RESPONSES TO THE QUERIES RECEIVED AGAINST TENDER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023

Cons. S. No.	VENDOR	Sr. No.	RFP Page No	Ref. Point	RFP Clause	Description	Comments	CCA/NIXI Response
1	VENDOR-1	1	79		4. HSM Module:	Symmetric: AES, Triple DES, DES (No separate license of Algorithm to be charged).	Please remove DES. DES has been already removed from NIST approved list and no longer needed to be part of the specification for HSM	Clause may be read as "Symmetric: AES, Triple DES (No separate license of Algorithm to be charged)".
2	VENDOR-1	2	79		4. HSM Module:	Support for Hash Message Digest HMAC, SHA1, SHA2 (512), SM3 and SM4	Please remove SM3 and SM4 as they are chinese algorithms and not used in India	Clause may be read as "Support for Hash Message Digest HMAC, SHA1, SHA2 (512) etc."
3	VENDOR-1	3	79		4. HSM Module:	HSM should be FIPS 140-2 Level 3 certified and certification should be in OEM Name. Certification Copy needs to be submitted	We request to remove term **"certification should be in OEM"** Currently, there is No Network Appliance HSM which is FIPS 140-2 Level 3 certified. There are OEM's who have certified their Cryptographic Module certified. All Network Appliance HSM OEM uses this Cryptographic Module in their Network Appliance HSM, however it's not necessary OEM of Cryptographic Module and Network Appliance HSM to be same. If cryptographic keys are stored in FIPS 140-2 Level 3 certified cryptographic module, it meets the CCA and Webtrust guidelines. So it is not necessary to have FIPS 140-2 Level 3 certification in name of Network Appliance HSM OEM. The need as per CCA and Webtrust Guidelines is that cryptographic keys should be stored in FIPS 140-2 Level 3 certified Cryptographic Module. Since the cryptographic key management / storage function is when managed within the certified cryptographic module and Cryptographic Module used in a Network Appliance HSM has valid FIPS certificate on the NIST website. So it is not necessary to have Network Appliance HSM OEM name on NIST website. In all previous RFP's even the last RFP which was scrapped, there was no term which mentions "FIPS Certificate should be in name of OEM". This term is particularly introduced to make sure Indian Network Appliance OEM are **restricted** to participate in RFP. As a reference, Current tender's first version was also without this clause and there are more RFPs mentioned below have had term without asking for this clause: 1. NIXI SSL Root CA : RFP No: CCA/01(1)-2022-NIXI & Ref: F.No.NIXI/CCA/01-2022 Dated 11/10/2022 2. SBI KMS : SBI/GITC/Platform Engineering-II/2021/2022/808 3. Tirupati Smart City : Ref.: TSCCL/Projects/223(Master System Integrator)/2022 4. TN-CCTNS : ELCOT/PROC/OT/33384/CCTNS 2.0 (SCRB)/ 2020-21 5. BHILAI Steel (SAIL) : Tender No. 21A02729001 / 2021400100 Dtd. 01/04/2021 There are many such government, banking, smart city and other RFPs which are without the same clause.	No change
4	VENDOR-1	4	79		4. HSM Module:	HSM should have simulator capabilities to provide development , integration and Testing of applications in restricted network with no outside connectivity to internet .	Please remove this clause "As Nixi is going to have physcial HSM, and Nixi can perform testing by using one partition of HSM"	**deleted.**
5	VENDOR-1	5	80		PCIe HSM - Host Connectivity	PCIe x4	Please change to PCIe x4 , x8 or x16	PCIe x1, x4, x8, x16 or compatible
6	**VENDOR**	**S.No.**	**Page No.**	**Point No.**	**Requirement**	**Specification**	**Justification and change**	**CCA/NIXI Response**
7	VENDOR-2	1	74	11	Load Balancer	The server load balancer should deliver atleast 10 Gbps or higher of SSL throughput on 4096 key	Since all OEM do not publishes the key size, please revise this clause as " The server load balancer should deliver atleast 10 Gbps or higher of SSL throughput"	Clause should be read as "The server load balancer should deliver atleast 10 Gbps or higher of SSL throughput"
8	VENDOR-2	2	74	12	Load Balancer	The server load balancer should cater up to at least 40K or higher SSL connections per second on 2K key from day 1	Kindly revise the specs for better participation and health competition. "The server load balancer should cater up to at least 35K or higher SSL connections per second from day 1"	Clause should be read as "The server load balancer should cater up to at least 35K or higher SSL connections per second from day 1"
9	VENDOR-2	3			Load Balancer	Additional Point	Load balancer should be capable to integrate with firewall to automatically block an IP with malicious activity detected.	No change.
10	VENDOR-2	4			Load Balancer	Additional Point	Load balancer should capable of anti-malware feature and integration with anti-apt solution for zero day inspection in future.	No Change
11	VENDOR-2	5	75	2	Firewall	Firewall appliance should be supplied with at least 4 x 1GE RJ-45 (expandable to total 8 ports) interfaces, 4 x 1G SFP slots (expandable to total 8 ports), 2 x10G SFP+ (expandable to total 8 ports). Solution should include all transceivers of populated modules (4x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports from day 1.	Kindly revise the specs for better participation and health competition. "Firewall appliance should be supplied with at least 4 x 1GE RJ-45 (expandable to total 8 ports) interfaces, 4 x 1G SFP slots (expandable to total 8 ports), 2 x10G SFP+ (expandable to total 4 ports). Solution should include all transceivers of populated modules (4x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports from day 1."	Clause should be read as "Firewall appliance should be supplied with at least 4 x 1GE RJ-45 (expandable to total 8 ports) interfaces, 4 x 1G SFP slots (expandable to total 8 ports), 2 x10G SFP+ (expandable to total 4 ports). Solution should include all transceivers of populated modules (4x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports from day 1."
12	VENDOR-2	6	75	2	Firewall	Each appliance should have local available storage of 200 GB SSD after 1+1 RAID.	Kindly revise the specs as lower end appliance comes with inbuilt single disk. "Each appliance should have local available storage of 200 GB SSD."	Clause should be read as "Each appliance should have local available storage of 200 GB SSD or higher from day 1."
13	VENDOR-2	7	75	5	Firewall	Appropriate energy efficient redundant (N+N) hot swappable power supplies.	Kindly remove this clause as high end appliance come with hot swappable power supply and this requirement is already captured under point number 34 for integrated redundant power supply.	Clause stands deleted
14	VENDOR-2	8	75	9	Firewall	Threat Protection Throughput: 5 Gbps	Kindly revise the specs as appliance with 10Gbps firewall throughput comes with lower threat protection throughput and asked throughput is supported on higher models. "Threat Protection Throughput: 3 Gbps"	Clause should be read as "Threat Protection Throughput of atleast 3 Gbps"
15	VENDOR-2	9	75	10	Firewall	Firewall should support at least 8 million concurrent sessions	Kindly revise the specs as 8 Million concurrent session seems higher on 10Gbps Firewall throughput appliance. "Firewall should support at least 3 million concurrent sessions"	Clause should be read as "Firewall should support at least 3 million concurrent sessions or higher from day 1"
16	VENDOR-2	10	75	24	Firewall	Should be supplied with 1000 SSL VPN users license.	Kindly revise the specs for better participation and health competition. "Should be supplied with 500 SSL VPN users license."	Clause should be read as "Should be supplied with atleast 500 SSL VPN users license or higher from day 1"
17	VENDOR-2	11	76	35	Firewall	Should have the IPS capability to inspect SSL traffic and SSL throughput of 9 Gbps.	Kindly revise the specs for better participation and healthy competition. "Should have the IPS capability to inspect SSL traffic and SSL throughput of 4 Gbps."	Clause should be read as "Should have the IPS capability to inspect SSL traffic and SSL throughput of 4 Gbps or above.
18	VENDOR-2	12	76	45	Firewall	Should support more than 2000+ application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	IPS signature supported is not mentioned, so request to revise specs. "Should support more than 2000+ application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness. Additonally firewall should have minimum 20000 IPS signature to prevent against vulnerabilities."	No Change
19	VENDOR-2	13	77	53	Firewall	Server Security.	This requirement is pertaining to endpoint and not part of firewall so should be asked separately and request to remove point 53 to 57.	RFP points from 53 to 57 stand deleted
20	VENDOR-2	14	77	61	Firewall	Local malware analysis appliance should be of same OEM with 4x 1GE RJ45 interface and minimum throughput of 500 files/hour process across 6VMs or more. All VMs should be included from day 1.	We understand APT (sandboxing) solution is required to address Zero day threats and is essential part of perimeter security. It must be provided 1 each at perimeter level in DC & DR. Please confirm.	Yes we need total 4 quantities of anti-apt solution should be factored which is one of DC and other of DR for both Root CCA and Issuing CA setup.
21	VENDOR-2	15	80		Switch	Additional Point	Solution should have capability of network access control. For example, feature should automatically detect the device type or OS and assign the respective VLAN to allow specific access through firewall.	"Solution should automatically detect the device type or OS and assign the respective VLAN."
22	**VENDOR**	**S.No.**	**Page No.**	**Point No.**	**Requirement**	**Specification**	**Justification and change**	**CCA/NIXI Response**
23	VENDOR-3	1	74	11	Load Balancer	The server load balancer should deliver at least 10 Gbps or higher of SSL throughput on 4096 key	Since all OEM do not publishes the key size, please revise this clause as " The server load balancer should deliver at least 10 Gbps or higher of SSL throughput"	Duplicate-Refer Response at Cons. S. No 7
24	VENDOR-3	2	74	12	Load Balancer	The server load balancer should cater up to at least 40K or higher SSL connections per second on 2K key from day 1	Kindly revise the specs for better participation and health competition. "The server load balancer should cater up to at least 35K or higher SSL connections per second from day 1"	Duplicate-Refer Response at Cons. S. No 8
25	VENDOR-3	3			Load Balancer	Additional Point	Load balancer should be capable to integrate with firewall to automatically block an IP with malicious activity detected.	Duplicate-Refer Response at Cons. S. No 9
26	VENDOR-3	4			Load Balancer	Additional Point	Load balancer should capable of anti-malware feature and integration with anti-apt solution for zero day inspection in future.	Duplicate-Refer Response at Cons. S. No 10
27	VENDOR-3	5	75	2	Firewall	Firewall appliance should be supplied with at least 4 x 1GE RJ-45 (expandable to total 8 ports) interfaces, 4 x 1G SFP slots (expandable to total 8 ports), 2 x10G SFP+ (expandable to total 8 ports). Solution should include all transceivers of populated modules (4x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fiber ports from day 1.	Kindly revise the specs for better participation and health competition. "Firewall appliance should be supplied with at least 4 x 1GE RJ-45 (expandable to total 8 ports) interfaces, 4 x 1G SFP slots (expandable to total 8 ports), 2 x10G SFP+ (expandable to total 4 ports). Solution should include all transceivers of populated modules (4x1Gb RJ-45, 4x1G SFP,2x10G SFP+) for fiber ports from day 1."	Duplicate-Refer Response at Cons. S. No 11
28	VENDOR-3	6	75	2	Firewall	Each appliance should have local available storage of 200 GB SSD after 1+1 RAID.	Kindly revise the specs as lower end appliance comes with inbuilt single disk. "Each appliance should have local available storage of 200 GB SSD."	Duplicate-Refer Response at Cons. S. No 12
29	VENDOR-3	7	75	5	Firewall	Appropriate energy efficient redundant (N+N) hot swappable power supplies.	Kindly remove this clause as high end appliance come with hot swappable power supply and this requirement is already captured under point number 34 for integrated redundant power supply.	Duplicate-Refer Response at Cons. S. No 13
30	VENDOR-3	8	75	9	Firewall	Threat Protection Throughput: 5 Gbps	Kindly revise the specs as appliance with 10Gbps firewall throughput comes with lower threat protection throughput and asked throughput is supported on higher models. "Threat Protection Throughput: 3 Gbps"	Duplicate-Refer Response at Cons. S. No 14
31	VENDOR-3	9	75	10	Firewall	Firewall should support at least 8 million concurrent sessions	Kindly revise the specs as 8 Million concurrent session seems higher on 10Gbps Firewall throughput appliance. "Firewall should support at least 3 million concurrent sessions"	Duplicate-Refer Response at Cons. S. No 15
32	VENDOR-3	10	75	24	Firewall	Should be supplied with 1000 SSL VPN users license.	Kindly revise the specs for better participation and health competition. "Should be supplied with 500 SSL VPN users license."	Duplicate-Refer Response at Cons. S. No 16
33	VENDOR-3	11	76	35	Firewall	Should have the IPS capability to inspect SSL traffic and SSL throughput of 9 Gbps.	Kindly revise the specs for better participation and healthy competition. "Should have the IPS capability to inspect SSL traffic and SSL throughput of 4 Gbps."	Duplicate-Refer Response at Cons. S. No 17
34	VENDOR-3	12	76	45	Firewall	Should support more than 2000+ application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	IPS signature supported is not mentioned, so request to revise specs. "Should support more than 2000+ application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness. Additionally firewall should have minimum 20000 IPS signature to prevent against vulnerabilities."	Duplicate-Refer Response at Cons. S. No 18

