4.2.3 mentioned that Bidder shall provide 24* 7. Request you to please amend and mention OEM name rather than Bidder Name	No change.
12	**5.4.2.1**	82	Installation and Commissioning of all Hardware	**Query from the bidder –** Delivery, installation, and commissioning of the hardware/software along with associated peripherals in the Data Centre space provided by UIDAI through the respective OEM/ OEM Authorized Partner	No change.
13	**5.4.2.5**	84	Ongoing Maintenance and support services	**Query from the bidder –** The successful bidder/ vendor shall provide onsite support at the Data Centres of UIDAI at Hebbal, Manesar and two upcoming DCs through OEMs/ OEM Authorized Partner for all equipments of the bid	No change.
14	**6.5.1 (16)**	105	SSL TPS more than 20k with RSA 2k key and 100k with ECC	**Query from the bidder –** Seems to be Typo Error.	Pl refer corrigendum.

				a) 3 out of 4 OEM's allowed DON'T have appliance which meets the ECC : 100K TPS requirement. Hence, unable to participate. b) As an Industry benchmark, the ECC value should be half of the RSA i.e. if RSA 2k TPS: 20k then ECC must be 10k TPS. c) In order to meet the 100K ECC requirement, the qualified OEM has to quote the Highest Model which would not be Commercially viable option considering the other sizing parameters pertaining to mid size product. Hence, please dilute this clause in order to allow competition & get healthy techno-commercial offer. **Suggested Clause**:- SSL TPS more than 20K with	

				RSA 2k key and 10k with ECC	
				Query from the bidder – There is a huge difference in the asked SSL TPS nos. with RSA vs ECC. With the given compression levels and SSL throughputs, 100K ECC TPS is not possible. We request you to revise the same to 20K (instead of 100K) for ECC	Pl refer corrigendum.
				Query from the bidder – It seems Typo Error as ECC SSL TPS will be almost half of the RSA 2K key SSL TPS. Request to change clause as "SSL TPS more than 20K with RSA 2k key and 10k with ECC"	Pl refer corrigendum.
				Query from the bidder – SSL TPS are calculated in proportion with the L4 and L7 Throughput. As per the throughput	Pl refer corrigendum.

				specification asked in the RFP, SSL TPS of 12K with RSA 2k key and 6k with ECC is suggested . Pl modify as “SSL TPS more than 12K with RSA 2k key and 6k with ECC”	
				Query from the bidder – SSL TPS more than 20k with RSA 2k and 10K with ECC. All the OEM's Recommend that ECC connections should be half in proportion to RSA. There is only one OEM that supports 100k with ECC. We request you to please amend for the maximum participation.	Pl refer corrigendum.
				Query from the bidder – Seems to be Typo Error. a) 3 out of 4 OEM's allowed DON'T have appliance which meets the ECC : 100K TPS	Pl refer corrigendum.

				requirement. Hence, unable to participate. b) As an Industry benchmark, the ECC value should be half of the RSA i.e. if RSA 2k TPS: 20k then ECC must be 10k TPS. c) In order to meet the 100K ECC requirement, the qualified OEM has to quote the Highest Model which would not be Commercially viable option considering the other sizing parameters pertaining to mid size product. Hence, please dilute this clause in order to allow competition & get healthy techno-commercial offer. **Suggested Clause**:- SSL TPS more than 20K with RSA 2k key and 10k with ECC	

15	**6.5.1 (14)**	105	Hardware Compression Support – 5 Gbps	**Query from the bidder –** Dedicated Hardware for compression will have dedicated resources (CPU & Memory) for compression and it will not use the system. With higher compression throughput application response time will improve and hence improve the user experience. Request to change clause as "Hardware Compression Support - 10 Gbps" **Query from the bidder –** Different OEMs provide different technologies for compression. Citrix provides software based compression. Thus request to make the change to support both Hardware/Software Compression Throughput. Also change the compression support	No change. No change.

				for 3 Gbps. This is as per the L7 throughput of 5Gbps. Pl modify as “Hardware/Software Compression Support – 5 Gbps”	
16	**6.5.1 (19)**	105	Should support Port Mirroring	**Query from the bidder –** Port Mirroring is required for packet capturing or sending the colonizing traffic to other devices. So Troubleshooting and packet capturing features should be inbuilt on the system through GUI/SSH. Request to change clause as **"Should support Port Mirroring/ Clone traffic to other devices"** **Query from the bidder –** Request you to remove this clause. Port Mirroring is primarily done on the Switches, as a Primary	No change. No change.

				function Port-Mirroring (SPAN/RSPAN) not a feature of ADC	
17	**6.5.1 (41)**	107	The Load Balancer should support virtualization or segmentation where it should be possible to create virtual partitions from day one. Each of this Partition should be completely isolated from each other w.r.t. dedicated access control.	**Query from the bidder –** SEGMENTATION IS AN OLD TECHNOLOGY whereas VIRTUALIZATION IS THE NEXT GEN Technology widely implemented across the Globe since last 5 years. Major Drawback of Partition or segmentation: a) USES ONLY SHARED RESOURCES: Layer 3 separation of virtual tenants which cannot provide complete isolation of resources hence impacts the performance. VIRTUALIZATION: ADC-VX is built on a unique architecture that virtualizes the	No change.

				resources—including CPU, memory, network, and acceleration resources. This specialized hypervisor runs fully functional virtual ADC instances, each of which delivers ADC functionality just like a dedicated physical ADC. Each virtual ADC instance contains a complete and separated environment of resources, configurations and management. **Suggested Clause**: The Load Balancer should support Virtualization. Each virtual ADC instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management. d) OS.	

