Cons. S. No.	VENDOP	Sr. No	RFP Page No	Ref. Point	RES RFP Clause	PONSES TO THE QUERIES RECEIVED AGAINST TENDI Description	ER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023 Comments	CCA/NIXI Response
1	VENDOR-1	1	79	incli i conte	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,	be part of the specification for HSW 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:	SN2 (532), SM3 and SM4 HSM should be FIPS 140-2 Level 3 certified and certification should be in OEM Name. Certification Copy needs to be submitted	Ve request to remove term "certification should be in OEM" Currently, there is No Network Appliance ISM which is IPS 140-2 Level 3 certified. There are OGM's win have certified their cryptographic Module certifical. All Network Appliance ISM OEM uses this Cryptographic Module in their Network Appliance ISM, however 's' not necessary OEM OF Cryptographic Module and Network Appliance ISM to be same and thereas are howed in PS 140 2 Level 3 certified cryptographic Module certificat PS 140 2 Level 3 certified cryptographic module, in meets the CCA and Wetrust guidelines. So It is and a per CCA and Wetrust Guidelines is that cryptographic key should be stored in PFS 20 2 Level 3 certified cryptographic Module. Since the cryptographic key should be stored in PFS 20 2 Level 3 certified cryptographic Module. Since the cryptographic key should be stored in PFS 20 2 Level 3 certified cryptographic Module. Since the cryptographic key should be stored in PFS 20 Level 3 certified cryptographic Module. Since the cryptographic key should be stored in PFS 20 Level 3 certified cryptographic Module. Since the cryptographic key should be stored in PFS 20 Level 3 certified cryptographic Module. Since the cryptographic key should be stored in PFS 20 Level 3 certified in the certified cryptographic module and Cryptographic Module and a periods. RFPs even the last SFP which was stored with introduced to make save Islan Network Appliance CDM are restricted to participate in RFP. As a reference, CLIPPS 20 Level 20 Level 3 certified to 20 Level 3 11/10/2022 2. 2. Sim McI 3 Level 3 Certified cryptographic module this clause and there are more RFPs mentioned below have had term without asking for this clause. 3. Tinvpati Sent Clip 3 - Rel 1. 2/100/2021/0021/2021/0022 3. Sim McI 3 Level 3 Certified cryptographic 2011/2022/2008 3. Tinvpati Sent Clip 3 - Rel 1. 2/2012/2022/2018 3. Rel 2 - Rel	HMAAC, SHA1, SHA2 (512) etc."
4	VENDOR-1	4	79		4. HSM Module:	development , integration and Testing of applications in restricted network with no outside	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	connectivity to internet . 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 Clause should be read as
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"	"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. Load balancer should capable of anti-malware feature and integration with anti-aot solution for	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 Clause should be read as
11	VENDOR-2	5	75	2	Firewall	Firewall appliance should be supplied with at least 4 x 1G ER-45 (expandable to total 8 ports) interfaces, 4 x 1G SF slots (expandable to total 8 ports), 2 x10G SFP+ (expandable to total 8 ports). Solution should include all transceivers of populated modules (4x1Gb R-4,5 4x1G SFP, 2x10G SFP+) for fibre ports from day 1.	Kindly revise the specs for better participation and health competition. "Forewall appliance should be ougsplied with at least 4 × 10 ER H-65 (responsible to total 8 ports) interfaces, 4 1 G SP 404 (sequentiable to total 8 ports). 2040 GPF (responsible to total 4 ports). Solution should include all transceivers of populated modules (44.1Gb Ri-45, 44.1G SP, 24.0G SPP-) for fibre ports from day 1."	Latuse should be read as "Firewall appliance should be supplied with at least 4 x 1GE RI-45 (expandable to total 8 ports), 2 x100 SP4 (expandable to total 4 ports), 5 voltion should include all transceives of oppolated modules (R4GB RI-45, 4x1G SP9, 2x105 SP4) 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
13	VENDOR-2	7	75	5	Firewall	Appropriate energy efficient redundant (N+N) hot swapable power supplies.	Lear opportune a solution have to easily of enables of the opportune of the opportune power supply and this requirement is already captured under point number 34 for integrated redundant power supply.	GB SSD or higher from day 1." 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.	Clause should be read as
							"Threat Protection Throughput: 3 Gbps" Kindly revise the specs as 8 Million concurrent session seems higher on 10Gbps Firewall throughput	"Threat Protection Throughput of atleast 3 Gbps" Clause should be read as
15	VENDOR-2	9	75	10	Firewall	Firewall should support at least 8 million concurrent sessions	appliance. "Firewall should support at least 3 million concurrent sessions"	"Firewall should support at least 3 million concurrent sessions or higher from day 1" Clause should be read as
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."	"Should be supplied with atleast 500 SSL VPN users license or higher from day 1" Clause should be read as
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."	"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 R145 interface and minimum throughput of 500 files/hour process across 6VMs or more. All VMs should be included	and request to remove point 33 to 37. 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	from day 1. 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 The server load balancer should cater up to at	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" Kindly revise the specs for better participation and health competition.	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	"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 4.1 LGE RI-45 (expandable to total 8 ports) interfaces. At 1G SFP slots (expandable to total 8 ports). 2.10G SFP+ (expandable to total 8 ports). 2.010 SFP+ (expandable to total 8 ports). 2010to should include all transceivers of populated modules (4.1GB RI- 45, 4.1G SFP, 2x10G SFP+) for fiber ports from day 1.	Kindly revise the specs for better participation and health competition. "Firewall applance should be supplied with at least 4 x LGE R4-8 (expandable to total 8 ports) interfaces, 4 x LGS P5 solts (expandable to total 8 ports), 2 x LGG SFP+ (expandable to total 4 ports). Solution should include all transceivers of populated modules (4xLGB R4 45, 4xLG SFP,2xLGG 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