RESPONSES TO THE QUERIES RECEIVED AGAINST TENDER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023

35	VENDOR-3	13	77	53	Firewall	Server Security.	This requirement is pertaining to endpoint and not part of firewall so should be asked separately and request to remove point 53 to 57.	Duplicate-Refer Response at Cons. S. No 19
36	VENDOR-3	14	77	61	Firewall	Local malware analysis appliance should be of same OEM with 4x 1GE RJ45 interface and minimum throughput of 500 files/hour process across 6VMs or more. All VMs should be included from day 1.	We understand APT (sandboxing) solution is required to address Zero day threats and is essential part of perimeter security. It must be provided 1 each at perimeter level in DC & DR. Please confirm.	Duplicate-Refer Response at Cons. S. No 20
37	VENDOR-3	15	80		Switch	Additional Point	Solution should have capability of network access control. For example, feature should automatically detect the device type or OS and assign the respective VLAN to allow specific access through firewall.	Duplicate-Refer Response at Cons. S. No 21
38	VENDOR-3	16	61	2	Root CA	OCSP should be EAL + Certified	The Eligibility criteria does not mention this point nor awards any marks for OCSP Certification , since certificate revocation is the most critical as well as important step in any Web Trust Certified CA. We recommend that OCSP – EAL 4+ certification should be included the Eligibility Criteria and Extra marks should be added for the same as the opportunity is country's first and prestigious. We submit that 75% criteria for qualifying is low and even vendors who do not have this certification can qualify.	No Change
39	VENDOR-3	17	74	11	Load Balancer	The server load balancer should deliver at least 10 Gbps or higher of SSL throughput on 4096 key	As per best practice SSL throughput has to be maximum 50% to 60% of L7 throughput . Request you to revise the SSL throughput as "The server load balancer should deliver at least 8 Gbps or higher of SSL throughput on 4096 key"	Duplicate-Refer Response at Cons. S. No 7
40	VENDOR-3	18	74	12	Load Balancer	The server load balancer should cater up to at least 40K or higher SSL connections per second on 2K key from day 1	40K SSL CPS on 10Gbps of SSL throughput is on a higher side. Request you to amend this clause as "The server load balancer should cater up to at least 15K or higher SSL connections per second on 2K key from day 1"	Duplicate-Refer Response at Cons. S. No 8
41	VENDOR-3	19	74	13	Load Balancer	The sever load balancer should be proposed with 8 Ports populated with 4x1GE, 4x1G SFP ports and atleast 8x10G SFP+ SR ports from day 1	Port density for a 10 Gbps appliance is on a higher side. Request you to change the clause as "The sever load balancer should be proposed with 5x1GE, 4x1G SFP ports and at least 4x10G SFP+ SR ports from day 1	No change.
42	VENDOR-3	20	80	5	HSM	FIPS 140-3 Level 3, NIST SP 800-131A with valid	Should FIPS 140-2 level 3 be considered as Current Standard is FIPS 140-2 level 3 ? FIPS 140-3 level will be applicable after 2025 or later. Same hsm can be upgraded to latest firmware to achieve FIPS 140-3 level 3 certification later when FIPS 140-3 level 3 becomes mandatory. Also , NIST SP 800-131A is guidance and not certification specifically designed for key management appliance. In CA setup , HSM is the requirement. HSM provides key management through GUI and is covered under FIPS 140-2 level 3 . **Suggestion**: Request you to change it : FIPS 140-3 Level 3 with valid certification in the name of HSM OEM.	Clause may be read as "FIPS 140-2 Level 3 or higher with valid certification in the name of OEM".
43	VENDOR-3	21	56	5 (a)	Payment Terms	60 % total value of installed & accepted items at individual site on the completion of all Items Delivery, Installation, Testing, Commissioning and Acceptance per site	This is requested to be revised to 70% as most of the infrastructure work is completed.	No Change
44	VENDOR-3	22	56	5 (b)	Payment Terms	20% of the total value of installed & accepted items shall become payable after obtaining WebTrust Certification	This is requested to be revised to 30% as all the implementation has been completed. Integration with major web browsers is dependent on respective browser owners, we as an SI shall facilitate with TOTAL support required for this activity. However linking payment with this is not justified. Moreover, 5% PBG is already deposited to NIXI.	No Change
45	VENDOR-3	23	56	5 (c)	Payment Terms	20% of the total value of installed & accepted items shall become payable after Incorporation of CCA root in all Major Web Browsers	Needs to be removed as it has been discussed above in serial number 22	No Change
46	VENDOR-3	24	2		PBG	66 months PBG 5% of Bid Value	We request you to kindly revise it to 3% for a health cashflow.	No Change
47	VENDOR-3	25	40	5.6	IPR Rights	All deliverables, outputs, plans, drawings, specifications, designs, reports, and other documents and software submitted by the contractor under this Contract shall become and remain the property of the NIXI and must not be shared with third parties or reproduced, whether in whole or part, without the NIXI's prior written consent. The contractor shall, not later than upon termination or expiration of this Contract, deliver all such documents and software to the NIXI, together with a detailed inventory thereof.	The IPR of the software is with the owner of the same. The IPR rights cannot be transferred. If needed, the source code can be escrowed based as per the arrangements made by NIXI and cost considerations.	All deliverables, outputs, plans, drawings, specifications, designs, reports, and other documents and customised software submitted by the contractor under this Contract shall become and remain the property of the NIXI for CA, CCA for Root respectively and must not be shared with third parties or reproduced, whether in whole or part, without the NIXI (for CA) and CCA (for root) prior written consent. The contractor shall, not later than upon termination or expiration of this Contract, deliver all such documents and such customised softwares to the NIXI and CCA, together with a detailed inventory thereof.
48	VENDOR-3	26	68	A (iv)	Administrator Credential Management	The content of smart cards / tokens and other credential forms should be configurable, e.g. number and purpose of certificates, key length, validity etc.	Whole section is not relevant for SSL. Request to remove the scope.	Deleted
49	VENDOR-3	27	70	4 (I)	Secure Access	The proposed solution should have the option to login using multi factor Authentication such as PKI and One Time Passwords to log in as Operator/Administrator to manage devices in CMS.	Use of OTP in CMS may not be feasible as this is operated in a secured environment where phones are not allowed. And all the activities carried out by users are to be signed using digital certificate for data integrity protection and accountability.	Clause may be read as "The proposed solution should have the option to login using multi factor Authentication such as PKI to log in as Operator/Administrator to manage devices in CMS."
50	VENDOR-3	28	63		Bill of Material (BoM) & Format for Commercial Bids B. For Issuing SSL – CA	Firewall - 9 Nos.	Could you please provide us the break-up of the required quantity for the firewall for issuing CA	The no is as per the specific design. However the biddes may assess the numbers based on their actual design meeting all the requirments
51	**VENDOR**	**Sr. No**	**Page No.**		**RFP Clause**		**Request for clarification/Change**	**CCA/NIXI Response**
52	VENDOR-4	1	65		Hardware Load Balance requirement		Request to be optional in BoQ and Compliance. This may not be required in Solution.	No change. If for a particular design, Load Balancer can be avoided, the bidder may particularly indicate in the Technical Bid as well as in the Commercial Bid. However, bidder will ensure the design meets all WebTrust requirements.
53	VENDOR-4	2	65		Switching		Need to more clarity on the switches sizing and counts.	Qty mentioned in RFP - refer RFP
54	VENDOR-4	3	81		zero day malware protection		Zero day malware protect will require cloud based API and Managed console integration , while RA/CA zone will be isolated and may not require XDR/EDR kind of product. Only DMZ facing component may be leveraged with service . However data export to Cloud may not be advisable in web trust.	No change.
55	VENDOR-4	4			New Clause		Is there any specification for storage device , if required to place in solution?	No change.
56	VENDOR-4	5			New Clause		Is there any deviation possible in server configurations , if Storage need to be placed to cater the requirement.	No change.
57	VENDOR-4	6			New Clause		What is the signing performance is being expected via HSM.?	No change.
58	VENDOR-4	7			Additional Query		There are two Pre Bid queries from our side that is regarding OCSP and payments a. While the Bill of material for Root CA and Issuing CA mention the OCSP should be EAL + Certified the Eligibility criteria does not mention this point nor awards any marks for OCSP Certification , since certificate revocation is a important step in any Web Trust Certified CA we feel that OCSP – EAL 4+ certification should be included the Eligibility Criteria and extra marks should be added for the same . We must point out that at 75% the criteria for qualifying is low and even vendors who do have this certification can qualify . b. On payment Terms : Please request for payment term to change to 70% on UAT , 20% after Web Trust Audit and 10% after the CAB forum embedding of certificate.. on the last point we actually have no role to play and is likely to take 2 years .. so the lesser the amount the better . You as a bidder can elaborate on this better .. but a better payment term means better prices to the customer as the last part is practically a right off for all bidders .	No Change
59	**VENDOR**	**Sr. No.**	**Page Number**	**Section**	**Original Content in RFQ**	**Change sought/ Clarification**	**Remarks**	**CCA/NIXI Response**
60	VENDOR-5	1	75	2. Firewall / SN 2	Firewall appliance should be supplied with at least 4 x 1GE RJ-45 (expandable to total 8 ports) interfaces, 4 x 1G SFP slots (expandable to total 8 ports), 2 x10G SFP+ (expandable to total 8 ports). Solution should include all transceivers of populated modules (4x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports from day 1.	Firewall appliance should be supplied with at least 16 x 1GE RJ-45 6 x 10G/1G SFP+ ports. Solution should include all transceivers of populated modules (16x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports (MMF) from day 1.	The interface requirement of expansion modules is specific to OEM, hence request to change the expansion modules to fixed port from day 1.	Clause should be read as "Firewall appliance should be supplied with at least 4 x 1GE RJ-45 (expandable to total 8 ports) interfaces, 4 x 1G SFP slots (expandable to total 8 ports), 2 x10G SFP+ (expandable to total 4 ports). Solution should include all transceivers of populated modules (4x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports from day 1."
61	VENDOR-5	2	75	2. Firewall / SN 2	Each appliance should have local available storage of 200 GB SSD after 1+1 RAID.	Each appliance should have local available storage of 1 TB SSD in-built in the firewall from day 1..	NIXI should have min 1 TB storage in-built in the firewall for storing config data and logs in case of management server failure.	Clause should be read as "Each appliance should have local available storage of 200 GB SSD or higher from day1"
62	VENDOR-5	3	75	2. Firewall / SN 6	Should support Active:Active & Active:Passive modes	Should support Active:Active / Active:Passive modes	Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change.	clause may be read as "should support Active:Active / Active:Passive modes"

RESPONSES TO THE QUERIES RECEIVED AGAINST TENDER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023

63	VENDOR-5	4	75	2. Firewall / Performance & Scalability / SN 7	Firewall Throughput: Minimum 10 Gbps or higher throughput on 64 byte packets. Performance should not degrade while IPv6 is enabled in future.(F)	Firewall Throughput: Minimum 9 Gbps or higher throughput on 64 byte packets as per RFC 2544 .	Request to change as per RFC 2544 the Firewall throughput for 64 byte packets.	No change
64	VENDOR-5	5	75	2. Firewall / Performance & Scalability / SN 10	Firewall should support at least 8 million concurrent sessions	Firewall should support at least 4 million concurrent sessions	8 million concurrent connection is on a very highrer side for a 10 Gbps Firewall, hence request to reduce to 4 million.	Clause should be read as "Firewall should support at least 3 million concurrent sessions"
65	VENDOR-5	6	75	2. Firewall / Performance & Scalability / SN 11	Firewall should support at least 500K sessions per second	Firewall should support at least 110K sessions / connections per second	500K sessions/connections per secong is also a huge number for a 10 Gbps throughput firewall, hence request to reduce to 110K.	Clause should be read as "Firewall should support at least 250K sessions per second"
66	VENDOR-5	7	75	2. Firewall / Performance & Scalability / SN 12	Firewall should support at least 1000 VLANs	Firewall should support at least 500 VLANs	In any enterprise network requirement of 1000 VLANs is a huge ask, and we think that 500 + VLANs should be sufficient to meet the current requirement of NIXI.	Clause should be read as "Firewall should support at least 500 VLANs"
67	VENDOR-5	8	75	2. Firewall / Performance & Scalability / SN 14	Firewall should provide application detection for DNS, FTP, HTTP, SMTP, ESMTP, LDAP, RTSP, SIP, SQLNET, H.323, SNMP	Firewall should provide application detection for DNS, FTP, HTTP, SMTP, LDAP, RTSP, SIP, SQLNET, H.323, SNMP	Pls remove ESMTP as this is a email protocol and this is not the requirement in the current scenario of NIXI, as NIXI has separate email security solution.	Clause should be read as "Firewall should provide application detection for DNS, FTP, HTTP, SMTP, LDAP, RTSP, SIP, SQLNET, H.323, SNMP"
68	VENDOR-5	9	75	2. Firewall / Performance & Scalability / SN 17	Should support Static, RIP, OSPF, OSPFv3 and BGP	Should support Static, RIP, OSPF/OSPFv3 and BGP	The requirement is for a firewall and not a Router, so the dynamic routing protocols shall be handled by the router/L3 switch. Request change.	Clause should be read as "Should support Static, RIP, OSPF and BGP"
69	VENDOR-5	10	75	2. Firewall / Performance & Scalability / SN 19	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4- to-IPv6) functionality or firewall should be capable of supporting dual stack.	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) / Nat46 (IPv4- to-IPv6) functionality or firewall should be capable of supporting dual stack.	Request change.	No Change
70	VENDOR-5	11	75	2. Firewall / Performance & Scalability / SN 24	Should be supplied with 1000 SSL VPN users license	Should support 1000 SSL VPN licenses and should be supplied with 10 active SSL VON licenses from day 1.	Knowing the requirement of NIXI, 1000 SSL VPN license is a very high ask and is biased to one OEM. Hence request change.	Clause should be read as "Should be supplied with 500 SSL VPN users license."
71	VENDOR-5	12	75	2. Firewall / Performance & Scalability / SN 25	Ability to configure, manage and monitor NGFW using CLI and GUI both without central management solution. University would like to have full feature parity of centralized management tool on the Next Generation Firewall itself, in case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool.	Ability to configure, manage and monitor NGFW using CLI / GUI with / without central management solution. NIXI would like to have full feature parity with centralized management to manage the Next Generation Firewall. In case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool then firewall should have basic management.	Since there are 9 firewalls so its imperative to have a management tool and analytics software for managing the firewalls. This would also ensure smooth management for the Admins. So, asking the firewall to have a self management is biased towards OEM, as every OEM have different mechanism to manage one or multiple or 100s of firewalls.	Clause should be read as "Ability to configure, manage and monitor NGFW using CLI and GUI both without central management solution. Organization would like to have full feature parity of centralized management tool on the Next Generation Firewall itself, in case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool."
72	VENDOR-5	13	76	2. Firewall / Performance & Scalability / SN 26	The proposed firewall should be included with a solution to monitor and alert about the health of servers in the university like CPU, memory, disk, performance metrics etc. The solution should monitor at-least 20 servers and should be of same OEM for tight integration with firewall.	The proposed firewall should be included with a solution to monitor and alert about the health of servers at NIXI like CPU, memory, disk, performance metrics etc. The solution should monitor at-least 10 firewalls and the management tool should be of same OEM for tight integration with firewall.	NIXI is not a university but an etnerprise customer, pls pls remove the word University from the specification. Also the proposed solution should have management tool which should manage atleast 10 firewalls as per the requirement and not the servers. Hence request change.	In place of universty, please read as NIXI, for the Clause.
73	VENDOR-5	14	76	2. Firewall / Performance & Scalability / SN 27	Should have inbuilt feature for two factor authentication via OTP (email or mobile) for atleast two admin users access.	Should have inbuilt feature for two factor authentication via OTP (email or mobile) for atleast two admin users access or Should have inbuilt feature like SSO for atleast two admin firewall users.	Request change.	Clause may be read as "Should have inbuilt feature for two factor authentication for admin/users access".
74	VENDOR-5	15	76	2. Firewall / Performance & Scalability / SN 28	The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, University should have visibility of all its external facing servers/applications/IP addresses directly exposed to internet so that appropriate action can be taken on the application/network/firewall to mitigate misconfiguration and vulnerability of assets.	The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, NIXI should have visibility of all its external facing servers/applications/IP addresses directly exposed to internet so that appropriate action can be taken on the application/network/firewall to mitigate misconfiguration and vulnerability of assets.	NIXI is not a university but an etnerprise customer, pls pls remove the word University from the specification.	deleted
75	VENDOR-5	16	76	2. Firewall / Performance & Scalability / SN 29	The solution must have service which scans for university's credential leaked in the dark web and report to stake holders.	Delete	Pls delete this clause.	deleted
76	VENDOR-5	17	76	2. Firewall / Performance & Scalability / SN 30	Firewall should support Active/Standby and Active/Active failover and should not be based on stacking units in clustering	Firewall should support Active/Standby or Active/Active failover and should not be based on stacking units in clustering	Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change.	clause may be read as " Firewall should support Active/Standby or Active/Active failover and should not be based on stacking units in clustering".
77	VENDOR-5	18	76	2. Firewall / Performance & Scalability / SN 35	Should have the IPS capability to inspect SSL traffic and SSL throughput of 9 Gbps.	Should have the IPS capability to inspect SSL traffic and SSL throughput of 5 Gbps.	Request change.	Clause should be read as "Should have the IPS capability to inspect SSL traffic and SSL throughput of 4 Gbps."
78	VENDOR-5	19	76	2. Firewall / Performance & Scalability / SN 42	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance	300 secs update is very specific to one OEM, hence request to remove.	Clause should be read as "Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using MD5 , SHA-1 , SHA-2 file-hash or signature as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance"
79	VENDOR-5	20	76	2. Firewall / Performance & Scalability / SN 44	Should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 75 categories from day one.	Should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 55 categories from day one.	Inspection of 50+ categories should be enough for and URL Filtering requirement. Hence request change.	No change
80	VENDOR-5	21	77	2. Firewall / Performance & Scalability / SN 50	Web Application Firewall Protection	Delete	The requirement is for a firewall and not a WAF, hence request change.	No change
81	VENDOR-5	22	77	2. Firewall / Performance & Scalability / SN 51	Proposed appliance should have in-build WAF with Reverse proxy support,	Delete	This is a WAF feature and hence pls delete this clause.	No change
82	VENDOR-5	23	77	2. Firewall / Performance & Scalability / SN 52	SQL injection protection, Cross-site scripting protection, HTTPS (TLS/SSL) encryption offloading.	SQL injection protection, Cross-site scripting protection, HTTPS (TLS/SSL) encryption offloading / decryption.	Request change as the requirement is not for a WAF but a firewall.	No change
83	VENDOR-5	24	77	2. Firewall / Performance & Scalability / SN 53	Server security	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
84	VENDOR-5	25	77	2. Firewall / Performance & Scalability / SN 54	Solution must protect against ransomware and exploit and able to able to capture Viruses, Trojans, Worms, Spyware and Malware, Adware and PUA from single agent.The solution should able to integrate with on-premise sandbox appliance for zero day malware inspection.	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
85	VENDOR-5	26	77	2. Firewall / Performance & Scalability / SN 55	The Server Security Solution Should Support Multi-Platform operating system (Windows,Linux) and the same should be managed from a single Centralised Management console	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19