				Number of Virtualization 10 vADC from Day1 and scalable upto 30. **Query from the bidder –** Pl retain this specification. We suggest no change in this specs. Virtualization increases the cost of the solution and all the required functionality can be provided with segmentation. Thus segmentation should be a part of the spec. **Query from the bidder –** SEGMENTATION IS AN OLD TECHNOLOGY whereas VIRTUALIZATION IS THE NEXT GEN Technology widely implemented across the Globe since last 5 years. Major Drawback of Partition or	No change. No change.

				segmentation: a) USES ONLY SHARED RESOURCES : Layer 3 separation of virtual tenants which cannot provide complete isolation of resources hence impacts the performance. VIRTUALIZATION : ADC-VX is built on a unique architecture that virtualizes the resources—including CPU, memory, network, and acceleration resources. This specialized hypervisor runs fully functional virtual ADC instances, each of which delivers ADC functionality just like a dedicated physical ADC. Each virtual ADC instance contains a complete and separated environment of resources, configurations	

				and management. Suggested Clause: The Load Balancer should support Virtualization. Each virtual ADC instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management. d) OS. Number of Virtualization 10 vADC from Day1 and scalable upto 30. **Query from the bidder –** SEGMENTATION IS AN OLD TECHNOLOGY whereas VIRTUALIZATION IS THE NEXT GEN Technology widely implemented across the Globe since last 5 years.	No change.

				Major Drawback of Partition or segmentation: a) USES ONLY SHARED RESOURCES: Layer 3 separation of virtual tenants which cannot provide complete isolation of resources hence impacts the performance. VIRTUALIZATION: ADC-VX is built on a unique architecture that virtualizes the resources—including CPU, memory, network, and acceleration resources. This specialized hypervisor runs fully functional virtual ADC instances, each of which delivers ADC functionality just like a dedicated physical ADC. Each virtual ADC instance contains a	

				complete and separated environment of resources, configurations and management. **Suggested Clause**: The Load Balancer should support Virtualization. Each virtual ADC instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management. d) OS. Number of Virtualization 10 vADC from Day1 and scalable upto 30.	
18	**6.5.1 (42)**	108	Should keep configuration files separately for each virtual partition or separate configuration files for each segment	**Query from the bidder –** In Segmentation, partition will be done at route domain based and hence there will not be dedicated resource, so configuration will be	The requirement is to keep separate configurations files for each segment (which can be on the same HDD). Hence, No Change.

				stored on same HDD drive. **Request you to please remove this clause.**	
19	**6.5.1 (48)**	108	Should support transparent failover between 2 devices/segments	**Query from the bidder –** Request to remove the segment word from clause and during the Failover it is essential to maintain the session on secondary device so that if primary goes down session will maintain by secondary device and there is effect on existing user connections. Request to change clause as **"Should support transparent failover between 2 devices and failover should support TCP session mirroring, SSL session mirroring and persistence mirroring."**	Pl refer corrigendum
20	**6.5.1 (61)**	109	Should use dedicated Hardware Card/Module for compression & not software based compression	**Query from the bidder –** Different OEMs provide different technologies for compression. Citrix provides software based	No change.

				compression. Thus request to make the change to support both Hardware/Software compression Throughput. In Gartner's own words ... "The ADC market continues to evolve, with various new cloud-integrated and software-centric use cases having arisen" Relevant documentation is attached in your reference. https://www.gartner.com/doc/3830093/market-guide-application-delivery-controllers This means that there is an industry-wide shift to a Software Model rather than Hardware-Centric approach. Therefore it is requested to change this Spec.	

				Pl modify as “Should use dedicated Hardware Card / Module / via Software for compression without any performance issues.”	
21	**6.5.1 (82)**	110	The OEM of the proposed equipment must be in the Leaders/Challengers Quadrant of Gartner Magic Quadrant for Application Delivery Controller in each of the last two reports	**Query from the bidder -** 3 OEM's i.e. Radware, F5, Citrix are qualifying in the Gartner LEADER Quadrant. All these OEM's put together share the majority market share across the Globe & leading the Market for the Technical Innovation. Diluting the clause till Challenger Quadrant would make it difficult for all the ADC Leader's to compete with the competition in terms of Commercial viability and impact our participation due to L1 bidding. Hence, kindly limit the	No change.

				participation among the Gartner Leader's only, in order to get Healthy competition within the technology leaders. **Suggested Clause:** Gartner Report Position - The OEM of the proposed equipment must be in the Leaders Quadrant of Gartner Magic Quadrant for Application Delivery Controller in each of the last two reports. **Query from the bidder –** We would like to share that Even Gartner has stopped publishing Magic Quadrant for this segment of products. This is because of the drastic changes in the product and developments in this domain. Referring to old reports of Gartner, which even Gartner does	No Change.

				not want to continue is not suggestible. We would request you to revise the clause as ""The OEM of the proposed equipment must be in the latest Gartner Market Guide for Application Delivery Controller or should be in Top 5 vendors of IDC reports"	
				Query from the bidder – Gartner leaders quadrant already has 3 OEM's hence request to make requested changes. Request to change clause as **"The OEM of the proposed equipment must be in the Leaders Quadrant of Gartner Magic Quadrant for Application Delivery Controller in each of the last two reports."**	No change.
				Query from the bidder – 3 OEM's i.e. Radware,	No change.

				F5, Citrix are qualifying in the Gartner LEADER Quadrant. All these OEM's put together share the majority market share across the Globe & leading the Market for the Technical Innovation. Diluting the clause till Challenger Quadrant would make it difficult for all the ADC Leader's to compete with the competition in terms of Commercial viability and impact our participation due to L1 bidding. Hence, kindly limit the participation among the Gartner Leader's only, in order to get Healthy competition within the technology leaders. Suggested Clause: Gartner Report Position - The OEM of the	

				proposed equipment must be in the Leaders Quadrant of Gartner Magic Quadrant for Application Delivery Controller in each of the last two reports. **Query from the bidder -** 3 OEM's i.e. Radware, F5, Citrix are qualifying in the Gartner LEADER Quadrant. All these OEM's put together share the majority market share across the Globe & leading the Market for the Technical Innovation. Diluting the clause till Challenger Quadrant would make it difficult for all the ADC Leader's to compete with the competition in terms of Commercial viability and impact our participation due to L1 bidding.	No change.