	VENDOR -				e. 11		Kindly revise the specs as appliance with 10Gbps firewall throughput comes with lower	Durland Bele Burg - 17 - 7
30	VENDOR-3	8	75	9	Firewall	Threat Protection Throughput: 5 Gbps Firewall should support at least 8 million	threat protection throughput and asked throughput is supported on higher models. "Threat Protection Throughput: 3 Gbps" Kindly revise the specs as 8 Million concurrent session seems higher on 10Gbps Firewall throughput apoliance.	Duplicate-Refer Response at Cons. S. No 14 Duplicate-Refer Response at Cons. S. No 15
						concurrent sessions	"Firewall should support at least 3 million concurrent sessions"	
32	VENDOR-3	10	75	24	Firewall	Should be supplied with 1000 SSL VPN users license. Should have the IPS capability to inspect SSL	Kindly revise the specs for better participation and health competition. "Should be supplied with 500 SSL VPN users license." Kindly revise the specs for better participation and healthy competition	Duplicate-Refer Response at Cons. S. No 16
33	VENDOR-3	11	76	35	Firewall	traffic and SSL throughput of 9 Gbps. Should support more than 2000+ application	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." IPS signature supported is not mentioned, so request to revise specs.	Duplicate-Refer Response at Cons. S. No 17
34	VENDOR-3	12	76	45	Firewall	layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	"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

					RES	PONSES TO THE QUERIES RECEIVED AGAINST TEND	ER 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 RI45 interface and minimum throughput of 500 files/hour process across 6VMs or more. All VMs should	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	be included from day 1. 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
							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.	
38	VENDOR-3	16	61	2	Root CA	OCSP should be EAL + Certified	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	No Change
						The server load balancer should deliver at	As per best practice SSL throughput has to be maximum 50% to 60%	
39	VENDOR-3	17	74	11	Load Balancer	least 10 Gbps or higher of SSL throughput on 4096 key The server load balancer should cater up to at	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" 40K SSL CPS on 10Gbps of SSL throughput is on a higher side. Request	Duplicate-Refer Response at Cons. S. No 7
40	VENDOR-3	18	74	12	Load Balancer	least 40K or higher SSL connections per second on 2K key from day 1	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 5xLGE, 4xLG SPP ports and at least 4xL0G SPP+ 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 him 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 applicance. In CA steur, VISM 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 S shall facilities with TOTAL support required for this sactivity. 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 All deliverables, outputs, plans, drawings,	We request you to kindly revise it to 3% for a health cashflow.	No Change
47	VENDOR-3	25	40	5.6	IPR Rights	executions, evidence, proofs, and other concentrations, evidence, proofs, and other concentration of onlymer submitted by the contractor under this Contract that Become and remain the property of the NNI wind must not be shared with third parties or reproduced, whether in whole or part, without the NNI's prior written consent. The contractor shall, not later than upon termination or expiration of this Contract, deliver all such documents and ochware to the NNI's together with a detailed inventory thereord	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 N00 and cost considerations.	All deliverables, outputs, plans, drawings, specifications, designs, report, and other documents and customised software submitted by the contractor under this Contract shall become and envianithe property the HeNIX for CA- bild become and envianithe property with the HONI for CA- thied particle or regroduced, whether in whole or part, whothout HeNIX (for CA) and CAC (for cond) perior writtee consent. The contractor shall, not later than upon termination or experiation of this Contract, deliver all sub- ducuments and such customized softwares to the NIX 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, kev length, validity etc.	Whole section is not relevant for SSL. Request to remove the scope.	Deleted
49	VENDOR-3	27	70	4 (1)	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	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	devices in CMS. Firewall - 9 Nos.	Could you please provide us the break-up of the required quantity for the firewall for	The no is as per the specific design. However the biddes may assess the numbers based on their actual design
51	VENDOR		Page No.		B. For Issuing SSL – CA RFP Clause		issuing CA Request for clarification/Change	meeting all the requirments CCA/NIXI Response
52	VENDOR-4	1	65		Hardware Load Balance		Research to be actional in Dath and Compliance. This was not be accurated in Columb	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,
32	Libble 4	1	65		requirement		Request to be optional in BoQ and Compliance. This may not be required in Solution.	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. Zero day malware protect will require cloud based API and Managed console integration,	Qty mentioned in RFP - refer RFP
54	VENDOR-4	3	81		zero day malware protection		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. 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	No change.