RESPONSES TO THE QUERIES RECEIVED AGAINST TENDER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023

86	VENDOR-5	27	77	2. Firewall / Performance & Scalability / SN 56	Server Security and Firewall should share the threat telemetry with each other, If both the solution are not from the same OEM it Should has open API option to integrate 3rd Party solution	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
87	VENDOR-5	28	77	2. Firewall / Performance & Scalability / SN 57	Solution must offer vulnerability management to verify servers	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
88	VENDOR-5	29	77	2. Firewall / Performance & Scalability / SN 59	Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware.	Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM-aware or memory based malware and protect from virtual sandbox evading advance unknown malware.	On-Premise sandbox has different advanced technologies for OEM to OEM, hence request change.	No change
89	VENDOR-5	30	77	2. Firewall / Performance & Scalability / SN 59	Solution should support OS type - Windows 10, Windows 8.1, Windows 7, Linux, Android.	Solution should support OS type - Windows 7 (32 / 64 bit), Linux 64	Request change as VMs in a on prem sandbox appliance vary from OEM to OEM.	Clause should be read as Solution should support latest/current versions OS types - Windows, Linux, Android.
90	VENDOR-5	31	77	2. Firewall / Performance & Scalability / SN 61	Local malware analysis appliance should be of same OEM with 4x 1GE RJ45 interface and minimum throughput of 500 files/hour process across 6VMs or more. All VMs should be included from day 1	Local malware analysis appliance should be of same OEM with 4x 1GE RJ45 interface and minimum throughput of 500 files/hour process across 6VMs or any other memory based technique.	Request change as VMs in a on prem sandbox appliance vary from OEM to OEM.	No change
91	VENDOR-5	32	77	2. Firewall / Performance & Scalability / SN 62	Solution should have feature to manually configure on what file types will run in which specific VM for optimal performance.	Solution should have feature to manually configure on what file types will run in which specific VM for optimal performance or should have memeory based inspection techniques	Request change as VMs in a on prem sandbox appliance vary from OEM to OEM.	No change
92	VENDOR-5	33	77	2. Firewall / Performance & Scalability / SN 71	Solution should have orchestrate, automate incident and response module for SOC operation with at least 2 user licenses from day 1.	Delete	Pls delete this clause, as this is not relevant in this specification.	No change
93	**VENDOR**	**Sr. No.**	**Page Number**	**Section**	**Original Content in RFQ**	**Change sought/ Clarification**	**Remarks**	**CCA/NIXI Response**
94	VENDOR-6	1	75	2. Firewall / SN 2	Firewall appliance should be supplied with at least 4 x 1GE RJ-45 (expandable to total 8 ports) interfaces, 4 x 1G SFP slots (expandable to total 8 ports), 2 x10G SFP+ (expandable to total 8 ports). Solution should include all transceivers of populated modules (4x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports from day 1.	Firewall appliance should be supplied with at least 16 x 1GE RJ-45 6 x 10G/1G SFP+ ports. Solution should include all transceivers of populated modules (16x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports (MMF) from day 1.	The interface requirement of expansion modules is specific to OEM, hence request to change the expansion modules to fixed port from day 1.	Duplicate-Refer Response at Cons. S. No 60
95	VENDOR-6	2	75	2. Firewall / SN 2	Each appliance should have local available storage of 200 GB SSD after 1+1 RAID.	Each appliance should have local available storage of 1 TB SSD in-built in the firewall from day 1..	NIXI should have min 1 TB storage in-built in the firewall for storing config data and logs in case of management server failure.	Duplicate-Refer Response at Cons. S. No 61
96	VENDOR-6	3	75	2. Firewall / SN 6	Should support Active:Active & Active:Passive modes	Should support Active:Active / Active:Passive modes	Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change.	Duplicate-Refer Response at Cons. S. No 62
97	VENDOR-6	4	75	2. Firewall / Performance & Scalability / SN 7	Firewall Throughput: Minimum 10 Gbps or higher throughput on 64 byte packets. Performance should not degrade while IPv6 is enabled in future.(F)	Firewall Throughput: Minimum 9 Gbps or higher throughput on 64 byte packets as per RFC 2544 .	Request to change as per RFC 2544 the Firewall throughput for 64 byte packets.	Duplicate-Refer Response at Cons. S. No 63
98	VENDOR-6	5	75	2. Firewall / Performance & Scalability / SN 10	Firewall should support at least 8 million concurrent sessions	Firewall should support at least 4 million concurrent sessions	8 million concurrent connection is on a very highrer side for a 10 Gbps Firewall, hence request to reduce to 4 million.	Duplicate-Refer Response at Cons. S. No. 64
99	VENDOR-6	6	75	2. Firewall / Performance & Scalability / SN 11	Firewall should support at least 500K sessions per second	Firewall should support at least 110K sessions / connections per second	500K sessions/connections per secong is also a huge number for a 10 Gbps throughput firewall, hence request to reduce to 110K.	Duplicate-Refer Response at Cons. S. No. 65
100	VENDOR-6	7	75	2. Firewall / Performance & Scalability / SN 12	Firewall should support at least 1000 VLANs	Firewall should support at least 500 VLANs	In any enterprise network requirement of 1000 VLANs is a huge ask, and we think that 500 + VLANs should be sufficient to meet the current requirement of NIXI.	Duplicate-Refer Response at Cons. S. No 66
101	VENDOR-6	8	75	2. Firewall / Performance & Scalability / SN 14	Firewall should provide application detection for DNS, FTP, HTTP, SMTP, ESMTP, LDAP, RTSP, SIP, SQLNET, H.323, SNMP	Firewall should provide application detection for DNS, FTP, HTTP, SMTP, LDAP, RTSP, SIP, SQLNET, H.323, SNMP	Pls remove ESMTP as this is a email protocol and this is not the requirement in the current scenario of NIXI, as NIXI has separate email security solution.	Duplicate-Refer Response at Cons. S. No 67
102	VENDOR-6	9	75	2. Firewall / Performance & Scalability / SN 17	Should support Static, RIP, OSPF, OSPFv3 and BGP	Should support Static, RIP, OSPF/OSPFv3 and BGP	The requirement is for a firewall and not a Router, so the dynamic routing protocols shall be handled by the router/L3 switch. Request change.	Duplicate-Refer Response at Cons. S. No 68
103	VENDOR-6	10	75	2. Firewall / Performance & Scalability / SN 19	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4- to-IPv6) functionality or firewall should be capable of supporting dual stack.	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) / Nat46 (IPv4- to-IPv6) functionality or firewall should be capable of supporting dual stack.	Request change.	Duplicate-Refer Response at Cons. S. No 69
104	VENDOR-6	11	75	2. Firewall / Performance & Scalability / SN 24	Should be supplied with 1000 SSL VPN users license	Should support 1000 SSL VPN licenses and should be supplied with 10 active SSL VON licenses from day 1.	Knowing the requirement of NIXI, 1000 SSL VPN license is a very high ask and is biased to one OEM. Hence request change.	Duplicate-Refer Response at Cons. S. No 70
105	VENDOR-6	12	75	2. Firewall / Performance & Scalability / SN 25	Ability to configure, manage and monitor NGFW using CLI and GUI both without central management solution. University would like to have full feature parity of centralized management tool on the Next Generation Firewall itself, in case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool.	Ability to configure, manage and monitor NGFW using CLI / GUI with / without central management solution. NIXI would like to have full feature parity with centralized management to manage the Next Generation Firewall. In case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool then firewall should have basic management.	Since there are 9 firewalls so its imperative to have a management tool and analytics software for managing the firewalls. This would also ensure smooth management for the Admins. So, asking the firewall to have a self management is biased towards OEM, as every OEM have different mechanism to manage one or multiple or 100s of firewalls.	Duplicate-Refer Response at Cons. S. No 71
106	VENDOR-6	13	76	2. Firewall / Performance & Scalability / SN 26	The proposed firewall should be included with a solution to monitor and alert about the health of servers in the university like CPU, memory, disk, performance metrics etc. The solution should monitor at-least 20 servers and should be of same OEM for tight integration with firewall.	The proposed firewall should be included with a solution to monitor and alert about the health of servers at NIXI like CPU, memory, disk, performance metrics etc. The solution should monitor at-least 10 firewalls and the management tool should be of same OEM for tight integration with firewall.	NIXI is not a university but an etnerprise customer, pls pls remove the word University from the specification. Also the proposed solution should have management tool which should manage atleast 10 firewalls as per the requirement and not the servers. Hence request change.	Duplicate-Refer Response at Cons. S. No 72
107	VENDOR-6	14	76	2. Firewall / Performance & Scalability / SN 27	Should have inbuilt feature for two factor authentication via OTP (email or mobile) for atleast two admin users access.	Should have inbuilt feature for two factor authentication via OTP (email or mobile) for atleast two admin users access or Should have inbuilt feature like SSO for atleast two admin firewall users.	Request change.	Duplicate-Refer Response at Cons. S. No 73
108	VENDOR-6	15	76	2. Firewall / Performance & Scalability / SN 28	The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, University should have visibility of all its external facing servers/applications/IP addresses directly exposed to internet so that appropriate action can be taken on the application/network/firewall to mitigate misconfiguration and vulnerability of assets.	The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, NIXI should have visibility of all its external facing servers/applications/IP addresses directly exposed to internet so that appropriate action can be taken on the application/network/firewall to mitigate misconfiguration and vulnerability of assets.	NIXI is not a university but an etnerprise customer, pls pls remove the word University from the specification.	Duplicate-Refer Response at Cons. S. No 74
109	VENDOR-6	16	76	2. Firewall / Performance & Scalability / SN 29	The solution must have service which scans for university's credential leaked in the dark web and report to stake holders.	Delete	Pls delete this clause.	Duplicate-Refer Response at Cons. S. No 75
110	VENDOR-6	17	76	2. Firewall / Performance & Scalability / SN 30	Firewall should support Active/Standby and Active/Active failover and should not be based on stacking units in clustering	Firewall should support Active/Standby or Active/Active failover and should not be based on stacking units in clustering	Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change.	Duplicate-Refer Response at Cons. S. No 76
111	VENDOR-6	18	76	2. Firewall / Performance & Scalability / SN 35	Should have the IPS capability to inspect SSL traffic and SSL throughput of 9 Gbps.	Should have the IPS capability to inspect SSL traffic and SSL throughput of 5 Gbps.	Request change.	Duplicate-Refer Response at Cons. S. No 77

RESPONSES TO THE QUERIES RECEIVED AGAINST TENDER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023

112	VENDOR-6	19	76	2. Firewall / Performance & Scalability / SN 42	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance	300 secs update is very specific to one OEM, hence request to remove.	Duplicate-Refer Response at Cons. S. No 78
113	VENDOR-6	20	76	2. Firewall / Performance & Scalability / SN 44	Should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 75 categories from day one.	Should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 55 categories from day one.	Inspection of 50+ categories should be enough for and URL Filtering requirement. Hence request change.	Duplicate-Refer Response at Cons. S. No 79
114	VENDOR-6	21	77	2. Firewall / Performance & Scalability / SN 50	Web Application Firewall Protection	Delete	The requirement is for a firewall and not a WAF, hence request change.	Duplicate-Refer Response at Cons. S. No 80
115	VENDOR-6	22	77	2. Firewall / Performance & Scalability / SN 51	Proposed appliance should have in-build WAF with Reverse proxy support,	Delete	This is a WAF feature and hence pls delete this clause.	Duplicate-Refer Response at Cons. S. No 81
116	VENDOR-6	23	77	2. Firewall / Performance & Scalability / SN 52	SQL injection protection, Cross-site scripting protection, HTTPS (TLS/SSL) encryption offloading.	SQL injection protection, Cross-site scripting protection, HTTPS (TLS/SSL) encryption offloading / decryption.	Request change as the requirement is not for a WAF but a firewall.	Duplicate-Refer Response at Cons. S. No 82
117	VENDOR-6	24	77	2. Firewall / Performance & Scalability / SN 53	Server security	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
118	VENDOR-6	25	77	2. Firewall / Performance & Scalability / SN 54	Solution must protect against ransomware and exploit and able to able to capture Viruses, Trojans, Worms, Spyware and Malware, Adware and PUA from single agent.The solution should able to integrate with on-premise sandbox appliance for zero day malware inspection.	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
119	VENDOR-6	26	77	2. Firewall / Performance & Scalability / SN 55	The Server Security Solution Should Support Multi-Platform operating system (Windows,Linux) and the same should be managed from a single Centralised Management console	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
120	VENDOR-6	27	77	2. Firewall / Performance & Scalability / SN 56	Server Security and Firewall should share the threat telemetry with each other, If both the solution are not from the same OEM it Should has open API option to integrate 3rd Party solution	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
121	VENDOR-6	28	77	2. Firewall / Performance & Scalability / SN 57	Solution must offer vulnerability management to verify servers	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
122	VENDOR-6	29	77	2. Firewall / Performance & Scalability / SN 59	Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware.	Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM-aware or memory based malware and protect from virtual sandbox evading advance unknown malware.	On-Premise sandbox has different advanced technologies for OEM to OEM, hence request change.	Duplicate-Refer Response at Cons. S. No 88
123	VENDOR-6	30	77	2. Firewall / Performance & Scalability / SN 59	Solution should support OS type - Windows 10, Windows 8.1, Windows 7, Linux, Android.	Solution should support OS type - Windows 7 (32 / 64 bit), Linux 64	Request change as VMs in a on prem sandbox appliance vary from OEM to OEM.	Duplicate-Refer Response at Cons. S. No 89
124	VENDOR-6	31	77	2. Firewall / Performance & Scalability / SN 61	Local malware analysis appliance should be of same OEM with 4x 1GE RJ45 interface and minimum throughput of 500 files/hour process across 6VMs or more. All VMs should be included from day 1	Local malware analysis appliance should be of same OEM with 4x 1GE RJ45 interface and minimum throughput of 500 files/hour process across 6VMs or any other memory based technique.	Request change as VMs in a on prem sandbox appliance vary from OEM to OEM.	Duplicate-Refer Response at Cons. S. No 90
125	VENDOR-6	32	77	2. Firewall / Performance & Scalability / SN 62	Solution should have feature to manually configure on what file types will run in which specific VM for optimal performance.	Solution should have feature to manually configure on what file types will run in which specific VM for optimal performance or should have memeory based inspection techniques	Request change as VMs in a on prem sandbox appliance vary from OEM to OEM.	Duplicate-Refer Response at Cons. S. No 91
126	VENDOR-6	33	77	2. Firewall / Performance & Scalability / SN 71	Solution should have orchestrate, automate incident and response module for SOC operation with at least 2 user licenses from day 1.	Delete	Pls delete this clause, as this is not relevant in this specification.	Duplicate-Refer Response at Cons. S. No 92
127	VENDOR-6	34	8	Eligibility Criteriaa	The Bidder shall have revenue of INR 75 crores and shall be profitable for the last 3 financial years (FY 2021-22, 20-21, 19-20). The evidences shall be provided.	The Bidder shall have revenue of INR 45 crores and shall be profitable for the last 3 financial years (FY 2021-22, 20-21, 19-20). The evidences shall be provided.	Pls aamend this clause, as this will help maany of the perspective serious bidders.	No Change
128	**VENDOR**	**Sr. No.**	**Page Number**	**Section**	**Original Content in RFQ**	**Change sought/ Clarification**	**Remarks**	**CCA/NIXI Response**
129	VENDOR-7	1	75	2. Firewall / SN 2	Firewall appliance should be supplied with at least 4 x 1GE RJ-45 (expandable to total 8 ports) interfaces, 4 x 1G SFP slots (expandable to total 8 ports), 2 x10G SFP+ (expandable to total 8 ports). Solution should include all transceivers of populated modules (4x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports from day 1.	Firewall appliance should be supplied with at least 16 x 1GE RJ-45 6 x 10G/1G SFP+ ports. Solution should include all transceivers of populated modules (16x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports (MMF) from day 1.	The interface requirement of expansion modules is specific to OEM, hence request to change the expansion modules to fixed port from day 1.	Duplicate-Refer Response at Cons. S. No 60
130	VENDOR-7	2	75	2. Firewall / SN 2	Each appliance should have local available storage of 200 GB SSD after 1+1 RAID.	Each appliance should have local available storage of 1 TB SSD in-built in the firewall from day 1..	NIXI should have min 1 TB storage in-built in the firewall for storing config data and logs in case of management server failure.	Duplicate-Refer Response at Cons. S. No 61
131	VENDOR-7	3	75	2. Firewall / SN 6	Should support Active:Active & Active:Passive modes	Should support Active:Active / Active:Passive modes	Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change.	Duplicate-Refer Response at Cons. S. No 62
132	VENDOR-7	4	75	2. Firewall / Performance & Scalability / SN 7	Firewall Throughput: Minimum 10 Gbps or higher throughput on 64 byte packets. Performance should not degrade while IPv6 is enabled in future.(F)	Firewall Throughput: Minimum 9 Gbps or higher throughput on 64 byte packets as per RFC 2544 .	Request to change as per RFC 2544 the Firewall throughput for 64 byte packets.	Duplicate-Refer Response at Cons. S. No 63
133	VENDOR-7	5	75	2. Firewall / Performance & Scalability / SN 10	Firewall should support at least 8 million concurrent sessions	Firewall should support at least 4 million concurrent sessions	8 million concurrent connection is on a very highrer side for a 10 Gbps Firewall, hence request to reduce to 4 million.	Duplicate-Refer Response at Cons. S. No. 64
134	VENDOR-7	6	75	2. Firewall / Performance & Scalability / SN 11	Firewall should support at least 500K sessions per second	Firewall should support at least 110K sessions / connections per second	500K sessions/connections per secong is also a huge number for a 10 Gbps throughput firewall, hence request to reduce to 110K.	Duplicate-Refer Response at Cons. S. No. 65
135	VENDOR-7	7	75	2. Firewall / Performance & Scalability / SN 12	Firewall should support at least 1000 VLANs	Firewall should support at least 500 VLANs	In any enterprise network requirement of 1000 VLANs is a huge ask, and we think that 500 + VLANs should be sufficient to meet the current requirement of NIXI.	Duplicate-Refer Response at Cons. S. No 66
136	VENDOR-7	8	75	2. Firewall / Performance & Scalability / SN 14	Firewall should provide application detection for DNS, FTP, HTTP, SMTP, ESMTP, LDAP, RTSP, SIP, SQLNET, H.323, SNMP	Firewall should provide application detection for DNS, FTP, HTTP, SMTP, LDAP, RTSP, SIP, SQLNET, H.323, SNMP	Pls remove ESMTP as this is a email protocol and this is not the requirement in the current scenario of NIXI, as NIXI has separate email security solution.	Duplicate-Refer Response at Cons. S. No 67
137	VENDOR-7	9	75	2. Firewall / Performance & Scalability / SN 17	Should support Static, RIP, OSPF, OSPFv3 and BGP	Should support Static, RIP, OSPF/OSPFv3 and BGP	The requirement is for a firewall and not a Router, so the dynamic routing protocols shall be handled by the router/L3 switch. Request change.	Duplicate-Refer Response at Cons. S. No 68
138	VENDOR-7	10	75	2. Firewall / Performance & Scalability / SN 19	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4- to-IPv6) functionality or firewall should be capable of supporting dual stack.	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) / Nat46 (IPv4- to-IPv6) functionality or firewall should be capable of supporting dual stack.	Request change.	Duplicate-Refer Response at Cons. S. No 69
139	VENDOR-7	11	75	2. Firewall / Performance & Scalability / SN 24	Should be supplied with 1000 SSL VPN users license	Should support 1000 SSL VPN licenses and should be supplied with 10 active SSL VON licenses from day 1.	Knowing the requirement of NIXI, 1000 SSL VPN license is a very high ask and is biased to one OEM. Hence request change.	Duplicate-Refer Response at Cons. S. No 70