				Hence, kindly limit the participation among the Gartner Leader's only, in order to get Healthy competition within the technology leaders. **Suggested Clause:** Gartner Report Position - The OEM of the proposed equipment must be in the Leaders Quadrant of Gartner Magic Quadrant for Application Delivery Controller in each of the last two reports.	
22	**6.5.3 (6)**	114	Standalone independent IPS Appliance	**Query from the bidder –** Application visibility with user control, IPS, APT are an integral part of current age NGFW platform. Asking for two separate devices (IPS and Firewall) will not only impact the performance but will also increase the manual intervention and	No change.

				complicate the management. It also lack in most important part in the security which is correlation and sharing of intelligence for effective security solution. The basic approach of platform based architecture of NGFW is to have complete automation, integration, automation and proactive prevention from the threats and this cannot be achieved by solid pin point devices. Please allow bidders to propose both firewall and IPS within the same device. So please remove the IPS portion and ask for IPS with application visibility in the Firewall device for better security in low OPEX cost. **Query from the bidder –**	No change.

				Application visibiity with user control, IPS, APT are a integral part of current age NGFW platform. Asking for two seprate devices (IPS and Firewall) will not only impact the performance but will also increase the manual intervention and complicate the management. It also lack in most important part in the security which is correlation and sharing of intelligence for effective security solution. The basic approach of platform based architecture of NGFW is to have complete automation, integration, automation and proactive prevention from the threats and this cannot be acheived by silod pin point devices. Please allow bidders to propose both firewall and IPS within the same	

				device. So Kindly remove the IPS portion and ask for IPS with application visibility in the Firewall device for better security in low opex cost.	
23	**6.5.3 (3)**	114	10 Gbps of real world throughput	**Query from the bidder –** Request to Amend to : Should support at least 8 Gbps of Threat Prevention throughput with Firewall, application control, IPS, Anti-Virus and Anti-malware enabled and with all updated signatures. The performance of many legacy architecture devices degrade as low as 90% on enabling Next Gen firewall features. Not mentioning this will block the devices and will not give the desired performance. **Query from the bidder –** As per RFP 7 years support (Warranty +	No change. No change.

				AMC) has been asked from proposed appliance but considering 7 years long duration there has no scalability demanded as per RFP. Considering 7 years long duration proposed solution should be capable and scalable to support at least 20 Gbps of inspection throughput to avoid any future performance degradation challenges which could lead to bad user experience. **Suggested Clause** : 10 Gbps of real world throughput with scalability up to 20 Gbps with a license upgrade **Query from the bidder –** The performance of many legacy architecture devices degrade as low as 90% on enabling Next	No change.

				Gen firewall features. Not mentioning this will block the devices and will not give the desired performance. Hence, it is requested to consider amendment to the said clause as : Should support at least 8 Gbps of Threat Prevention throughput with Firewall, application control, IPS, Anti-Virus and Antimalware enabled and with all updated signatures. **Query from the bidder –** As per RFP 7 years support (Warranty + AMC) has been asked from proposed appliance but considering 7 years long duration there has no scalability demanded as per RFP. Considering 7 years long duration proposed solution should be capable and scalable to support at	No change.

				least 20 Gbps of inspection throughput to avoid any future performance degradation challenges which could lead to bad user experience. We may request/ recommend the authorities to ammend the clause as :10 Gbps of real world throughput with scalability up to 20 Gbps with a license upgrade **Query from the bidder –** As per RFP 7 years support (Warranty + AMC) has been asked from proposed appliance but considering 7 years long duration there has no scalability demanded as per RFP. Considering 7 years long duration proposed solution should be capable and scalable to support at least 20 Gbps	No change.

				of inspection throughput to avoid any future performance degradation challenges which could lead to bad user experience. Current Clause : 10 Gbps of real world throughput Suggested Clause : 10 Gbps of real world throughput with scalability up to 20 Gbps with a license upgrade	
				Query from the bidder – As per RFP 7 years support (Warranty + AMC) has been asked from proposed appliance but considering 7 years long duration there has no scalability demanded as per RFP. Considering 7 years long duration proposed	No change.

				solution should be capable and scalable to support at least 20 Gbps of inspection throughput to avoid any future performance degradation challenges which could lead to bad user experience. Current Clause : 10 Gbps of real world throughput Suggested Clause : 10 Gbps of real world throughput with scalability up to 20 Gbps with a license upgrade	
24	**6.5.3 (45)**	116	Latency should be less than 150 microsecond	**Query from the bidder –** As per RFP 150 microsecond of latency has been accepted by UIDAI which is huge and could impact performance. NIPS could be unable to perform full packet	No change.

				analysis of malicious traffic under high loads. This could cause some attacks to go undetected also considering nature of TCP/IP latency has a more complex and far reaching impact on performance hence latency drives throughput as well. **Suggested Clause :** Latency should be less than 50 micro-second. **Query from the bidder –** As per RFP 150 microsecond of latency has been accepted by UIDAI which is huge and could impact performance NIPS could be unable to perform full packet analysis of malicious traffic under high loads. This could cause some attacks to go undetected also considering nature of	No change.