RESPONSES TO THE QUERIES RECEIVED AGAINST TENDER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023

140	VENDOR-7	12	75	2. Firewall / Performance & Scalability / SN 25	Ability to configure, manage and monitor NGFW using CLI and GUI both without central management solution. University would like to have full feature parity of centralized management tool on the Next Generation Firewall itself, in case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool.	Ability to configure, manage and monitor NGFW using CLI / GUI with / without central management solution. NIXI would like to have full feature parity with centralized management to manage the Next Generation Firewall. In case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool then firewall should have basic management.	Since there are 9 firewalls so its imperative to have a management tool and analytics software for managing the firewalls. This would also ensure smooth management for the Admins. So, asking the firewall to have a self management is biased towards OEM, as every OEM have different mechanism to manage one or multiple or 100s of firewalls.	Duplicate-Refer Response at Cons. S. No 71
141	VENDOR-7	13	76	2. Firewall / Performance & Scalability / SN 26	The proposed firewall should be included with a solution to monitor and alert about the health of servers in the university like CPU, memory, disk, performance metrics etc. The solution should monitor at-least 20 servers and should be of same OEM for tight integration with firewall.	The proposed firewall should be included with a solution to monitor and alert about the health of servers at NIXI like CPU, memory, disk, performance metrics etc. The solution should monitor at-least 10 firewalls and the management tool should be of same OEM for tight integration with firewall.	NIXI is not a university but an etnerprise customer, pls pls remove the word University from the specification. Also the proposed solution should have management tool which should manage atleast 10 firewalls as per the requirement and not the servers. Hence request change.	Duplicate-Refer Response at Cons. S. No 72
142	VENDOR-7	14	76	2. Firewall / Performance & Scalability / SN 27	Should have inbuilt feature for two factor authentication via OTP (email or mobile) for atleast two admin users access.	Should have inbuilt feature for two factor authentication via OTP (email or mobile) for atleast two admin users access or Should have inbuilt feature like SSO for atleast two admin firewall users.	Request change.	Duplicate-Refer Response at Cons. S. No 73
143	VENDOR-7	15	76	2. Firewall / Performance & Scalability / SN 28	The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, University should have visibility of all its external facing servers/applications/IP addresses directly exposed to internet so that appropriate action can be taken on the application/network/firewall to mitigate misconfiguration and vulnerability of assets.	The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, NIXI should have visibility of all its external facing servers/applications/IP addresses directly exposed to internet so that appropriate action can be taken on the application/network/firewall to mitigate misconfiguration and vulnerability of assets.	NIXI is not a university but an etnerprise customer, pls pls remove the word University from the specification.	Duplicate-Refer Response at Cons. S. No 74
144	VENDOR-7	16	76	2. Firewall / Performance & Scalability / SN 29	The solution must have service which scans for university's credential leaked in the dark web and report to stake holders.	Delete	Pls delete this clause.	Duplicate-Refer Response at Cons. S. No 75
145	VENDOR-7	17	76	2. Firewall / Performance & Scalability / SN 30	Firewall should support Active/Standby and Active/Active failover and should not be based on stacking units in clustering	Firewall should support Active/Standby or Active/Active failover and should not be based on stacking units in clustering	Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change.	Duplicate-Refer Response at Cons. S. No 76
146	VENDOR-7	18	76	2. Firewall / Performance & Scalability / SN 35	Should have the IPS capability to inspect SSL traffic and SSL throughput of 9 Gbps.	Should have the IPS capability to inspect SSL traffic and SSL throughput of 5 Gbps.	Request change.	Duplicate-Refer Response at Cons. S. No 77
147	VENDOR-7	19	76	2. Firewall / Performance & Scalability / SN 42	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance	300 secs update is very specific to one OEM, hence request to remove.	Duplicate-Refer Response at Cons. S. No 78
148	VENDOR-7	20	76	2. Firewall / Performance & Scalability / SN 44	Should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 75 categories from day one.	Should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 55 categories from day one.	Inspection of 50+ categories should be enough for and URL Filtering requirement. Hence request change.	Duplicate-Refer Response at Cons. S. No 79
149	VENDOR-7	21	77	2. Firewall / Performance & Scalability / SN 50	Web Application Firewall Protection	Delete	The requirement is for a firewall and not a WAF, hence request change.	Duplicate-Refer Response at Cons. S. No 80
150	VENDOR-7	22	77	2. Firewall / Performance & Scalability / SN 51	Proposed appliance should have in-build WAF with Reverse proxy support,	Delete	This is a WAF feature and hence pls delete this clause.	Duplicate-Refer Response at Cons. S. No 81
151	VENDOR-7	23	77	2. Firewall / Performance & Scalability / SN 52	SQL injection protection, Cross-site scripting protection, HTTPS (TLS/SSL) encryption offloading.	SQL injection protection, Cross-site scripting protection, HTTPS (TLS/SSL) encryption offloading / decryption.	Request change as the requirement is not for a WAF but a firewall.	Duplicate-Refer Response at Cons. S. No 82
152	VENDOR-7	24	77	2. Firewall / Performance & Scalability / SN 53	Server security	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
153	VENDOR-7	25	77	2. Firewall / Performance & Scalability / SN 54	Solution must protect against ransomware and exploit and able to able to capture Viruses, Trojans, Worms, Spyware and Malware, Adware and PUA from single agent.The solution should able to integrate with on-premise sandbox appliance for zero day malware inspection.	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
154	VENDOR-7	26	77	2. Firewall / Performance & Scalability / SN 55	The Server Security Solution Should Support Multi-Platform operating system (Windows,Linux) and the same should be managed from a single Centralised Management console	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
155	VENDOR-7	27	77	2. Firewall / Performance & Scalability / SN 56	Server Security and Firewall should share the threat telemetry with each other, If both the solution are not from the same OEM it Should has open API option to integrate 3rd Party solution	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
156	VENDOR-7	28	77	2. Firewall / Performance & Scalability / SN 57	Solution must offer vulnerability management to verify servers	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
157	VENDOR-7	29	77	2. Firewall / Performance & Scalability / SN 59	Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware.	Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM-aware or memory based malware and protect from virtual sandbox evading advance unknown malware.	On-Premise sandbox has different advanced technologies for OEM to OEM, hence request change.	Duplicate-Refer Response at Cons. S. No 88
158	VENDOR-7	30	77	2. Firewall / Performance & Scalability / SN 59	Solution should support OS type - Windows 10, Windows 8.1, Windows 7, Linux, Android.	Solution should support OS type - Windows 7 (32 / 64 bit), Linux 64	Request change as VMs in a on prem sandbox appliance vary from OEM to OEM.	Duplicate-Refer Response at Cons. S. No 89
159	VENDOR-7	31	77	2. Firewall / Performance & Scalability / SN 61	Local malware analysis appliance should be of same OEM with 4x 1GE RJ45 interface and minimum throughput of 500 files/hour process across 6VMs or more. All VMs should be included from day 1	Local malware analysis appliance should be of same OEM with 4x 1GE RJ45 interface and minimum throughput of 500 files/hour process across 6VMs or any other memory based technique.	Request change as VMs in a on prem sandbox appliance vary from OEM to OEM.	Duplicate-Refer Response at Cons. S. No 90
160	VENDOR-7	32	77	2. Firewall / Performance & Scalability / SN 62	Solution should have feature to manually configure on what file types will run in which specific VM for optimal performance.	Solution should have feature to manually configure on what file types will run in which specific VM for optimal performance or should have memeory based inspection techniques	Request change as VMs in a on prem sandbox appliance vary from OEM to OEM.	Duplicate-Refer Response at Cons. S. No 91
161	VENDOR-7	33	77	2. Firewall / Performance & Scalability / SN 71	Solution should have orchestrate, automate incident and response module for SOC operation with at least 2 user licenses from day 1.	Delete	Pls delete this clause, as this is not relevant in this specification.	Duplicate-Refer Response at Cons. S. No 92
162	**VENDOR**	**Sl. No.**	**RFP Page No.**	**RFP Section**	**Content of RFP requiring clarification(s)**	**Points of clarification**	**Remarks / Suggestions (If Any)**	**CCA/NIXI Response**

RESPONSES TO THE QUERIES RECEIVED AGAINST TENDER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023

163	VENDOR-8	**1**	78	4. HSM Module: Minimum Technical Specification	HSM should be network based appliance with inbuilt NIC support for 1 GB and 10 GB network.	As per the industry standard, an HSM comes with Dual Gigabit network interface with port bonding support. 10 network ports is not mandatory.	Please revise it to Dual Gigabit or Dual 10G network interfaces.	No Change
164	VENDOR-8	2	79	4. HSM Module: Minimum Technical Specification	Host Interface: Should have inbuilt Dual Gigabit Ethernet ports with port bonding and Dual 10G network port with port bonding. All four NICs should have IPv4 and IPv6 support. Capabilities should be from day 1	As per the industry standard, an HSM comes with Dual Gigabit network interface with port bonding support. 10 network ports is not mandatory.	Please revise it to Dual Gigabit or Dual 10G network interfaces.	Host Interface: Should have inbuilt Dual Gigabit (or Higher Gigabit) port with port bonding and should be ready from day 1. All NICs should have IPv4 and IPv6 support capabilities from day 1.
165	VENDOR-8	3	79	4. HSM Module: Minimum Technical Specification	Support for Hash Message Digest HMAC, SHA1, SHA2 (512), SM3 and SM4	Please note that SM3 and SM4 are Chinese hashing algorithms required for Chinese regulations. This does not apply to Indian regulations.	Request you to kindly remove the clause.	Duplicate-Refer Response at Cons. S. No 2
166	VENDOR-8	4	79	4. HSM Module: Minimum Technical Specification	HSM should have simulator capabilities to provide development , integration and Testing of applications in restricted network with no outside connectivity to internet .	Please note that an HSM simulator should not be used for development and integration, primarily because the keys are stored in the application itself. Moreover, the test results on a HSM simulator will differ drastically with a real HSM. Instead a low performance should be used for test and integration purposes.	Request you to kindly remove the clause.	Deleted
167	VENDOR-8	5	79	4. HSM Module: Minimum Technical Specification	HSM should have unlimited client Licenses (Should not have separate cost of any client License)	Could someone please confirm the rationnale behind the ask. Unlimited client licenses suggest that any no. of client applications can connect to the HSM. This makes the HSM more vulnerable and the performance of the HSM will degrade.	Request you to kindly remove the clause.	No change
168	VENDOR-8	6	79	4. HSM Module: Minimum Technical Specification	HSM should be FIPS 140-2 Level 3 certified and certification should be in OEM Name. Certification Copy needs to be submitted	The newer or latest certification of HSMs is FIPS 140-3 Level 3.	Request you to kindly make it to FIPS 140-3 Level 3.	Duplicate-Refer Response at Cons. S. No 3
169	VENDOR-8	7	61	Section IV	BOM Root CA: 4x network HSM, 2x PCI HSM	Can we assume there are 3 environments - PDN, DR and UAT(QA)?. Can we know how is the HSM quantity derived?		The quantity is as per the Tender indicative design. Bidder will offer their design meeting all the requirements of the Tender. However for cost comparisions, the tender indicative quantities will be considered if the proposed design carry less no of items as compared to the tender indicated items. Howeever, if the requirements as per the bidder's design, are more, then actual numbers of items will be considerd (based on the unit rates) for comparisions.
170	VENDOR-8	8	63	Section IV	BOM Issuing CA: 10x network HSM, 2x PCI HSM	Can we assume there are 3 environments - PDN, DR and UAT(QA)?. Can we know how is the HSM quantity derived?		The quantity is as per the Tender indicative design. Bidder will offer their design meeting all the requirements of the Tender. However for cost comparisions, the tender indicative quantities will be considered if the proposed design carry less no of items as compared to the tender indicated items. However, if the requirements as per the bidder's design, are more, then actual numbers of items will be considerd (based on the unit rates) for comparisions.
171	VENDOR-8	9	80	4. HSM Module: Minimum Technical Specification	FIPS 140-3 Level 3, NIST SP 800-131A with valid certification	As of today, FIPS 140-3 level 3 certification is in progress and should be available in near future.	Please confirm if FIPS 140-3 Level 3 is the ask.	Clause may be read as "FIPS 140-2 Level 3" or higher, with valid certification in the name of OEM".
172	VENDOR-8	10	9	1	The Bidder shall ... perform the WebTrust certification program including incorporation of CA root in Major Web Browsers	Usually auditors are engaged by the CA owner, as it will be a multi year project to get into the broswer and is costly. Suggestion is for CA Vendor to provide PKI discovery workshop, steps, governance consultancuy for NIXI to get into Webtrust and browser program. Audit should be taken up by NIXI with the support of CA Vendor.	From Entrust's experience, it will take 2 - 3 years to get into all browsers and operating systems, assuming passing audit the first time. Typically, getting into all the browser vendor programs will take more than 5 years. Acceptance into each vendor root programs is by submission of a recognized audit report. Each vendor program makes its own decisions on adding a CA. It will require dedicated NIXI staffs to manage the compliance program	No change
173	VENDOR-8	11	44	6	The Bidder shall ... perform the WebTrust certification program including incorporation of CA root in Major Web Browsers	Current broswers under CA/B forum are Mozilla, Microsoft, Google, Apple. What is the priority of broswers to be recognized?		There is no priority as per NIXI is concerend.
174	VENDOR-8	12	48	6.1	Contractor will carry out Vulnerability assessment (VA) and Penetration Testing (PT) using certified tool through a Third-party certified agency before acceptance, if required.	Under what situation are the 2 tests required?		This is a security norm and needs to be followed as per the Audit Requirements.
175	VENDOR-8	13	49	6.2	compliance requirements set forth by the CA/Browser Forum for publicly-trusted CAs (i.e. Baseline Requirements, Network Security Requirements, Code Signing, Extended Validation, etc.) in the conduct of any assurance engagement or internal audits for Public PKIs.	Other than DV, EV and OV TLS certs, is Code-signing cert required? It was not mentioned in page 43 "solution should mean for Organization Validation (OV) and Domain Validation (DV)"		The requiremnt is a generic one and even if it is not required in the first year, it will be reqiuired in the subsequently.
176	VENDOR-8	14	68	Section V	There should be a powerful API that supports certification, revocation for any end entity as well as to retrieve user and certificate information. The API should be access controlled	What needs to be integrated with the CA?		The clause is self explanatory and for further information, WebTrust requirements may be referred.
177	VENDOR-8	15	71	Section B	Suggested Architecture for Root SSL CA	Can we propose other architecture e.g. offline Root, based on best practices instead?		The Root may be offline and design may accordingly be proposed.
178	VENDOR-8	16	141	Checklist	The CA follows a CA key migration script for key migration events that includes the following...	What existing keys need to be migrated, and from what system?		Checklist Point is self explainatory
179	**VENDOR**	**Sr. No.**	**Page Number**	**Section**	**Original Content in RFQ**	**Change sought/ Clarification**	**Remarks**	**CCA/NIXI Response**
180	VENDOR-9	1	75	2. Firewall / SN 2	Firewall appliance should be supplied with at least 4 x 1GE RJ-45 (expandable to total 8 ports) interfaces, 4 x 1G SFP slots (expandable to total 8 ports), 2 x10G SFP+ (expandable to total 8 ports). Solution should include all transceivers of populated modules (4x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports from day 1.	Firewall appliance should be supplied with at least 16 x 1GE RJ-45 6 x 10G/1G SFP+ ports. Solution should include all transceivers of populated modules (16x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports (MMF) from day 1.	The interface requirement of expansion modules is specific to OEM, hence request to change the expansion modules to fixed port from day 1.	Duplicate-Refer Response at Cons. S. No 60
181	VENDOR-9	2	75	2. Firewall / SN 2	Each appliance should have local available storage of 200 GB SSD after 1+1 RAID.	Each appliance should have local available storage of 1 TB SSD in-built in the firewall from day 1..	NIXI should have min 1 TB storage in-built in the firewall for storing config data and logs in case of management server failure.	Duplicate-Refer Response at Cons. S. No 61
182	VENDOR-9	3	75	2. Firewall / SN 6	Should support Active:Active & Active:Passive modes	Should support Active:Active / Active:Passive modes	Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change.	Duplicate-Refer Response at Cons. S. No 62
183	VENDOR-9	4	75	2. Firewall / Performance & Scalability / SN 7	Firewall Throughput: Minimum 10 Gbps or higher throughput on 64 byte packets. Performance should not degrade while IPv6 is enabled in future.(F)	Firewall Throughput: Minimum 9 Gbps or higher throughput on 64 byte packets as per RFC 2544 .	Request to change as per RFC 2544 the Firewall throughput for 64 byte packets.	Duplicate-Refer Response at Cons. S. No 63
184	VENDOR-9	5	75	2. Firewall / Performance & Scalability / SN 10	Firewall should support at least 8 million concurrent sessions	Firewall should support at least 4 million concurrent sessions	8 million concurrent connection is on a very highrer side for a 10 Gbps Firewall, hence request to reduce to 4 million.	Duplicate-Refer Response at Cons. S. No. 64
185	VENDOR-9	6	75	2. Firewall / Performance & Scalability / SN 11	Firewall should support at least 500K sessions per second	Firewall should support at least 110K sessions / connections per second	500K sessions/connections per secong is also a huge number for a 10 Gbps throughput firewall, hence request to reduce to 110K.	Duplicate-Refer Response at Cons. S. No. 65
186	VENDOR-9	7	75	2. Firewall / Performance & Scalability / SN 12	Firewall should support at least 1000 VLANs	Firewall should support at least 500 VLANs	In any enterprise network requirement of 1000 VLANs is a huge ask, and we think that 500 + VLANs should be sufficient to meet the current requirement of NIXI.	Duplicate-Refer Response at Cons. S. No 66
187	VENDOR-9	8	75	2. Firewall / Performance & Scalability / SN 14	Firewall should provide application detection for DNS, FTP, HTTP, SMTP, ESMTP, LDAP, RTSP, SIP, SQLNET, H.323, SNMP	Firewall should provide application detection for DNS, FTP, HTTP, SMTP, LDAP, RTSP, SIP, SQLNET, H.323, SNMP	Pls remove ESMTP as this is a email protocol and this is not the requirement in the current scenario of NIXI, as NIXI has separate email security solution.	Duplicate-Refer Response at Cons. S. No 67

RESPONSES TO THE QUERIES RECEIVED AGAINST TENDER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023

188	VENDOR-9	9	75	2. Firewall / Performance & Scalability / SN 17	Should support Static, RIP, OSPF, OSPFv3 and BGP	Should support Static, RIP, OSPF/OSPFv3 and BGP	The requirement is for a firewall and not a Router, so the dynamic routing protocols shall be handled by the router/L3 switch. Request change.	Duplicate-Refer Response at Cons. S. No 68
189	VENDOR-9	10	75	2. Firewall / Performance & Scalability / SN 19	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4- to-IPv6) functionality or firewall should be capable of supporting dual stack.	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) / Nat46 (IPv4- to-IPv6) functionality or firewall should be capable of supporting dual stack.	Request change.	Duplicate-Refer Response at Cons. S. No 69
190	VENDOR-9	11	75	2. Firewall / Performance & Scalability / SN 24	Should be supplied with 1000 SSL VPN users license	Should support 1000 SSL VPN licenses and should be supplied with 10 active SSL VON licenses from day 1.	Knowing the requirement of NIXI, 1000 SSL VPN license is a very high ask and is biased to one OEM. Hence request change.	Duplicate-Refer Response at Cons. S. No 70
191	VENDOR-9	12	75	2. Firewall / Performance & Scalability / SN 25	Ability to configure, manage and monitor NGFW using CLI and GUI both without central management solution. University would like to have full feature parity of centralized management tool on the Next Generation Firewall itself, in case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool.	Ability to configure, manage and monitor NGFW using CLI / GUI with / without central management solution. NIXI would like to have full feature parity with centralized management to manage the Next Generation Firewall. In case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool then firewall should have basic management.	Since there are 9 firewalls so its imperative to have a management tool and analytics software for managing the firewalls. This would also ensure smooth management for the Admins. So, asking the firewall to have a self management is biased towards OEM, as every OEM have different mechanism to manage one or multiple or 100s of firewalls.	Duplicate-Refer Response at Cons. S. No 71
192	VENDOR-9	13	76	2. Firewall / Performance & Scalability / SN 26	The proposed firewall should be included with a solution to monitor and alert about the health of servers in the university like CPU, memory, disk, performance metrics etc. The solution should monitor at-least 20 servers and should be of same OEM for tight integration with firewall.	The proposed firewall should be included with a solution to monitor and alert about the health of servers at NIXI like CPU, memory, disk, performance metrics etc. The solution should monitor at-least 10 firewalls and the management tool should be of same OEM for tight integration with firewall.	NIXI is not a university but an etnerprise customer, pls pls remove the word University from the specification. Also the proposed solution should have management tool which should manage atleast 10 firewalls as per the requirement and not the servers. Hence request change.	Duplicate-Refer Response at Cons. S. No 72
193	VENDOR-9	14	76	2. Firewall / Performance & Scalability / SN 27	Should have inbuilt feature for two factor authentication via OTP (email or mobile) for atleast two admin users access.	Should have inbuilt feature for two factor authentication via OTP (email or mobile) for atleast two admin users access or Should have inbuilt feature like SSO for atleast two admin firewall users.	Request change.	Duplicate-Refer Response at Cons. S. No 73
194	VENDOR-9	15	76	2. Firewall / Performance & Scalability / SN 28	The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, University should have visibility of all its external facing servers/applications/IP addresses directly exposed to internet so that appropriate action can be taken on the application/network/firewall to mitigate misconfiguration and vulnerability of assets.	The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, NIXI should have visibility of all its external facing servers/applications/IP addresses directly exposed to internet so that appropriate action can be taken on the application/network/firewall to mitigate misconfiguration and vulnerability of assets.	NIXI is not a university but an etnerprise customer, pls pls remove the word University from the specification.	Duplicate-Refer Response at Cons. S. No 74
195	VENDOR-9	16	76	2. Firewall / Performance & Scalability / SN 29	The solution must have service which scans for university's credential leaked in the dark web and report to stake holders.	Delete	Pls delete this clause.	Duplicate-Refer Response at Cons. S. No 75
196	VENDOR-9	17	76	2. Firewall / Performance & Scalability / SN 30	Firewall should support Active/Standby and Active/Active failover and should not be based on stacking units in clustering	Firewall should support Active/Standby or Active/Active failover and should not be based on stacking units in clustering	Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change.	Duplicate-Refer Response at Cons. S. No 76
197	VENDOR-9	18	76	2. Firewall / Performance & Scalability / SN 35	Should have the IPS capability to inspect SSL traffic and SSL throughput of 9 Gbps.	Should have the IPS capability to inspect SSL traffic and SSL throughput of 5 Gbps.	Request change.	Duplicate-Refer Response at Cons. S. No 77
198	VENDOR-9	19	76	2. Firewall / Performance & Scalability / SN 42	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance	300 secs update is very specific to one OEM, hence request to remove.	Duplicate-Refer Response at Cons. S. No 78
199	VENDOR-9	20	76	2. Firewall / Performance & Scalability / SN 44	Should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 75 categories from day one.	Should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 55 categories from day one.	Inspection of 50+ categories should be enough for and URL Filtering requirement. Hence request change.	Duplicate-Refer Response at Cons. S. No 79
200	VENDOR-9	21	77	2. Firewall / Performance & Scalability / SN 50	Web Application Firewall Protection	Delete	The requirement is for a firewall and not a WAF, hence request change.	Duplicate-Refer Response at Cons. S. No 80
201	VENDOR-9	22	77	2. Firewall / Performance & Scalability / SN 51	Proposed appliance should have in-build WAF with Reverse proxy support,	Delete	This is a WAF feature and hence pls delete this clause.	Duplicate-Refer Response at Cons. S. No 81
202	VENDOR-9	23	77	2. Firewall / Performance & Scalability / SN 52	SQL injection protection, Cross-site scripting protection, HTTPS (TLS/SSL) encryption offloading.	SQL injection protection, Cross-site scripting protection, HTTPS (TLS/SSL) encryption offloading / decryption.	Request change as the requirement is not for a WAF but a firewall.	Duplicate-Refer Response at Cons. S. No 82
203	VENDOR-9	24	77	2. Firewall / Performance & Scalability / SN 53	Server security	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
204	VENDOR-9	25	77	2. Firewall / Performance & Scalability / SN 54	Solution must protect against ransomware and exploit and able to able to capture Viruses, Trojans, Worms, Spyware and Malware, Adware and PUA from single agent.The solution should able to integrate with on-premise sandbox appliance for zero day malware inspection.	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
205	VENDOR-9	26	77	2. Firewall / Performance & Scalability / SN 55	The Server Security Solution Should Support Multi-Platform operating system (Windows,Linux) and the same should be managed from a single Centralised Management console	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
206	VENDOR-9	27	77	2. Firewall / Performance & Scalability / SN 56	Server Security and Firewall should share the threat telemetry with each other, If both the solution are not from the same OEM it Should has open API option to integrate 3rd Party solution	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
207	VENDOR-9	28	77	2. Firewall / Performance & Scalability / SN 57	Solution must offer vulnerability management to verify servers	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
208	VENDOR-9	29	77	2. Firewall / Performance & Scalability / SN 59	Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware.	Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM-aware or memory based malware and protect from virtual sandbox evading advance unknown malware.	On-Premise sandbox has different advanced technologies for OEM to OEM, hence request change.	Duplicate-Refer Response at Cons. S. No 88
209	VENDOR-9	30	77	2. Firewall / Performance & Scalability / SN 59	Solution should support OS type - Windows 10, Windows 8.1, Windows 7, Linux, Android.	Solution should support OS type - Windows 7 (32 / 64 bit), Linux 64	Request change as VMs in a on prem sandbox appliance vary from OEM to OEM.	Duplicate-Refer Response at Cons. S. No 89
210	VENDOR-9	31	77	2. Firewall / Performance & Scalability / SN 61	Local malware analysis appliance should be of same OEM with 4x 1GE RJ45 interface and minimum throughput of 500 files/hour process across 6VMs or more. All VMs should be included from day 1	Local malware analysis appliance should be of same OEM with 4x 1GE RJ45 interface and minimum throughput of 500 files/hour process across 6VMs or any other memory based technique.	Request change as VMs in a on prem sandbox appliance vary from OEM to OEM.	Duplicate-Refer Response at Cons. S. No 90

RESPONSES TO THE QUERIES RECEIVED AGAINST TENDER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023

211	VENDOR-9	32	77	2. Firewall / Performance & Scalability / SN 62	Solution should have feature to manually configure on what file types will run in which specific VM for optimal performance.	Solution should have feature to manually configure on what file types will run in which specific VM for optimal performance or should have memeory based inspection techniques	Request change as VMs in a on prem sandbox appliance vary from OEM to OEM.	Duplicate-Refer Response at Cons. S. No 91
212	VENDOR-9	33	77	2. Firewall / Performance & Scalability / SN 71	Solution should have orchestrate, automate incident and response module for SOC operation with at least 2 user licenses from day 1.	Delete	Pls delete this clause, as this is not relevant in this specification.	Duplicate-Refer Response at Cons. S. No 92
213	**VENDOR**	**Sr. No.**	**Page Number**	**Section**	**Original Content in RFQ**	**Change sought/ Clarification**	**Remarks**	**CCA/NIXI Response**
214	VENDOR-10	1	75	2. Firewall / SN 2	Firewall appliance should be supplied with at least 4 x 1GE RJ-45 (expandable to total 8 ports) interfaces, 4 x 1G SFP slots (expandable to total 8 ports), 2 x10G SFP+ (expandable to total 8 ports). Solution should include all transceivers of populated modules (4x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports from day 1.	Firewall appliance should be supplied with at least 16 x 1GE RJ-45 6 x 10G/1G SFP+ ports. Solution should include all transceivers of populated modules (16x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports (MMF) from day 1.	The interface requirement of expansion modules is specific to OEM, hence request to change the expansion modules to fixed port from day 1.	Duplicate-Refer Response at Cons. S. No 60
215	VENDOR-10	2	75	2. Firewall / SN 2	Each appliance should have local available storage of 200 GB SSD after 1+1 RAID.	Each appliance should have local available storage of 1 TB SSD in-built in the firewall from day 1..	NIXI should have min 1 TB storage in-built in the firewall for storing config data and logs in case of management server failure.	Duplicate-Refer Response at Cons. S. No 61
216	VENDOR-10	3	75	2. Firewall / SN 6	Should support Active:Active & Active:Passive modes	Should support Active:Active / Active:Passive modes	Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change.	Duplicate-Refer Response at Cons. S. No 62
217	VENDOR-10	4	75	2. Firewall / Performance & Scalability / SN 7	Firewall Throughput: Minimum 10 Gbps or higher throughput on 64 byte packets. Performance should not degrade while IPv6 is enabled in future.(F)	Firewall Throughput: Minimum 9 Gbps or higher throughput on 64 byte packets as per RFC 2544 .	Request to change as per RFC 2544 the Firewall throughput for 64 byte packets.	Duplicate-Refer Response at Cons. S. No 63
218	VENDOR-10	5	75	2. Firewall / Performance & Scalability / SN 10	Firewall should support at least 8 million concurrent sessions	Firewall should support at least 4 million concurrent sessions	8 million concurrent connection is on a very highrer side for a 10 Gbps Firewall, hence request to reduce to 4 million.	Duplicate-Refer Response at Cons. S. No. 64
219	VENDOR-10	6	75	2. Firewall / Performance & Scalability / SN 11	Firewall should support at least 500K sessions per second	Firewall should support at least 110K sessions / connections per second	500K sessions/connections per secong is also a huge number for a 10 Gbps throughput firewall, hence request to reduce to 110K.	Duplicate-Refer Response at Cons. S. No. 65
220	VENDOR-10	7	75	2. Firewall / Performance & Scalability / SN 12	Firewall should support at least 1000 VLANs	Firewall should support at least 500 VLANs	In any enterprise network requirement of 1000 VLANs is a huge ask, and we think that 500 + VLANs should be sufficient to meet the current requirement of NIXI.	Duplicate-Refer Response at Cons. S. No 66
221	VENDOR-10	8	75	2. Firewall / Performance & Scalability / SN 14	Firewall should provide application detection for DNS, FTP, HTTP, SMTP, ESMTP, LDAP, RTSP, SIP, SQLNET, H.323, SNMP	Firewall should provide application detection for DNS, FTP, HTTP, SMTP, LDAP, RTSP, SIP, SQLNET, H.323, SNMP	Pls remove ESMTP as this is a email protocol and this is not the requirement in the current scenario of NIXI, as NIXI has separate email security solution.	Duplicate-Refer Response at Cons. S. No 67
222	VENDOR-10	9	75	2. Firewall / Performance & Scalability / SN 17	Should support Static, RIP, OSPF, OSPFv3 and BGP	Should support Static, RIP, OSPF/OSPFv3 and BGP	The requirement is for a firewall and not a Router, so the dynamic routing protocols shall be handled by the router/L3 switch. Request change.	Duplicate-Refer Response at Cons. S. No 68
223	VENDOR-10	10	75	2. Firewall / Performance & Scalability / SN 19	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4- to-IPv6) functionality or firewall should be capable of supporting dual stack.	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) / Nat46 (IPv4- to-IPv6) functionality or firewall should be capable of supporting dual stack.	Request change.	Duplicate-Refer Response at Cons. S. No 69
224	VENDOR-10	11	75	2. Firewall / Performance & Scalability / SN 24	Should be supplied with 1000 SSL VPN users license	Should support 1000 SSL VPN licenses and should be supplied with 10 active SSL VON licenses from day 1.	Knowing the requirement of NIXI, 1000 SSL VPN license is a very high ask and is biased to one OEM. Hence request change.	Duplicate-Refer Response at Cons. S. No 70
225	VENDOR-10	12	75	2. Firewall / Performance & Scalability / SN 25	Ability to configure, manage and monitor NGFW using CLI and GUI both without central management solution. University would like to have full feature parity of centralized management tool on the Next Generation Firewall itself, in case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool.	Ability to configure, manage and monitor NGFW using CLI / GUI with / without central management solution. NIXI would like to have full feature parity with centralized management to manage the Next Generation Firewall. In case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool then firewall should have basic management.	Since there are 9 firewalls so its imperative to have a management tool and analytics software for managing the firewalls. This would also ensure smooth management for the Admins. So, asking the firewall to have a self management is biased towards OEM, as every OEM have different mechanism to manage one or multiple or 100s of firewalls.	Duplicate-Refer Response at Cons. S. No 71
226	VENDOR-10	13	76	2. Firewall / Performance & Scalability / SN 26	The proposed firewall should be included with a solution to monitor and alert about the health of servers in the university like CPU, memory, disk, performance metrics etc. The solution should monitor at-least 20 servers and should be of same OEM for tight integration with firewall.	The proposed firewall should be included with a solution to monitor and alert about the health of servers at NIXI like CPU, memory, disk, performance metrics etc. The solution should monitor at-least 10 firewalls and the management tool should be of same OEM for tight integration with firewall.	NIXI is not a university but an etnerprise customer, pls pls remove the word University from the specification. Also the proposed solution should have management tool which should manage atleast 10 firewalls as per the requirement and not the servers. Hence request change.	Duplicate-Refer Response at Cons. S. No 72
227	VENDOR-10	14	76	2. Firewall / Performance & Scalability / SN 27	Should have inbuilt feature for two factor authentication via OTP (email or mobile) for atleast two admin users access.	Should have inbuilt feature for two factor authentication via OTP (email or mobile) for atleast two admin users access or Should have inbuilt feature like SSO for atleast two admin firewall users.	Request change.	Duplicate-Refer Response at Cons. S. No 73
228	VENDOR-10	15	76	2. Firewall / Performance & Scalability / SN 28	The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, University should have visibility of all its external facing servers/applications/IP addresses directly exposed to internet so that appropriate action can be taken on the application/network/firewall to mitigate misconfiguration and vulnerability of assets.	The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, NIXI should have visibility of all its external facing servers/applications/IP addresses directly exposed to internet so that appropriate action can be taken on the application/network/firewall to mitigate misconfiguration and vulnerability of assets.	NIXI is not a university but an etnerprise customer, pls pls remove the word University from the specification.	Duplicate-Refer Response at Cons. S. No 74
229	VENDOR-10	16	76	2. Firewall / Performance & Scalability / SN 29	The solution must have service which scans for university's credential leaked in the dark web and report to stake holders.	Delete	Pls delete this clause.	Duplicate-Refer Response at Cons. S. No 75
230	VENDOR-10	17	76	2. Firewall / Performance & Scalability / SN 30	Firewall should support Active/Standby and Active/Active failover and should not be based on stacking units in clustering	Firewall should support Active/Standby or Active/Active failover and should not be based on stacking units in clustering	Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change.	Duplicate-Refer Response at Cons. S. No 76
231	VENDOR-10	18	76	2. Firewall / Performance & Scalability / SN 35	Should have the IPS capability to inspect SSL traffic and SSL throughput of 9 Gbps.	Should have the IPS capability to inspect SSL traffic and SSL throughput of 5 Gbps.	Request change.	Duplicate-Refer Response at Cons. S. No 77
232	VENDOR-10	19	76	2. Firewall / Performance & Scalability / SN 42	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance	300 secs update is very specific to one OEM, hence request to remove.	Duplicate-Refer Response at Cons. S. No 78
233	VENDOR-10	20	76	2. Firewall / Performance & Scalability / SN 44	Should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 75 categories from day one.	Should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 55 categories from day one.	Inspection of 50+ categories should be enough for and URL Filtering requirement. Hence request change.	Duplicate-Refer Response at Cons. S. No 79
234	VENDOR-10	21	77	2. Firewall / Performance & Scalability / SN 50	Web Application Firewall Protection	Delete	The requirement is for a firewall and not a WAF, hence request change.	Duplicate-Refer Response at Cons. S. No 80
235	VENDOR-10	22	77	2. Firewall / Performance & Scalability / SN 51	Proposed appliance should have in-build WAF with Reverse proxy support,	Delete	This is a WAF feature and hence pls delete this clause.	Duplicate-Refer Response at Cons. S. No 81
236	VENDOR-10	23	77	2. Firewall / Performance & Scalability / SN 52	SQL injection protection, Cross-site scripting protection, HTTPS (TLS/SSL) encryption offloading.	SQL injection protection, Cross-site scripting protection, HTTPS (TLS/SSL) encryption offloading / decryption.	Request change as the requirement is not for a WAF but a firewall.	Duplicate-Refer Response at Cons. S. No 82
237	VENDOR-10	24	77	2. Firewall / Performance & Scalability / SN 53	Server security	Delete		Duplicate-Refer Response at Cons. S. No 19