				TCP/IP latency has a more complex and far reaching impact on performance hence latency drives throughput as well. We may request/ recommend the authorities to amend the clause : Latency should be less than 50 micro-second **Query from the bidder –** As per RFP 150 microsecond of latency has been accepted by UIDAI which is huge and could impact performance NIPS could be unable to perform full packet analysis of malicious traffic under high loads. This could cause some attacks to go undetected also considering nature of TCP/IP latency has a more complex and far	No change.

				reaching impact on performance hence latency drives throughput as well. Current Clause : Latency should be less than 150 microsecond Suggested Clause : Latency should be less than 50 micro-second **Query from the bidder –** As per RFP 150 microsecond of latency has been accepted by UIDAI which is huge and could impact performance NIPS could be unable to perform full packet analysis of malicious traffic under high loads. This could cause some attacks to go undetected also considering nature of TCP/IP latency has a	No change.

				more complex and far reaching impact on performance hence latency drives throughput as well. Current Clause : Latency should be less than 150 microsecond Suggested Clause : Latency should be less than 50 micro-second	
25	**6.5.4 (4)**	119	System should have Firewall, IPSec, VPN, Unlimited users/nodes except VPN	**Query from the bidder –** All the important parameter for prevention at the perimeter level including application visibility, user awareness, Malware prevention, gateway Antivirus are missing in the features asked. In absence of this the device will be legacy device and will be blind to 80-90% of the threats. all the malicious traffic will be allowed to enter the network using	No change.

				dynamic ports and will be a major loop hole in security solution. Request you to please amend to :**System should support Firewall, Application visibility, User awareness, anti malware with zero day attack prevention, IPSec, VPN and Antivirus** **Query from the bidder –** All the important parameter for prevention at the perimeter level including application visibility, user awareness, Malware prevention, gateway Antivirus are missing in the features asked. In absence of this the device will be legacy device and will be blind to 80-90% of the threats. all the malicious traffic will be allowed to enter the network using	No change.

				dynamic ports and will be a major loop hole in security solution. Hence, it is requested to kindly consider ammendment to the said clause as : System should support Firewall, Application visibility, User awareness, anti malware with zero day attack prevention, IPSec, VPN and Antivirus	
26	**6.5.4 (5)**	119	The appliance should support at least 4*1G ports, 8*10G ports	**Query from the bidder –** This category of devices comes with higher density interfaces for future scalability and flexibility on the interfaces. The same was also been asked in the last RFP. Request you to please amend to for clarity, future scalability and flexibility :**The appliance should support atleast 4 * 1G /10 G Copper ports, 8* 10G Fiber ports and 4x 40 G Ports**	Pl refer corrigendum

				Query from the bidder – This category of devices comes with higher density interfaces for future scalability and flexibility on the interfaces. The same was also been asked in the last RFP. Request you to please amend to for clarity, future scalability and flexibility :The appliance should support atleast 4 * 1G /10 G Copper ports, 8* 10G Fiber ports and 4x 40 G Ports	Pl refer corrigendum
27	**6.5.4 (6)**	119	Should support at least 10 Gbps of Firewall throughput with all functionality mentioned in point 4 above	**Query from the bidder –** Traffic pattern has been changed with evolution of applications. Application traffic is not just only TCP and UDP and most of the firewall vendors use by default TCP and UDP for the performance measures. Production traffic is mix of HTTP, HTTPS, SMTP,	No change. No change

				POP3, DNS and it is highly recommended that throughput number should be based on real world traffic not based on Just TCP and UDP. Request you to change the clause. **Query from the bidder –** Request you to please amend to: **System Throughput - at least 8 Gbps with all functionality mentioned in point 4 on 64 KB/ real world production environment.** **This will allow all major OEM on the level play.** **Query from the bidder –** Only firewall will not be going to protect from today's sophisticated attacks. Request you to pls ask for **Should support at least 10 Gbps of real world / mix traffic of Firewall with**	No change.

				Application visibility, User awareness, anti malware with zero day attack prevention, Antivirus. **Query from the bidder –** Request you to revise the clause to 'Should support at least 10 Gbps of Threat prevention (FW + IPS + AVC + Antimalware) throughput on Mix / real-world production traffic' Only firewall functionality will not be able to protect from latest sophisticated attacks. It is suggest to ask for Threat prevention functionality instead of throughput for only Firewall functionality. **Query from the bidder –** It is requested to kindly	No change. No change.

				consider amendment to the said clause to: System Throughput - at least 8 Gbps with all functionality mentioned in point 4 on 64 KB/ real world production environment This will allow all major OEM on the level play **Query from the bidder –** Only firewall will not be going to protect from today's sophisticated attacks. Request you to pls ask for **Should support at least 10 Gbps of real world / mix traffic of Firewall with Application visibility, User awareness, anti malware with zero day attack prevention, Antivirus**.	No change.
28	**6.5.4 (7)**	120	SSL Inspection Throughput – at least 5 Gbps	**Query from the bidder –** SSL inspection throughputs differ based on testing conditions, SSL protocols and key	Pl refer corrigendum.

				size. Please clarify on below requirements for SSL sizing. 1. Please clarify which SSL standard support is required? ECC, RSA etc. 2. What SSL key size vendor should consider for SSL throughput Since SSL demands more hardware resources, it's always recommended to offload expensive SSL encryption and decryption to dedicated acceleration hardware to meet the desired production performance. Request you to incorporate the SSL inspection using SSL acceleration card. **Query from the bidder –** This is duplication of functionality and is been asked in the load balancer as well.	Pl refer corrigendum.

				Please remove either from Firewall or from the load balancers. **Query from the bidder –** Today 80% of web traffic is encrypted. It is suggested that the inbuilt IPS functionality should be able to inspect SSL traffic and SSL inspection throughput for IPS should be at least 10Gbps or more. **Query from the bidder –** This is duplication of functionality and has been asked in the load balancer as well. It is requested to kindly consider removing it either from Firewall or from the load balancers	Pl refer corrigendum. Pl refer corrigendum.
29	**6.5.4 (8 – 9)**	120	8) Firewall should support at least 15,000,000 concurrent sessions 9) Firewall should support at least 200,000 connections per second	**Query from the bidder –** Considering production traffic with higher % of HTTP & HTTPS along with other TCP and UDP based applications,	Pl refer corrigendum.

				average time out of applications is 5-10 minutes (600 seconds) and same goes on firewall as well. Connections per second number can derived from application timeout and concurrent sessions using formula CC=CPS x timeout. Connection per second (200,000) is not inline to concurrent connection number and seems to be oversized and favourable to one specific OEM. it is recommend to change it to lower number i.e. 150,000 and allow equitable competition among vendors **Query from the bidder –** 8) 15 million sessions is too high for a 8-10 Gig device. Even if we consider 1 session for 10 Kbps. The total sessions	Pl refer corrigendum.