RESPONSES TO THE QUERIES RECEIVED AGAINST TENDER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023

238	VENDOR-10	25	77	2. Firewall / Performance & Scalability / SN 54	Solution must protect against ransomware and exploit and able to able to capture Viruses, Trojans, Worms, Spyware and Malware, Adware and PUA from single agent.The solution should able to integrate with on-premise sandbox appliance for zero day malware insoection.	Delete	Server security is a separate solution and is not part of firewall solution. Hence request to remove the server security clauses.	Duplicate-Refer Response at Cons. S. No 19
239	VENDOR-10	26	77	2. Firewall / Performance & Scalability / SN 55	The Server Security Solution Should Support Multi-Platform operating system (Windows,Linux) and the same should be managed from a single Centralised Management console	Delete		Duplicate-Refer Response at Cons. S. No 19
240	VENDOR-10	27	77	2. Firewall / Performance & Scalability / SN 56	Server Security and Firewall should share the threat telemetry with each other, If both the solution are not from the same OEM it Should has open API option to integrate 3rd Party solution	Delete		Duplicate-Refer Response at Cons. S. No 19
241	VENDOR-10	28	77	2. Firewall / Performance & Scalability / SN 57	Solution must offer vulnerability management to verify servers	Delete		Duplicate-Refer Response at Cons. S. No 19
242	VENDOR-10	29	77	2. Firewall / Performance & Scalability / SN 59	Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware.	Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM-aware or memory based malware and protect from virtual sandbox evading advance unknown malware.	On-Premise sandbox has different advanced technologies for OEM to OEM, hence request change.	Duplicate-Refer Response at Cons. S. No 88
243	VENDOR-10	30	77	2. Firewall / Performance & Scalability / SN 59	Solution should support OS type - Windows 10, Windows 8.1, Windows 7, Linux, Android.	Solution should support OS type - Windows 7 (32 / 64 bit), Linux 64	Request change as VMs in a on prem sandbox appliance vary from OEM to OEM.	Duplicate-Refer Response at Cons. S. No 89
244	VENDOR-10	31	77	2. Firewall / Performance & Scalability / SN 61	Local malware analysis appliance should be of same OEM with 4x 1GE RJ45 interface and minimum throughput of 500 files/hour process across 6VMs or more. All VMs should be included from day 1	Local malware analysis appliance should be of same OEM with 4x 1GE RJ45 interface and minimum throughput of 500 files/hour process across 6VMs or any other memory based technique.	Request change as VMs in a on prem sandbox appliance vary from OEM to OEM.	Duplicate-Refer Response at Cons. S. No 90
245	VENDOR-10	32	77	2. Firewall / Performance & Scalability / SN 62	Solution should have feature to manually configure on what file types will run in which specific VM for optimal performance.	Solution should have feature to manually configure on what file types will run in which specific VM for optimal performance or should have memeory based inspection techniques	Request change as VMs in a on prem sandbox appliance vary from OEM to OEM.	Duplicate-Refer Response at Cons. S. No 91
246	VENDOR-10	33	77	2. Firewall / Performance & Scalability / SN 71	Solution should have orchestrate, automate incident and response module for SOC operation with at least 2 user licenses from day 1.	Delete	Pls delete this clause, as this is not relevant in this specification.	Duplicate-Refer Response at Cons. S. No 92
247	**VENDOR**	**S.No.**	**Page No**	**Point No**		**Specification**	**Changes Request**	**CCA/NIXI Response**
248	VENDOR-11	1	22 of 32	2		Firewall appliance should be supplied with at least 4 x 1GE RJ-45 (expandable to total 8 ports) interfaces, 4 x 1G SFP slots (expandable to total 8 ports), 2 x10G SFP+ (expandable to total 8 ports). Solution should include all transceivers of populated modules (4xIGb RJ- 45, 4x1G SFP, 2x10G SFP+) for fibre ports from day 1.Each appliance should have local available storage of 200 GB SSD after 1+1 RAID.	Firewall appliance should be supplied with at least 16 x 1GE RJ-45 interfaces with 3 x10G SFP+ ports. Solution should have 2 USB 3.0, 1 Console, 1 Mgmt. porti and should include all transceivers populated modules on fibre ports from day 1. Firewall appliance should have local available storage of 256 GB SSD.	Clause should be read as "Firewall appliance should be supplied with at least 4 x 1GE RJ-45 (expandable to total 8 ports) interfaces, 4 x 1G SFP slots (expandable to total 8 ports), 2 x10G SFP+ (expandable to total 4 ports). Solution should include all transceivers of populated modules (4x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports from day 1." "Each appliance should have local available storage of 200 GB SSD."
249	VENDOR-11	2	22 of 32	7		Firewall Throughput: 50Gbps of throughput on 64 byte packets. Performance should not degrade while IPv6 is enabled in future.(F)	Firewall inspection throughput: 5Gbps	Incorrect specification/page is being referred.
250	VENDOR-11	3	22 of 32	8		IPS Throughput 12 Gbps	IPS Throughput: 3.3 Gbps	Incorrect specification/page is being referred.
251	VENDOR-11	4	22 of 32	9		NGFW Throughput: 9 Gbps	NGFW Throughput: 1.5 Gbps	Incorrect specification/page is being referred.
252	VENDOR-11	5	22 of 32	10		Threat Protection Throughput: 10 Gbps	Threat Protection Throughput: 3 Gbps	Incorrect specification/page is being referred.
253	VENDOR-11	6	22 of 32	11		Firewall should support at least 8 million concurrent sessions	Firewall should support at least 500,000 DPI Connections	Incorrect specification/page is being referred.
254	VENDOR-11	7	22 of 32	12		Firewall should support at least 55K New sessions per second	Firewall should support at least 21,000 Connections per second	Incorrect specification/page is being referred.
255	VENDOR-11	8	22 of 32	13		Firewall should support at least 1000 VLANs	Firewall should support at least 255 Logical VLAN	Incorrect specification/page is being referred.
256	VENDOR-11	9	22 of 32	14		Firewall should support at least 50 Gbps of IPSEC VPN throughput	Firewall should support at least 2.1 Gbps of IPSEC VPN throughput	Incorrect specification/page is being referred.
257	VENDOR-11	10	23 of 32	25		Should be supplied with 1000 SSL VPN users	Firewall should support 500 SSL VPN users.	Incorrect specification/page is being referred.
258	VENDOR-11	11	23 of 32	26		Ability to configure, manage and monitor NGFW using CLI and GUI both without central management solution. University would like to have full feature parity of centralized management tool on the Next Generation Firewall itself, in case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool The proposed firewall should be included with a solution to monitor and alert about the health of servers in the university like CPU, memory, disk, performance metrics etc. The solution should monitor at-least 20 servers and should be of same OEM for tight integration with firewall.	Firewall should have the ability to configure, manage and monitor NGFW using CLI and GUI both without central management solution. Institution would like to have feature parity of centralized management tool on the Next Generation Firewall itself. In case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool. The proposed firewall should be included with a solution to monitor and alert about the health firewalls in the Institution like CPU, memory, disk, performance metrics etc. The solution should able to monitor at-least 10 firewalls and should be of same OEM for tight integration with firewall.	Incorrect specification/page is being referred.
259	VENDOR-11	12	23 of 32	27		Should have inbuilt feature for two factor authentication via OTP (email or mobile) for atleast two admin users access.	Should have inbuilt feature like SSO for atleast two admin firewall users.	Incorrect specification/page is being referred.
260	VENDOR-11	13	23 of 32	28		The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, University should have visibility of all its external facing servers/applications/IP addresses directly exposed to internet so that appropriate action can be taken on the application/network/firewall to mitigate misconfiguration and vulnerability of assets	The proposed firewall should be able to monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, Institution should have visibility of all its external facing servers / Applications / IP's directly exposed to internet so that appropriate action can be taken on the Application / Network Firewall to mitigate the issues.	Incorrect specification/page is being referred.
261	VENDOR-11	14	23 of 32	29		The solution must have service which scans for university's credential leaked in the dark web and report to stake holders	The proposed firewall OEM should have facility or have service which scans for Institution credential leaked in the dark web.	Incorrect specification/page is being referred.
262	VENDOR-11	15	23 of 32	35		Should have the IPS capability to inspect SSL traffic and SSL throughput of 9 Gbps.	Should have the IPS capability to inspect SSL traffic and SSL throughput of 800 Mbps.	Incorrect specification/page is being referred.
263	VENDOR-11	16	24 of 32	51		I Proposed appliance should have in-build WAF with Reverse proxy support,	Request to remove (WAF Features)	Incorrect specification/page is being referred.
264	VENDOR-11	17	24 of 32	52		SQL injection protection, Cross-site scripting protection, HTTPS (TLS/SSL) encryption offloading.	Request to remove (WAF Features)	Incorrect specification/page is being referred.
265	**VENDOR**	**S. No**	**RFP Reference Page**		**RFP Reference Section**	**Content of RFP requiring clarification**	**Points of clarification required**	**CCA/NIXI Response**
266	VENDOR-12	1	1		E. Suggested Specifications: 1. Load Balancer	The Load Balancer shall deliver the high availability required by modern data centres. It should support Active/Passive or Active / Active HA configurations. The Load Balancer shall automatically synchronize configurations between the pair and automatically failover if any fault is detected with the primary unit	As per our experience from the Industry, VRRP is the industry standard and widely used protocol for high availability. Based on our understanding from the Clause, proposed solution should not use Proprietary protocol for high Availability. Kindly Confirm. **Suggested Clause :** **The Load Balancer shall deliver the high availability required by modern data centres. It should support Active/Passive or Active / Active HA configurations. The Load Balancer shall automatically synchronize configurations in real time between the pairs. The proposed device should use standard VRRP (RFC - 2338) for High Availability purpose (no proprietary protocol).**	No change.
267	VENDOR-12	2	2		E. Suggested Specifications: 1. Load Balancer	Most applications use cookies or hidden, read-only parameters for application session state and other sensitive information. The Load Balancer shall encrypt or sign these tokens to prevent third party impersonation attacks	Specification clearly mentioned that the requirement is of Load Balancer. The feature asked in this Clause is relevant for Web application Firewall NOT for a Load Balancer appliance. However, Load balancer can be used to insert or rewrite cookie parameters. Hence, we request you amend this clause: **Suggested Clause :** **Most applications use cookies, session IDs for application session state. The Load Balancer shall be able to insert cookie from LB or rewrite the cookie in the response.**	No change
268	VENDOR-12	3	3		E. Suggested Specifications: 1. Load Balancer	The server load balancer should deliver at least 10 Gbps or higher of layer 7 throughput	The Sizing parameter is not inclined with other parameter such as SSL throughput and SSL CPS. Hence we request to amend this clause. **Suggested Clause:** **The server load balancer should deliver at least 30 Gbps or higher of layer 4/7 throughput and should be scalable to 60 Gbps.**	No change.

RESPONSES TO THE QUERIES RECEIVED AGAINST TENDER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023

269	VENDOR-12	4	4		E. Suggested Specifications: 1. Load Balancer	The server load balancer should deliver atleast 10 Gbps or higher of SSL throughput on 4096 key	As per industry standard, SSL Sizing is done of 2K key NOT the 4k Key size **Suggested Clause:** **The server load balancer should deliver atleast 20 Gbps or higher of SSL throughput on 2048 key.**	Duplicate-Refer Response at Cons. S. No 7
270	VENDOR-12	5	5		E. Suggested Specifications: 1. Load Balancer	The server load balancer should cater up to at least 40K or higher SSL connections per second on 2K key from day 1	ECC is the latest cipher suite used in most the application. ECC allows to provide same or higher level of Security with a much smaller key size as compared to RSA. Hence, we request to include the same. **Suggested Clause :** **The server load balancer should cater up to at least 50 K or higher SSL connections per second on 2K key and 25 K CPS on ECC from day 1**	Duplicate-Refer Response at Cons. S. No 8
271	VENDOR-12	6	6		E. Suggested Specifications: 1. Load Balancer	The sever load balancer should be proposed with 8 Ports populated with 4x1GE, 4x1G SFP ports and atleast 8 x 10G SFP+ SR ports from day 1	As per our experience, some of the vendor just to comply the clause propose break out cable functionality (for eg. 1 x 40G can be converted to 4x10G) to support number of ports requirements. Additionally, solution should have redundant out of band management port and dedicated console port of configuration and management. **Suggested Clause :** **The sever load balancer should be proposed with 8 Ports populated with 8 x1GE, 8 x 1G SFP ports and atleast 8 x 10G SFP+ SR ports from day 1 (without BreakOut Cable support)** **The proposed appliance should have 2 x 1G dedicated management port and 1 RJ45 Serial port.**	No change
272	VENDOR-12	7	7		E. Suggested Specifications: 1. Load Balancer	New Clause Request	Propose appliance should support next generation features like Virtualization that can virtualizes the device resources—including CPU, memory, network, acceleration resources, operating system, management to provide complete separate environment from applications and management perspective. **Suggested Clause :** **The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources.** **The Hypervisor used to virtualize the hardware should be a specialized purpose build hypervisor and NOT a commercially available hypervisor (like XEN, VMware,KVM etc.). (Public Available Reference link should be shared)** **Each Virtual Instance contains a complete and separated environment of the Following:** **a) Resources,** **b) Configurations,** **c) Management,** **d) Operating System** **The proposed device should support 5 Virtual Instance from Day 1 and support upto 30 Virtual Instances for future Scalability on the same hardware. Appliance should have capability to use in standalone as well as virtualized mode.**	No change
273	VENDOR-12	8	8		E. Suggested Specifications: 1. Load Balancer	New Clause Request	Minimum Eligibility Criteria should be mentioned to have a benchmark and healthy competition among the Industry Leading Solution. **Suggested Clause :** **1. OEM should have OEM TAC in INDIA. (since last 10 years)** **2. OEM/OEM subsidiary/OEM Sister Concern Company must have at least 5 successful implementation at INDIAN Government/BFSI/Telecom Organizations in last 3 years** **3. The proposed OEM should be Parent Technology OEM only (Should NOT be Whitelabled or Co-branding or 3rd Party Technology or Open Source or Reseller Agreement** **4. OEM must be Make in INDIA Class-1 compliant as per Government MII Guidelines & subsequent amendments.** **5. MII OEM (MSME) is exempted from OEM turnover and Number of year experience eligibility criteria.** **6. OEM/OEM subsidiary/OEM Sister concern Company should be present in INDIA for more than 15 years**	No change
274	**VENDOR**	**S.No.**	**Document Reference**		**Content of the RFP**	**Justification for change**	**Suggested Modification**	**CCA/NIXI Response**
275	VENDOR-13	1	Page 78; Minimum Technical Specification (HSM Module). S No 1		HSM should be network based appliance with inbuilt NIC support for 1 GB and 10 GB network .	Requested network stack mentioned in the RFP, includes capability of sending data both at 1G and 10G .10GbE connection are backward compatible to 1GBE but in order to reduce & remove network perfomance issues , devices should only communicate using either 1GB or 10GB interface at a given time .Thus HSMs will only be using either 1GBE or 10GBE interface . Also adding both options will lead to single vendor particiaprtion ,request you to make this generic .	HSM should be network based appliance with inbuilt NIC support for 1 GB or 10 GB network .	Duplicate-Refer Response at Cons. S. No 163
276	VENDOR-13	2	Page 79; Minimum Technical Specification (HSM Module). S No 4		Host Interface: Should have inbuilt Dual Gigabit Ethernet ports with port bonding and Dual 10G network port with port bonding. All four NICs should have IPv4 and IPv6 support. Capabilities should be from day 1	Requested network stack mentioned in the RFP, includes capability of sending data both at 1G and 10G .10GbE connection are backward compatible to 1GBE but in order to reduce & remove network perfomance issues , devices should only communicate using either 1GB or 10GB interface at a given time .Thus HSMs will only be using either 1GBE or 10GBE interface	Host Interface: Should have inbuilt Dual Gigabit Ethernet ports with port bonding or Dual 10G network port with port bonding. All four NICs should have IPv4 and IPv6 support. Capabilities should be from day 1	Duplicate-Refer Response at Cons. S. No 164
277	VENDOR-13	3	Page 78; Minimum Technical Specification (HSM Module). S No 21		Minimum Performance: RSA-2048:	In case of Hardware replacement or addition of new appliance to increase the TPS , Cost of additional hardware should be included by HSM OEM in BOM during initial stage as per organization's guidelines	Minimum Performance: RSA-2048: 500 TPS to a maximum of 1000 TPS	Minimum Performance: RSA-2048: 500 TPS or higher
278	VENDOR-13	4	Page 78; Minimum Technical Specification (HSM Module). S No 22		HSM should have capabilities to increase TPS on same appliance by applying license or upgrade package . In case of Hardware replacement or addition of new appliance to increase the TPS , Cost of additional hardware should be included by HSM OEM in BOM during initial stage as per organization's guidelines. OEM must provide Doom's Day service whenever needed by client at no additional cost	In order to include cost , please mention range with minimum and maximum values. Dooms Day service is OEM specific feature and would prevent participation. It essentially means the HSM has a backdoor for key extraction which can be done by the OEM.	HSM should have capabilities to increase TPS on same appliance by applying license or upgrade package . In case of Hardware replacement or addition of new appliance to increase the TPS , Cost of additional hardware should be included by HSM OEM in BOM during initial stage as per organization's guidelines. For this purpose a maximum increase of minimum TPS to 1000 must be considered.	This clause may be read as "HSM should have capabilities to increase TPS on same appliance by applying license or upgrade package . In case of Hardware replacement or addition of new appliance to increase the TPS (upto 1000), Cost of additional hardware should be included by HSM OEM in BOM during initial stage. OEM must provide emergency support of any nature (including extraction of keys from devices, if any) and transition to others systems whenever needed by client at no additional cost."
279	VENDOR-13	5	Page 78; Minimum Technical Specification (HSM Module). S No 11		HSM should be FIPS 140-2 Level 3 certified and certification should be in OEM Name. Certification Copy needs to be submitted	Please also include Common Criteria EAL4+ certification which ensures not only the hardware but also the software running inside the HSM has been certified as secure. This is also in line to the certifications asked in the tender for other solutions like CA Software, Digital Certificate Life Cycle Manager, OCSP Responder & the CC EAL4+ certification carries scores too as per the RFP.	HSM should be FIPS 140-2 Level 3 & Common Criteria EAL4+ certified and certification should be in OEM Name. Certification Copy needs to be submitted.	Duplicate-Refer Response at Cons. S. No 3
280	VENDOR-13	6	Page 78; Minimum Technical Specification (HSM Module). S No 13		HSM should have simulator capabilities to provide development , integration and Testing of applications in restricted network with no outside connectivity to internet .	Simulation is usually done within software. Secure HSM's do not support such features as it adds to vulnerability of the device with the potential of migrating keys from simulation software to HSM and vice versa. Recommend to remove this point as it would prevent participation in the RFP	Please remove this point.	Duplicate-Refer Response at Cons. S. No 4
281	**VENDOR-13**		**Features**		**Minimum Technical Specification**	**Justification**	**Recommended Text**	**CCA/NIXI Response**
282	VENDOR-13	7	Physical Characteristics		Should Support PCIe with external	Different OEM's use different things like tokens	Should Support Low profile PCIe card with external smart card / token with their own PIN or	Should Support PCIe card with external smart card /
283	VENDOR-13				smart card reader	instead of smartcards . Recommend to make this	Password for multifactor authentication	token
284	VENDOR-13	8	Host Connectivity		PCIe x4	PCIe X4 is just a slot in the Server. Recommend to set the PCI-E standard being used for the bus communication such as PCI-Express CEM 3.0, PCI, PCI Express Base 2.0	PCI-Express CEM 3.0, PCI, PCI Express Base 2.0	Duplicate-Refer Response at Cons. S. No 5
285	VENDOR-13	9	Key backup		Support for key backup in external storage media in encrypted form	If external storage media is not FIPS certified to the same level then that would mean the HSM supports key extraction into software.	Support for key backup in FIPS 140-2 Level 3 certified Backup device.	No change
286	VENDOR-13	10	Safety , Security and Environmental Compliance		FIPS 140-3 Level 3, NIST SP 800-131A with valid certification	Recommend including eIDAS CC EAL4+ certification as well to ensure associated accedition for digital signing use case.	FIPS 140-3 Level 3, NIST SP 800-131A and eIDAS CC EAL4+ with valid certification	Duplicate-Refer Response at Cons. S. No 171
287	**Vendor**	**S.No.**	**RFP Page**	**Section**	**Clause**	**Change required**	**Justification**	**CCA/NIXI Response**
288	VENDOR-14	1	80	6. Layer 3 Switch	4. General Requirements- The Ethernet switch being proposed must be a Secure Access switches deliver a Secure, Simple, Scalable Ethernet solution with outstanding security, performance and manageability for threat	Please remove the clause	This is a OEM specific feature and is blocking other OEMs to participate. So, kindly remove for wider OEM participation.	No Change

RESPONSES TO THE QUERIES RECEIVED AGAINST TENDER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023

289	VENDOR-14	2	81	6. Layer 3 Switch	9. Authentication Requirements- Switch should support DHCP snooping IPv4 / IPv6, IP source guard, IP sourceguard violation log, Dynamic ARP inspection, IPv6 RA guard, IGMP snooping/proxy/querier, VLAN stacking (QnQ) , MCLAG, QoS marking (IPv4/IPv6), Should have management protocol that allows NGFW Security Appliance to seamlessly manage any Ethernet Switch	Switch should support DHCP snooping IPv4 / IPv6, IP source guard, IP sourceguard violation log**/counters**, Dynamic ARP inspection **or equivalent feature,** IPv6 RA guard **or equivalent feature**, IGMP snooping/proxy/querier, VLAN stacking (QnQ) , MCLAG, QoS marking (IPv4/IPv6), ~~**Should have management protocol that allows NGFW Security Appliance to seamlessly manage any Ethernet Switch**~~	Different OEMs have different ways of implementing same feature. Please add equivalent option with the feature request. The management protocol asked is an OEM specific feature and is blocking other OEMs to participate. So, kindly remove for wider OEM participation.	Clause should be read as Authentication Requirements- Switch should support DHCP snooping IPv4 / IPv6, IP source guard, IP sourceguard violation log, Dynamic ARP inspection, IPv6 RA guard, IGMP snooping/proxy/querier, VLAN stacking (QnQ) , MCLAG, QoS marking (IPv4/IPv6), should have single pane of management via NGFW or through separate management tool along with required hardware to manage the proposed ethernet switches.
290	VENDOR-14	3	81	6. Layer 3 Switch	10. Authentication Requirements- Should support IEEE 802.1AX Link Aggregation, IEEE 802.1q VLAN tagging, LLDP/MED	Should support IEEE 802.1AX/**802.3ad** Link Aggregation, IEEE 802.1q VLAN tagging, LLDP/MED	As there is no functional difference between 802.1ax and 802.3ad please add it for wider OEM participation.	Clause may be read as "Should support IEEE 802.1AX/802.3ad Link Aggregation, IEEE 802.1q VLAN tagging, LLDP/MED"
291	VENDOR-14	4	81	6. Layer 3 Switch	11. Authentication Requirements- Switch should prevent direct client-to-client traffic visibility at the layer-2 VLAN.	Please remove the clause	This is a OEM specific feature and is blocking other OEMs to participate. So, kindly remove for wider OEM participation.	No Change
292	VENDOR-14	5	81	6. Layer 3 Switch	20. Authentication Requirements- Switch should support Layer 3 Policy-based routing, OSPF (IPv4/IPv6), BFD for OSPF (IPv4/IPv6), RIP (IPv4/IPv6), BFD for RIP (IPv4/IPv6) ,VRRP (IPv4/IPv6), BGP (IPv4/IPv6) , IS-IS (IPv4/IPv6) , BFD for IS-IS (IPv4/IPv6)	Switch should support Layer 3 Policy-based routing, OSPF (IPv4/IPv6), BFD for OSPF (IPv4/IPv6), ~~**RIP (IPv4/IPv6), BFD for RIP (IPv4/IPv6)**~~ ,VRRP (IPv4/IPv6), BGP (IPv4/IPv6) , IS-IS (IPv4/IPv6) , BFD for IS-IS (IPv4/IPv6)	As RIP is legacy protocol & obsolete today and also nt asked in router, please remove it for wider OEM participation.	No Change
293	VENDOR-14	6	82	6. Layer 3 Switch	31. Management - Switch must have option to ping using Switch serial number instead of the Switch IP address.	Please remove the clause	This is a OEM specific feature and is blocking other OEMs to participate. So, kindly remove for wider OEM participation.	Deleted
294	VENDOR-14	7	82	6. Layer 3 Switch	32. Management -Switch should support in-built network access control feature to bounce all the devices by default in onboarding VLAN. And Based on the devices matching with the specified criteria devices should be assigned to a specific VLAN. Criteria: a.MAC address, b. hardware vendor, c. device family, d. device type, e. device operating system and user group. If bidder not supported in-built they should include all the required hardware and software resources	Please remove the clause	This is a OEM specific feature and is blocking other OEMs to participate. Also, this is a campus feature not required in DC switch. So, kindly remove for wider OEM participation.	Deleted
295	VENDOR-14	8	82	6. Layer 3 Switch	33. Management -Switch should have option to allow administrators to quarantine hosts and users connected to a Switch via GUI. Quarantined MAC addresses should be isolated from the rest of the network and LAN.	Please remove the clause	This is a OEM specific feature and is blocking other OEMs to participate. Also, this is a campus feature not required in DC switch. So, kindly remove for wider OEM participation.	Clause can be read as Management -Switch should have option to allow administrators to quarantine hosts and users connected to a Switch via GUI. Quarantined MAC addresses should be isolated from the rest of the network and LAN. In case, any OEM don't have inbuilt functionality on their switch, they can provide additional required software and hardware to meet the technical requirement
296	VENDOR-14	9	82	6. Layer 3 Switch	36. Environment - Operating Temperature : 0–45°C, Storage temperature: -40–70°C, Humidity: 5–95% non-condensing	Operating Temperature : 0–~~45~~ **40**°C, Storage temperature: -40–70°C, Humidity: 5–95% non-condensing	40°C is more than sufficient for any enterprise environment and is industry wide standard. So, please change higher limit to 40C for wider participation.	Clause should be read as : "Environment - Operating Temperature : 0–40°C, Storage temperature: -40–70°C, Humidity: 5–95% non-condensing "
297	VENDOR-14	10	82	6. Layer 3 Switch	37. Certification - FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2	37. Certification - FCC, CE, RCM, VCCI, BSMI, UL, CB/RoHS2	Please change for wider OEM particiaption.	No Change
298	VENDOR-14	11	77	2. Firewall	59. Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware.	These specification is specific to OEM. Not all Firewall OEMs have zero day threat protection appliance. Some OEMs provide this protection in the cloud also. We would request yourself to create a separate section for zero day protection. This will not only provide extended zeroday protection coverage but also prevent vendor lockin or you can also allow cloud based zero day protection.		Duplicate-Refer Response at Cons. S. No 88
299	VENDOR-14	12	77	2. Firewall	60. Solution should support OS type Windows 10, Windows 8.1, Windows 7, Linux, Android			Duplicate-Refer Response at Cons. S. No 89
300	VENDOR-14	13	77	2. Firewall	61. Local malware analysis appliance should be of same OEM with 4x 1GE RJ45 interface and minimum throughput of 500 files/hour process across 6VMs or more. All VMs should be included from day 1			Duplicate-Refer Response at Cons. S. No 90
301	VENDOR-14	14	77	2. Firewall	62. Solution should have feature to manually configure on what file types will run in which specific VM for optimal performance			Duplicate-Refer Response at Cons. S. No 91
302	VENDOR-14	15	77	2. Firewall	63. Local Malware appliance should have inbuilt feature to send alert over email of detected malware post analysis. For example, if malware has high risk, alert should be notified to security team for further analysis if required.			No Change
303	VENDOR-14	16	77	2. Firewall	50 Web Application Firewall Protection	This is not part of network firewall. We would request to have a separate section for this requirement		Duplicate-Refer Response at Cons. S. No 80
304	VENDOR-14	17	77	2. Firewall	Zero Day threat protection	We understand that the bidder has to provide separate solution independent of Firewall.		Duplicate-Refer Response at Cons. S. No 88
305	VENDOR-14	18	76	2. Firewall	42 Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance	This is not functionality of Firewall but of Zero day threat protection. We would request you to either move it the said section or remove the clause		Duplicate-Refer Response at Cons. S. No 78
306	VENDOR-14	19	76	2. Firewall	29 The solution must have service which scans for university's credential leaked in the dark web and report to stake holders.	Not sure what "university" means here. Moreover, it this clause is not functionality of firewall. We request you to remove the clause.		Duplicate-Refer Response at Cons. S. No 75
307	VENDOR-14	20	76	2. Firewall	28 The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, University should have visibility of all its external facing servers/applications/IP addresses directly exposed to internet so that appropriate action can be taken on the application/network/firewall to mitigate misconfiguration and vulnerability of assets.	Not sure what "university" means here. Moreover, it this clause is not functionality of firewall. We request you to remove the clause.		Duplicate-Refer Response at Cons. S. No 74
308	VENDOR-14	21	76	2. Firewall	27 Should have inbuilt feature for two factor authentication via OTP (email or mobile) for atleast two admin users access.	Not all firewall OEMs provide two factor authentication, usually Firewalls use authentication methods like RADUIS, Active Directory etc. We request you to amend the clause to read "Additionally, external authentication and authorization servers should be integrated with any of these RADIUS, LDAP, LDAP Secure, or TACACS protocols. "		Duplicate-Refer Response at Cons. S. No 73