				in a 8-10 Gig device can only be 1 Million. Even if we take 2-4 times as buffer it will never increase 4 Million or 4,000,000 concurrent Sessions. Request you to please amend to so that the major security OEMS can participate. Request you to please amend to : **Firewall should support at least 4,000,000 concurrent sessions** **9)** Request you to please amend to for level playing field for all OEM : **Firewall must support at least 160,000 connections per second with application visibility** **Query from the bidder –** Today there are many applications which keep	Pl refer corrigendum.

				running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These applications keeps opening sessions automatically. The firewall should not become a bottleneck in case of a virus or trojan generating huge nos. of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling very high concurrent sessions and new sessions per second. 8) It is suggested that the Firewall should support minimum 40 million new sessions per second	

				9) It is suggested that the Firewall should support minimum 400,000 new sessions per second **Query from the bidder –** Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. The firewall should not become a bottleneck in case of a virus or trojan generating huge nos. of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling very	Pl refer corrigendum.

				high concurrent sessions and new sessions per second. 8) It is suggested that the Firewall should support minimum 40 million new sessions per second 9) It is suggested that the Firewall should support minimum 400,000 new sessions per second **Query from the bidder –** 8) 15 million sessions is too high for a 8-10 Gig device. Even if we consider 1 session for 10 Kbps. The total sessions in a 8-10 Gig device can only be 1 Million. Even if we take 2-4 times as buffer it will never increase 4 Million or 4,000,000 concurrent Sessions. Request you to please amend to so that the major security OEMS can participate. It is	Pl refer corrigendum.

				requested to kindly consider amendment to the said clause to: Firewall should support at least 4,000,000 concurrent sessions 9) In order to have a level playing field for all OEMs, It is requested to kindly consider amendment to the said clause to: Firewall must support at least 160,000 connections per second with application visibility **Query from the bidder –** Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These applications keep	Pl refer corrigendum.

				opening sessions automatically. The firewall should not become a bottleneck in case of a virus or trojan generating huge nos. of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling very high concurrent sessions and new sessions per second. 8) It is suggested that the Firewall should support minimum 40 million new sessions per second 9) It is suggested that the Firewall should support minimum 400,000 new sessions per second	
30	**6.5.4 (16)**	120	Firewall should support manual NAT and Auto-NAT, static NAT, Dynamic NAT, dynamic PAT	**Query from the bidder –** Auto-NAT is not a feature of a Firewall and is not supported by all	Pl refer corrigendum.

				leading OEMs. Request you to please remove thus enabling all leading OEMs to participate. **Query from the bidder –** Auto-NAT is not a feature of a Firewall and is not supported by all leading OEMs. In order to have a level playing field for all OEMs, It is requested to kindly consider removal of the said clause	Pl refer corrigendum.
31	**6.5.4 (17)**	120	Firewall should support NAT66 (IPv6 to IPv6), NAT64 (IPv6-to-IPv4) & NAT46 (IPv4-to-IPv6) functionality	**Query from the bidder –** Please amend so that all leading OEMs can participate: Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) / Nat46 (IPv4- to-IPv6) functionality **Query from the bidder –** The NAT64 and NAT46 is ISP requirement not end customer. It is suggested to amend the clause as	Pl refer corrigendum. Pl refer corrigendum.

				Firewall should support Nat66 (IPv6-to-IPv6) and NAT44 **Query from the bidder –** It is specific to a OEM so suggested to delete **Query from the bidder –** In order to have a level playing field for all OEMs, It is requested to kindly consider amendment to the said clause to: Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-toIPv4) / Nat46 (IPv4- to-IPv6) functionality	Pl refer corrigendum. Pl refer corrigendum.
32	**6.5.4 (24)**	121	Firewall should support redundant interfaces to provide interface level redundancy before device failover	**Query from the bidder –** It is specific to a OEM so suggested to delete **Query from the bidder –** It is specific to a OEM so suggested to delete	Pl refer corrigendum.
33	**6.5.4 (28)**	121	Firewall should have redundant hot-swappable FANs	**Query from the bidder –** Requirement of hot swappable FAN is dependent on hardware	Pl refer corrigendum.

				architecture of OEM. ASIC and FPGA's based appliances dissipate more heat and require redundant and hot swappable Fans. However CPU based architecture is comparatively better in terms of power consumption and may not require this functionality. This requirement is favourable to specific OEM. it is recommend to dilute and allow equitable competition among vendors	
				Query from the bidder – It is specific to a OEM so suggested to delete	Pl refer corrigendum.
				Query from the bidder – It is specific to a OEM so suggested to delete	Pl refer corrigendum.
				Query from the bidder – requirement of hot	Pl refer corrigendum.

				swappable FAN is dependent on hardware architecture of OEM. ASIC and FPGA's based appliances dissipate more heat and require redundant and hot swappable Fans. However CPU based architecture comparatively better in terms of power consumption and may not require this functionality. This requirement is favourable to specific OEM. it is recommend to dilute and allow equitable competition among vendors.	
34	**6.5.4 (43)**	123	Hot swappable power supply proposed	**Query from the bidder –** It is specific to a OEM so suggested to delete **Query from the bidder –** It is specific to a OEM so suggested to delete	Not Specific to OEM. Hence No Change in Specification.

35	**6.5.4 (44)**	123	(N+1) redundant power supply proposed	**Query from the bidder –** Most of the Data Centres are using 1+1 power supply. This requirement is favourable to specific OEM. It is recommend to delete and allow equitable competition among vendors **Query from the bidder –** most of the datacenters are using 1+1 power supply. This requirement is favorable to specific OEM. it is recommend to delete and allow equitable competition among vendors.	Pl refer corrigendum. Pl refer corrigendum.
36	**6.5.4 (47)**	124	Hot swappable cooling fans	**Query from the bidder –** It is specific to a OEM so suggested to delete **Query from the bidder –** It is specific to a OEM so suggested to delete	Pl refer corrigendum. Pl refer corrigendum.
37	**6.5.4 (48)**	124	(N+1) redundant Cooling Fans proposed	**Query from the bidder –** Requirement of hot swappable FAN is dependent on hardware	Pl refer corrigendum.

				architecture of OEM. ASIC and FPGA's based appliances dissipate more heat and require redundant and hot swappable Fans. However CPU based architecture comparatively better in terms of power consumption and may not require this functionality. This requirement is favourable to specific OEM. It is recommend to dilute and allow equitable competition among vendors.	
				Query from the bidder – It is specific to a OEM so suggested to delete	Pl refer corrigendum.
				Query from the bidder – It is specific to a OEM so suggested to delete	Pl refer corrigendum.
				Query from the bidder – requirement of hot	Pl refer corrigendum.

				swappable FAN is dependent on hardware architecture of OEM. ASIC and FPGA's based appliances dissipate more heat and require redundant and hot swappable Fans. However CPU based architecture comparatively better in terms of power consumption and may not require this functionality. This requirement is favourable to specific OEM. it is recommend to dilute and allow equitable competition among vendors	
38	**6.5.4 (52)**	124	The Firewall solution offered must be rated as ‘leaders’ or 'Challengers' in the Magic Quadrant for Enterprise Firewall in each of the last two reports published by Gartner.	**Query from the bidder –** NSS report is also third party credible report for NGFW from security prospective. We request to have Gartner report or NSS report as OEM qualification criteria to allow other OEM. It is	No change.

				suggested that the Firewall solution offered must be rated as ‘leaders’ or 'Challengers' in the Magic Quadrant for Enterprise Firewall in each of the last two reports published by Gartner or The NGFW should have recommended status of latest NSS report . Bidder shall submit the latest authentic Gartner reference report and NSS report. **Query from the bidder –** NSS report is also third party credible report for NGFW from security prospective. We request to have Gartner report or NSS report as OEM qualification criteria to allow other OEM. It is suggested that the Firewall solution offered must be rated as ‘leaders’ or 'Challengers'	

				in the Magic Quadrant for Enterprise Firewall in each of the last two reports published by Gartner or The NGFW should have recommended status of latest NSS report . Bidder shall submit the latest authentic Gartner reference report and NSS report.	
39	**6.5.5 (6)**	125	48 * 10G ports with 10 G MM transceivers. Switch should be standalone	**Query from the bidder –** There is no Spine/ Core Switch asked in the RFP. Please confirm where these Access/ ToR will be hooked on. **Query from the bidder –** There is no Spine/ Core Switch asked in the RFP. Please confirm where these Access/ ToR will be hooked on. **Query from the bidder –** There is no Spine/ Core Switch asked in the RFP. Please confirm where	Design documents are internal to UIDAI. Design documents are internal to UIDAI. Design documents are internal to UIDAI.

				these Access/ ToR will be hooked on.	
40	**6.5.5 (15)**	126	Datacenter bridging exchange, ieee 802.1Qbb and ieee802.1Qaz	**Query from the bidder –** Its Campus LAN deployment. Hence respective protocol is not required. Please remove	Pl refer corrigendum.
41	**6.5.5 (20)**	126	Support for minimum 4 K IPv4 and 4k IPv6 ACLs like port based, VLAN based and Standard/Extended ACLs	**Query from the bidder –** Request you to kindly change this clause as "Support for minimum 4K IPv4 and 2k IPv6 ACLs like port based, VLAN based and Standard/Extended ACLs L2-L4" Normally the performance of IPv6 is just half of IPv4 performance value because IPv6 addressing is 128-bit whereas IPv4 addressing is 32-bit. Request you to kindly change so that max. OEM can participate.	Pl refer corrigendum.

42	**6.5.5 (27)**	127	Support 12k IPv4 and 12k IPv6 multicast routes	**Query from the bidder –** Since architecture and technology design differ from OEM to OEM, The multicast is form of Broadcast, so one multicast entry means route for thousands of IP Devices. Basically the IP Multicast route is distributed in multiple switches, not in one switch. Now if the customer wants to keep provision for future scalability than request you to kindly modify this clause as "Support 8k IPv4 and 4k IPv6 multicast routes" so that max. OEM can participate. **Query from the bidder –** asked Multicast Route is very high on single switch deployment or group of switch (stacking / Clustering). Request you reduce the	Pl refer corrigendum. Pl refer corrigendum.

				parameter with 8K for both IP version which will enable us for bidding.	
43	**6.5.5 (43)**	128	Operating temperature range : 20-24 ºC	**Query from the bidder –** I think it is Typo Error any standard switches comes with the range of −5°C to 45°C, of temperature support. Request you to change the parameter like " Operating temperature range : −5°C to 45°C which enable us for bidding.	20-24 ºC is the normal temperature maintained in the Data Center and the proposed equipment should work under these conditions.
44	**6.5.5 (45)**	128	Gartner Report Position : The OEM of the proposed equipment must be in the Leaders/ Challengers Quadrant of Gartner Magic Quadrant for Data Centre Networking in each of the last two reports	**Query from the bidder –** Its Campus LAN deployment. Hence Gartner Wired & Wireless report / IDC Report. Please include IDC Report	No change.
45	**6.5.6 (41)**	132	Operating temperature range 20-24 ºC	**Query from the bidder –** I think it is Typo Error any standard switches comes with the range of −5°C to 45°C, of temperature support. Request you to change	20-24 ºC is the normal temperature maintained in the Data Center and the proposed equipment should work under these conditions.