RESPONSES TO THE QUERIES RECEIVED AGAINST TENDER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023

309	VENDOR-14	22	76	2. Firewall	25 Ability to configure, manage and monitor NGFW using CLI and GUI both without central management solution. University would like to have full feature parity of centralized management tool on the Next Generation Firewall itself, in case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool	Seems OEM specific clause.Request you to amend the clause to " Ability to configure, manage and monitor NGFW using CLI and GUI both without central management solution.NIXI should have CLI, in case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool"		Duplicate-Refer Response at Cons. S. No 71
310	**Vendor**	**S. No**	**RFP Reference Page**	**RFP Reference S**	**Content of RFP requiring clarification**		**Points of clarification required**	**CCA/NIXI Response**
311	VENDOR-15	1	74	E. Suggested Specifications: 1. Load Balancer	The Load Balancer shall deliver the high availability required by modern data centres. It should support Active/Passive or Active / Active HA configurations. The Load Balancer shall automatically synchronize configurations between the pair and automatically failover if any fault is detected with the primary unit		As per our experience from the Industry, VRRP is the industry standard and widely used protocol for high availability. Based on our understanding from the Clause, proposed solution should not use Proprietary protocol for high Availability. Kindly Confirm. **Suggested Clause :** **The Load Balancer shall deliver the high availability required by modern data centres. It should support Active/Passive or Active / Active HA configurations. The Load Balancer shall automatically synchronize configurations in real time between the pairs. The proposed device should use standard VRRP (RFC - 2338) for High Availability purpose (no proprietary protocol).**	Duplicate-Refer Response at Cons. S. No 266
312	VENDOR-15	2	74	E. Suggested Specifications: 1. Load Balancer	Most applications use cookies or hidden, read-only parameters for application session state and other sensitive information. The Load Balancer shall encrypt or sign these tokens to prevent third party impersonation attacks		Specification clearly mentioned that the requirement is of Load Balancer. The feature asked in this Clause is relevant for Web application Firewall NOT for a Load Balancer appliance. However, Load balancer can be used to insert or rewrite cookie parameters. Hence, we request you amend this clause: **Suggested Clause :** **Most applications use cookies, session IDs for application session state. The Load Balancer shall be able to insert cookie from LB or rewrite the cookie in the response.**	Duplicate-Refer Response at Cons. S. No 267
313	VENDOR-15	3	74	E. Suggested Specifications: 1. Load Balancer	The server load balancer should deliver at least 10 Gbps or higher of layer 7 throughput		The Sizing parameter is not inclined with other parameter such as SSL throughput and SSL CPS. Hence we request to amend this clause. **Suggested Clause:** **The server load balancer should deliver at least 30 Gbps or higher of layer 4/7 throughput and should be scalable to 60 Gbps.**	Duplicate-Refer Response at Cons. S. No 268
314	VENDOR-15	4	74	E. Suggested Specifications: 1. Load Balancer	The server load balancer should deliver atleast 10 Gbps or higher of SSL throughput on 4096 key		As per industry standard, SSL Sizing is done of 2K key NOT the 4k Key size **Suggested Clause:** **The server load balancer should deliver atleast 20 Gbps or higher of SSL throughput on 2048 key.**	Duplicate-Refer Response at Cons. S. No 7
315	VENDOR-15	5	74	E. Suggested Specifications: 1. Load Balancer	The server load balancer should cater up to at least 40K or higher SSL connections per second on 2K key from day 1		ECC is the latest cipher suite used in most the application. ECC allows to provide same or higher level of Security with a much smaller key size as compared to RSA. Hence, we request to include the same. **Suggested Clause :** **The server load balancer should cater up to at least 50 K or higher SSL connections per second on 2K key and 25 K CPS on ECC from day 1**	Duplicate-Refer Response at Cons. S. No 8
316	VENDOR-15	6	74	E. Suggested Specifications: 1. Load Balancer	The sever load balancer should be proposed with 8 Ports populated with 4x1GE, 4x1G SFP ports and atleast 8 x 10G SFP+ SR ports from day 1		As per our experience, some of the vendor just to comply the clause propose break out cable functionality (for eg. 1 x 40G can be converted to 4x10G) to support number of ports requirements. Additionally, solution should have redundant out of band management port and dedicated console port of configuration and management. **Suggested Clause :** **The sever load balancer should be proposed with 8 Ports populated with 8 x1GE, 8 x 1G SFP ports and atleast 8 x 10G SFP+ SR ports from day 1 (without BreakOut Cable support)** **The proposed appliance should have 2 x 1G dedicated management port and 1 RJ45 Serial port.**	Duplicate-Refer Response at Cons. S. No 271
317	VENDOR-15	7	74	E. Suggested Specifications: 1. Load Balancer	New Clause Request		Propose appliance should support next generation features like Virtualization that can virtualizes the device resources—including CPU, memory, network, acceleration resources, operating system, management to provide complete separate environment from applications and management perspective. **Suggested Clause :** **The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources.** **The Hypervisor used to virtualize the hardware should be a specialized purpose build hypervisor and NOT a commercially available hypervisor (like XEN, VMware,KVM etc.). (Public Available Reference link should be shared)** **Each Virtual Instance contains a complete and separated environment of the Following:** **a) Resources,** **b) Configurations,** **c) Management,** **d) Operating System** **The proposed device should support 5 Virtual Instance from Day 1 and support upto 30 Virtual Instances for future Scalability on the same hardware. Appliance should have capability to use in standalone as well as virtualized mode.**	Duplicate-Refer Response at Cons. S. No 272
318	VENDOR-15	8	74	E. Suggested Specifications: 1. Load Balancer	New Clause Request		Minimum Eligibility Criteria should be mentioned to have a benchmark and healthy competition among the Industry Leading Solution. **Suggested Clause :** **1. OEM should have OEM TAC in INDIA. (since last 10 years)** **2. OEM/OEM subsidiary/OEM Sister Concern Company must have at least 5 successful implementation at INDIAN Government/BFSI/Telecom Organizations in last 3 years** **3. The proposed OEM should be Parent Technology OEM only (Should NOT be Whitelabled or Co-branding or 3rd Party Technology or Open Source or Reseller Agreement** **4. OEM must be Make in INDIA Class-1 compliant as per Government MII Guidelines & subsequent amendments.** **5. MII OEM (MSME) is exempted from OEM turnover and Number of year experience eligibility criteria.** **6. OEM/OEM subsidiary/OEM Sister concern Company should be present in INDIA for more than 15 years**	Duplicate-Refer Response at Cons. S. No 273
319	VENDOR-15	9		**New Solution Re**	**New Solution Request**		Cyber Security is very important aspect in the entire datacenter services. As per our industry experience, Solution should include DDoS Protection for Complete Infrastructure protection and the technical specification is missing in the RFP. We request to include the same, as the DDoS is the major component to protect against Network, Application and Server Floods/DDoS Attacks.	No Change
320	VENDOR-15	10		**New Solution Re**	**New Solution Request**		Cyber Security is very important aspect in the entire datacenter services. As per our industry experience, Solution should include Web Application Firewall for Web Application Protection and the technical specification is missing in the RFP. We request to include the same, as the WAF is the major component to protect against Application & DB attacks including API protection.	No Change.
321	VENDOR-15	11		**New Solution Re**	**New Solution Request**		Cyber Security is very important aspect in the entire datacenter services. As per our industry experience, Solution should include Intrusion Prevention System for Complete Network protection and the technical specification is missing in the RFP. We request to include the same, as the NIPS is the major component to protect against Network, Application, Server, Data centre Intrusion based attack prevention.	No Change
322	**Vendor**	**S. No**	**RFP Reference Page**	**RFP Reference S**	**Content of RFP requiring clarification**		**Points of clarification required**	**CCA/NIXI Response**
323	VENDOR-16	1	74	E. Suggested Specifications: 1. Load Balancer	The Load Balancer shall deliver the high availability required by modern data centres. It should support Active/Passive or Active / Active HA configurations. The Load Balancer shall automatically synchronize configurations between the pair and automatically failover if any fault is detected with the primary unit		As per our experience from the Industry, VRRP is the industry standard and widely used protocol for high availability. Based on our understanding from the Clause, proposed solution should not use Proprietary protocol for high Availability. Kindly Confirm. **Suggested Clause :** **The Load Balancer shall deliver the high availability required by modern data centres. It should support Active/Passive or Active / Active HA configurations. The Load Balancer shall automatically synchronize configurations in real time between the pairs. The proposed device should use standard VRRP (RFC - 2338) for High Availability purpose (no proprietary protocol).**	Duplicate-Refer Response at Cons. S. No 266
324	VENDOR-16	2	74	E. Suggested Specifications: 1. Load Balancer	Most applications use cookies or hidden, read-only parameters for application session state and other sensitive information. The Load Balancer shall encrypt or sign these tokens to prevent third party impersonation attacks		Specification clearly mentioned that the requirement is of Load Balancer. The feature asked in this Clause is relevant for Web application Firewall NOT for a Load Balancer appliance. However, Load balancer can be used to insert or rewrite cookie parameters. Hence, we request you amend this clause: **Suggested Clause :** **Most applications use cookies, session IDs for application session state. The Load Balancer shall be able to insert cookie from LB or rewrite the cookie in the response.**	Duplicate-Refer Response at Cons. S. No 267
325	VENDOR-16	3	74	E. Suggested Specifications: 1. Load Balancer	The server load balancer should deliver at least 10 Gbps or higher of layer 7 throughput		The Sizing parameter is not inclined with other parameter such as SSL throughput and SSL CPS. Hence we request to amend this clause. **Suggested Clause:** **The server load balancer should deliver at least 30 Gbps or higher of layer 4/7 throughput and should be scalable to 60 Gbps.**	Duplicate-Refer Response at Cons. S. No 268

RESPONSES TO THE QUERIES RECEIVED AGAINST TENDER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023

326	VENDOR-16	4	74	E. Suggested Specifications: 1. Load Balancer	The server load balancer should deliver atleast 10 Gbps or higher of SSL throughput on 4096 key		As per industry standard, SSL Sizing is done of 2K key NOT the 4k Key size **Suggested Clause:** **The server load balancer should deliver atleast 20 Gbps or higher of SSL throughput on 2048 key.**	Duplicate-Refer Response at Cons. S. No 7
327	VENDOR-16	5	74	E. Suggested Specifications: 1. Load Balancer	The server load balancer should cater up to at least 40K or higher SSL connections per second on 2K key from day 1		ECC is the latest cipher suite used in most the application. ECC allows to provide same or higher level of Security with a much smaller key size as compared to RSA. Hence, we request to include the same. **Suggested Clause :** **The server load balancer should cater up to at least 50 K or higher SSL connections per second on 2K key and 25 K CPS on ECC from dav 1**	Duplicate-Refer Response at Cons. S. No 8
328	VENDOR-16	6	74	E. Suggested Specifications: 1. Load Balancer	The sever load balancer should be proposed with 8 Ports populated with 4x1GE, 4x1G SFP ports and atleast 8 x 10G SFP+ SR ports from day 1		As per our experience, some of the vendor just to comply the clause propose break out cable functionality (for eg. 1 x 40G can be converted to 4x10G) to support number of ports requirements. Additionally, solution should have redundant out of band management port and dedicated console port of configuration and management. **Suggested Clause :** **The sever load balancer should be proposed with 8 Ports populated with 8 x1GE, 8 x 1G SFP ports and atleast 8 x 10G SFP+ SR ports from day 1 (without BreakOut Cable support)** **The proposed appliance should have 2 x 1G dedicated management port and 1 RJ45 Serial port.**	Duplicate-Refer Response at Cons. S. No 271
329	VENDOR-16	7	74	E. Suggested Specifications: 1. Load Balancer	New Clause Request		Propose appliance should support next generation features like Virtualization that can virtualizes the device resources—including CPU, memory, network, acceleration resources, operating system, management to provide complete separate environment from applications and management perspective. **Suggested Clause :** **The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources.** **The Hypervisor used to virtualize the hardware should be a specialized purpose build hypervisor and NOT a commercially available hypervisor (like XEN, VMware,KVM etc.). (Public Available Reference link should be shared)** **Each Virtual Instance contains a complete and separated environment of the Following:** **a) Resources,** **b) Configurations,** **c) Management,** **d) Operating System** **The proposed device should support 5 Virtual Instance from Day 1 and support upto 30 Virtual Instances for future Scalability on the same hardware. Appliance should have capability to use in standalone as well as virtualized mode.**	Duplicate-Refer Response at Cons. S. No 272
330	VENDOR-16	8	74	E. Suggested Specifications: 1. Load Balancer	New Clause Request		Minimum Eligibility Criteria should be mentioned to have a benchmark and healthy competition among the Industry Leading Solution. **Suggested Clause :** **1. OEM should have OEM TAC in INDIA. (since last 10 years)** **2. OEM/OEM subsidiary/OEM Sister Concern Company must have at least 5 successful implementation at INDIAN Government/BFSI/Telecom Organizations in last 3 years** **3. The proposed OEM should be Parent Technology OEM only (Should NOT be Whitelabled or Co-branding or 3rd Party Technology or Open Source or Reseller Agreement** **4. OEM must be Make in INDIA Class-1 compliant as per Government MII Guidelines & subsequent amendments.** **5. MII OEM (MSME) is exempted from OEM turnover and Number of year experience eligibility criteria.** **6. OEM/OEM subsidiary/OEM Sister concern Company should be present in INDIA for more than 15 years**	Duplicate-Refer Response at Cons. S. No 273
331	VENDOR-16	9		**New Solution Re**	**New Solution Request**		Cyber Security is very important aspect in the entire datacenter services. As per our industry experience, Solution should include DDoS Protection for Complete Infrastructure protection and the technical specification is missing in the RFP. We request to include the same, as the DDoS is the major component to protect against Network, Application and Server Floods/DDoS Attacks.	Duplicate-Refer Response at Cons. S. No 319
332	VENDOR-16	10		**New Solution Re**	**New Solution Request**		Cyber Security is very important aspect in the entire datacenter services. As per our industry experience, Solution should include Web Application Firewall for Web Application Protection and the technical specification is missing in the RFP. We request to include the same, as the WAF is the major component to protect against Application & DB attacks including API protection.	Duplicate-Refer Response at Cons. S. No 320
333	VENDOR-16	11		**New Solution Re**	**New Solution Request**		Cyber Security is very important aspect in the entire datacenter services. As per our industry experience, Solution should include Intrusion Prevention System for Complete Network protection and the technical specification is missing in the RFP. We request to include the same, as the NIPS is the major component to protect against Network, Application, Server, Data centre Intrusion based attack prevention.	Duplicate-Refer Response at Cons. S. No 321
334	**Vendor**	**Sno**	**Page No**	**Section**	**Clause**		**Clarification**	**CCA/NIXI Response**
335	VENDOR-17	1	77	2. Firewall	59. Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware.		These specification is specific to OEM. Not all Firewall OEMs have zero day threat protection appliance. Some OEMs provide this protection in the cloud also. We would request yourself to create a separate section for zero day protection. This will not only provide extended zeroday protection coverage but also prevent vendor lockin or you can also allow cloud based zero day protection.	No Change
336	VENDOR-17	2	77	2. Firewall	60. Solution should support OS type Windows 10, Windows 8.1, Windows 7, Linux, Android.			Duplicate-Refer Response at Cons. S. No 89
337	VENDOR-17	3	77	2. Firewall	61. Local malware analysis appliance should be of same OEM with 4x 1GE RJ45 interface and minimum throughput of 500 files/hour process across 6VMs or more. All VMs should be included from day 1			Duplicate-Refer Response at Cons. S. No 90
338	VENDOR-17	4	77	2. Firewall	62. Solution should have feature to manually configure on what file types will run in which specific VM for optimal performance.			Duplicate-Refer Response at Cons. S. No 91
339	VENDOR-17	5	77	2. Firewall	63. Local Malware appliance should have inbuilt feature to send alert over email of detected malware post analysis. For example, if malware has high risk, alert should be notified to security team for further analysis if required.			Duplicate-Refer Response at Cons. S. No 302
340	VENDOR-17	6	77	2. Firewall	50 Web Application Firewall Protection		This is not part of network firewall. We would request to have a separate section for this requirement	No Change
341	VENDOR-17	7	77	2. Firewall	Zero Day threat protection		We understand that the bidder has to provide separate solution independent of Firewall.	No Change
342	VENDOR-17	8	76	2. Firewall	42 Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance		This is not functionality of Firewall but of Zero day threat protection. We would request you to either move it the said section or remove the clause	Duplicate-Refer Response at Cons. S. No 78
343	VENDOR-17	9	76	2. Firewall	29 The solution must have service which scans for university's credential leaked in the dark web and report to stake holders.		Not sure what "university" means here. Moreover, it this clause is not functionality of firewall. We request you to remove the clause.	Duplicate-Refer Response at Cons. S. No 75
344	VENDOR-17	10	76	2. Firewall	28 The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, University should have visibility of all its external facing servers/applications/IP addresses directly exposed to internet so that appropriate action can be taken on the application/network/firewall to mitigate misconfiguration and vulnerability of assets.		Not sure what "university" means here. Moreover, it this clause is not functionality of firewall. We request you to remove the clause.	Duplicate-Refer Response at Cons. S. No 74
345	VENDOR-17	11	76	2. Firewall	27 Should have inbuilt feature for two factor authentication via OTP (email or mobile) for atleast two admin users access.		Not all firewall OEMs provide two factor authentication, usually Firewalls use authentication methods like RADUIS, Active Directory etc. We request you to amend the clause to read "Additionally, external authentication and authorization servers should be integrated with any of these RADIUS, LDAP, LDAP Secure, or TACACS protocols. "	Duplicate-Refer Response at Cons. S. No 73

RESPONSES TO THE QUERIES RECEIVED AGAINST TENDER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023

346	VENDOR-17	12	76	2. Firewall	25 Ability to configure, manage and monitor NGFW using CLI and GUI both without central management solution. University would like to have full feature parity of centralized management tool on the Next Generation Firewall itself, in case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool		Seems OEM specific clause.Request you to amend the clause to " Ability to configure, manage and monitor NGFW using CLI and GUI both without central management solution.NIXI should have CLI, in case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool"	Duplicate-Refer Response at Cons. S. No 71

*** End of Document ***