				the parameter like " Operating temperature range : −5°C to 45°C which enable us for bidding.	
46	**6.5.6 (43)**	132	Gartner Report Position : The OEM of the proposed equipment must be in the Leaders/ Challengers Quadrant of Gartner Magic Quadrant for Data Centre Networking in each of the last two reports	**Query from the bidder –** Its Campus LAN deployment. Hence Gartner Wired & Wireless report / IDC Report. Please include IDC Report	No change.
47	**6.5.7 (14)**	135	Backplane of each slot should be minimum 20 Gbps	**Query from the bidder –** Please change the clause to "Backplane of each slot should be minimum 160 Gbps". The Router is asked with 8 x 10G Ports Wirespeed Ports. To meet this requirement the per slot capacity should be 160Gbps (80 x 2 = 160). Please change the clause for non Blocking / Wire-speed performance. **Query from the bidder –** Please change the clause	Pl refer corrigendum. Pl refer corrigendum.

				to "Backplane of each slot should be minimum 160 Gbps". The Router is asked with 8 x 10G Ports Wire-speed Ports. To meet this requirement the per slot capacity should be 160Gbps (80 x 2 = 160). Please change the clause for non Blocking / Wire-speed performance. **Query from the bidder –** Please change the clause to "Backplane of each slot should be minimum 160 Gbps". The Router is asked with 8 x 10G Ports Wirespeed Ports. To meet this requirement the per slot capacity should be 160Gbps (80 x 2 = 160). Please change the clause for non Blocking / Wire-speed performance.	Pl refer corrigendum.

48	**6.5.7 (20)**	135	SSL/IPSec capability	**Query from the bidder –** Please confirm if IPSec is to be enabled from Day 1 with at least 10Gbps Encryption. **Query from the bidder –** Please confirm if IPSec is to be enabled from Day 1 with at least 10Gbps Encryption. **Query from the bidder –** Please confirm if IPSec is to be enabled from Day 1 with at least 10Gbps Encryption.	Pl refer corrigendum. Pl refer corrigendum. Pl refer corrigendum.
49	**6.5.7 (40)**	138	8k IPv4 and 8k IPv6 unicast routes	**Query from the bidder –** Please change the clause to" 50K IPv4 and 50k IPv6 unicast routes with 12K Multicast Routes." 8K IPv4 and 8K IPv6 scale is too less for such class of Router. Even the 6.5.5 Access Switch is asked with 12K Routes Multicast. Please change the clause to 50K IPv4 and 50k IPv6 Routes with	No change.

				12k Multicast routes to avoid forklift upgrade and performance bottleneck. **Query from the bidder –** Please change the clause to" 100K IPv4 and 100k IPv6 unicast routes with 12K Multicast Routes." 8K IPv4 and 8K IPv6 scale is too less for such class of Router. Even the 6.5.5 Access Switch is asked with 12K Routes Multicast. Please change the clause to 100K IPv4 and 100k IPv6 Routes with 12k Multicast routes to avoid forklift upgrade and performance bottleneck. **Query from the bidder –** Please change the clause to" 50K IPv4 and 50k IPv6 unicast routes with 12K Multicast Routes." 8K IPv4 and 8K IPv6 scale	No change. No change.

				is too less for such class of Router. Even the 6.5.5 Access Switch is asked with 12K Routes Multicast. Please change the clause to 50K IPv4 and 50k IPv6 Routes with 12k Multicast routes to avoid forklift upgrade and performance bottleneck.	
50	-	-	-	**Query from the bidder – Request for addition in Firewall:** The proposed solution shall provide sandbox behaviour based inspection and protection of unknown viruses and zero-day malware for any application and protocol (not limited to HTTP, SMTP, FTP) from day one and the solution shall be able to provide automated signature generation for discovered zero-day	Suggested changes Not considered.

				malware and the solution should ensure the delivery of the signature in 5 mins from the time of detection. The environment should support both cloud based and on premise architecture. Separate on premise device with support for 36 VM and clustering support of upto 20 devices has to be provided. **Note** - Zero day unknown attacks is completely missing in the RFP. WE recommend to include this as the unknown threats are the major cause of compromise. The SLA and response turnaround time to convert unknown to known is very important aspect. The solution should be	

				capable of protection against millions of unknown zero day attach and this should support automated signature creation and converting the unknown into known within 5-10 mins of Zero-day/Unknown malware detection. **Query from the bidder –** The proposed solution shall provide sandbox behavior based inspection and protection of unknown viruses and zero-day malware for any application and protocol (not limited to HTTP, SMTP, FTP) from day one and the solution shall be able to provide automated signature generation for discovered zero-day malware and the solution should ensure the delivery of the	Suggested changes Not considered.

				signature in 5 mins from the time of detection. The environment should support both cloud based and on premise architecture. Separate on premise device with support for 36 VM and clustering support of upto 20 devices has to be provided. Zero day unknown attacks is completely missing in the RFP. WE recommend to include this as the unknown threats are the major cause of compromise. The SLA and response turnaround time to convert unknown to known is very important aspect. The solution should be capable of protection against millions of unknown zero day attach and this should support automated signature	

				creation and converting the unknown into known within 5- 10 mins of Zero-day/Unknown malware detection.	
51	-	-	-	**Query from the bidder – Request for addition in Firewall:** The proposed solution must support on appliance Per policy SSL and SSH decryption for both inbound and outbound traffic **Note** - Most of the applications run on SSL encryption and management on SSH. Current day attacks can also be embedded in this encrypted traffic. This feature is missing and is very important for protection against such threats. **Query from the bidder – Request for addition in Firewall:**	Suggested changes Not considered. Suggested changes Not considered.

				The proposed solution must support on appliance Per policy SSL and SSH decryption for both inbound and outbound traffic. **Note** - Most of the applications run on SSL encryption and management on SSH. Current day attacks can also be embedded in this encrypted traffic. This feature is missing and is very important for protection against such threats.	
52	-	-	-	**Query from the bidder – Request for addition in Firewall:** The device should be capable to identify and prevent in-progress phishing attacks by controlling sites to which users can submit credentials based on the site's URL category thus blocking users from submitting credentials to	Suggested changes Not considered.

				un-trusted sites while allowing users to continue to submit credentials to organization and sanctioned sites. **Note** - Credential theft is the major concern for UIDAI and is most common phishing attack. Will suggest to include this very important feature requirement. **Query from the bidder – Request for addition in Firewall:** The device should be capable to identify and prevent in-progress phishing attacks by controlling sites to which users can submit credentials based on the site's URL category thus blocking users from submitting credentials to untrusted sites while allowing users to	Suggested changes Not considered.

				continue to submit credentials to organization and sanctioned sites. **Note -** Credential theft is the major concern for UIDAI and is most common phishing attack. It is suggest to kindly include this very important feature requirement.	
53	-	-	-	**Query from the bidder – Request for addition in Firewall:** "Firewall should have minimum 20 Gbps of VPN throughput" **Note -** high performance VPN capabilities to address performance and connectivity to DC and DR. **Query from the bidder – Request for addition in Firewall:** "Firewall should have minimum 20 Gbps of	Suggested changes Not considered. Suggested changes Not considered.

				VPN throughput" **Note -** high performance VPN capabilities to address performance and connectivity to DC and DR. **Query from the bidder – Request for addition in Firewall:** "Firewall should have minimum 20 Gbps of VPN throughput" **Note -** high performance VPN capabilities to address performance and connectivity to DC and DR.	Suggested changes Not considered.
54	**-**	-	-	**Query from the bidder – Request for addition in Firewall:** "Firewall should have minimum 10,000 concurrent SSL VPN users and should be scalable in future"	Suggested changes Not considered.

				Note - SSL VPN required for allowing access to Users accessing the Network from Outside for Management purpose or for accessing applications through a secure connection	
				Query from the bidder – Request for addition in Firewall: "Firewall should have minimum 10,000 concurrent SSL VPN users and should be scalable in future"	Suggested changes Not considered.
				Note - SSL VPN required for allowing access to Users accessing the Network from Outside for Management purpose or for accessing applications through a secure connection	
				Query from the bidder – Request for addition in	Suggested changes Not considered.

				Firewall: "Firewall should have minimum 10,000 concurrent SSL VPN users and should be scalable in future" **Note -** SSL VPN required for allowing access to Users accessing the Network from Outside for Management purpose or for accessing applications through a secure connection	
55	**-**	-	-	**Query from the bidder – Request for addition in Firewall:** "The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts."	Suggested changes Not considered.

				Query from the bidder – Request for addition in Firewall: "The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts."	Suggested changes Not considered.
56	-	-	-	**Query from the bidder –** Should support VPN Clustering and Load balancing/sharing. VPN clustering and load balancing are basic features of routers and should be relaxed on the security device thus enabling all leading OEMs to participate. Request you to please	Referred clause not in the RFP. Hence, no change considered.

				amend to: **Should support Clustering/ HA and Load balancing/sharing** **Query from the bidder –** VPN clustering and load balancing are basic features of routers and should be relaxed on the security device thus enabling all leading OEMs to participate. In order to have a level playing field for all OEMs, It is requested to kindly consider ammendmnet to the said clause to: Should support Clustering/ HA and Load balancing/sharing	Referred clause not in the RFP. Hence, No change considered.
57	**-**	-	-	**Query from the bidder – Request for addition in IPS :** As per RFP new connection per second has not been incorporated as a parameter to size the IPS	Suggested changes Not considered.

				appliance. Hence request you to please incorporate new connection per second parameter so that optimum performance can be delivered to process malicious traffic. **Suggested Clause :** Proposed solution should offer 500,000 of New Connections per second **Query from the bidder – Request for addition in IPS :** As per RFP new connection per second has not been incorporated as a parameter to size the IPS appliance. Hence request you to please incorporate new connection per second parameter so that optimum performance can be delivered to	Suggested changes Not considered.

				process malicious traffic. **Suggested Clause :** Proposed solution should offer 500,000 of New Connections per second	
				Query from the bidder – Request for addition in IPS : As per RFP new connection per second has not been incorporated as a parameter to size the IPS appliance. Hence request you to please incorporate new connection per second parameter so that optimum performance can be delivered to process malicious traffic. **Suggested Clause :** Proposed solution should offer 500,000 of New Connections per	Suggested changes Not considered.

				second	
58	-	-	-	**Query from the bidder – Request to add this clause for Load Balancer** **"**The proposed solution should offer Centralized console for Orchestration , Configuration, Analytics and Management Platform from Day 1**"** **Note –** **This will ensure that UIDAI is will be future proof.** UIDAI-wide network and application management and analytics will deliver a powerful visibility across the infrastructure, which means that UIDAI will be able to meet the performance and security requirements. In addition to reducing operational costs and	Suggested changes Not considered.

				simplifying tasks, having a centralized solution will provides a real-time analytics to help administrators identify and address application performance and security issues across the UIDAI's infrastructure. Furthermore, this will provide an application-level integration with external orchestration systems.	
59				**Query from the bidder – Request to add this clause for Load Balancer:** **"**The proposed solution should be have ability to monitor secure web applications and have SSL statistics to be recorded and logged for every SSL transaction. All licences should be included in the proposed solution**"**	Suggested changes Not considered.

				Note - This will unsure greater security infrastructure for UIDAI. This will allows UIDAI's IT administrators to monitor all the secure web applications being served by the ADC by providing integrated and real-time and historic monitoring of secure web transactions. With this level of visibility the administrator can assess the Quantify client performance and Application Security without any compromise.	

60	-	-	-	**Query from the bidder – Request to add this clause for Load Balancer:** **"**Load Balancer should support detailed Application Performance Analytics on Day 1**"** **Note –** This will unsure greater security infrastructure for UIDAI. With Analytics, a UIDAI will be able to combat advanced security threats based on user & entity behaviour. UIDAI will be able to track all aspects of user behaviour and by leveraging advanced Machine Learning algorithms distinguish normal employee behaviour from that of a malicious attacker.	Suggested changes Not considered.