57	VENDOR-4	6		<u> </u>	New Clause		cater the requirement. What is the signing performance is being expected via HSM.?	No change.
58	VENDOR-4	7			Additional Query		What is the signing performance is being expected via HSM.7 There are two Pre 81d queries from our side that is regraining CSPs 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 CGSP certification, since certificate revocation is a important step in any Web Trust Certified CA we feel that CCSP = EAL 4+ certification should be included the Eligibility Criteria and extra mask should be acided 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 sa s bidder can elaborate on this tert. but a better, but a better payment term mens 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 IGE RI- 45 (expandable to total 8 ports) interfaces, 4 x IG SP plots (expandable to total 8 ports), 2 x10G SPP (expandable to total 8 ports). Solution should include all transceivers of populated modules (4x106 RH-3, 4x10 SPP, 2x100 SPP+) for fibre ports from day 1.	Firewall appliance should be supplied with at least 16 x 1GE RI-45 G x 106/1G SPP- ports. Solution should include all transceivers of populated modules (1EaL6 B-45, s.AtC SPP, 2x10G SPP-) for fibre ports (MMF) from day 1.	The interface requirement of expansion modules is specific to DEM, 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 LGR H-35 (expandable to total 8 ports). JLIG STP+ (expandable to taid 4 ports). JLIG STP+ (expandable to taid 4 ports). Solution should include all transceivers of populated modules (6x1Gb RI-45, 6x1G STP, 2x1GS STP+) 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"

				1	RES Firewall Throughput: Minimum 10	PONSES TO THE QUERIES RECEIVED AGAINST TEND	ER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023	
63	VENDOR-5	4	75	2. Firewall / Performance & Scalability / SN 7	Gbps or higher throughput: Niminum 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
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.	sessions" 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 NRI.	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	Pis 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 NDX, 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 of failure in central management tool.	Ability to configure, manage and monitor NGFW using CLI / CUI with / without central management solution. NGV would like to have full feature party with centralized management to manage the Next Generation Firewall. In Case there is any construint jusces between Next Generation contral management bod then firewall should have basic management.	Since there are 9 frewalls 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 blased 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 Cul and GUI both without central management solution. Organization would like to have full feature party of centralined management look on the Nett Generation centralined management look on the Nett Generation 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 CBM for tight integration with firewall.	The proposed firewall should be included with a solution to monitor and alert about the health of servers at NOI like CPU, memory, disk, performance metrics etc. The solution should monitor at-least 10 firewalls and the management tool should be of same DEM for tight integration with firewall.	NIXI is not a university but an etnerprise customer, pis pis remove the word University from the specification. Also the proposed solution should have management tool which should manage advest 10 firewalls as per the requirement and not the servers. Hence request change.	In place of university, 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 schould have visibility of all it external facing server/applications/IP addresses directly engosed to internet so that appropriate action can be taken on the application/network/firerwall to miligate misconfiguration and vulnerability of assets.	The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, N00 should have visibility of all its external facing servers/application/P addresses directly exposed to internet so that appropriate action can be taken on the application/reducrif/iterval to mitigate misconfiguration and vulnerability of assets.	NIXI is not a university but an etnerprise customer, pis pis 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 SHA256 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.	Cause should be read as "Should support the capability of providing network-based detection of makement by checking the disposition of unknown files using MDS, 5104-1, 5104-2 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 2. Firewall /	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	Performance & Scalability / SN 52 2. Firewall /	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.		No change
83	VENDOR-5	24	77	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 S4	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. 5. No 19

					RES	PONSES TO THE QUERIES RECEIVED AGAINST TENDE	ER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023	
86	VENDOR-5	27	77	2. Firewall / Performance & Scalability / SN 56 2. Firewall /	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. 5. No 19
87	VENDOR-5	28	77	2. Firewall / Performance & Scalability / SN	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 on 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 not traffic go on cloud of an ark indi a dhankisi) is and of a dhankis solution, detecting VM-ware or memory based malware and portect 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 DEM 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 RI45 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	Pis 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). Solution should include all transcieves of poulated modules (4x1Gb RJ-45, 4x1G SFP, 2x10G SFP+) for fibre ports from day 1.	Firewail appliance should be supplied with at least 16 x 1GF R445 fx 100/1G SPP ports. Solution about include all macketwise of populated modules (16x1Gb R145, 6x1G SPP, 2x10G SPP+) 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	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 2. Firewall /	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	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 NDKI.	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	Pis 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-IPv6) / 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 CLJ CJU with / without central management solution. NGW would like to have full fature parity with centralized management to manage the Next Generation Firewall. In case there is any connectivity issues between Next Generation Fixewall and central management tool of failure in central management.	Since there are 9 frewalls 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 soft management is based 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 CPM for light integration with firewall.	The proposed firewall should be included with a solution to monitor and alert about the health of servers at NRUI Rec(7), memory, day, performance metrics etc. The solution should monitor at-less 11 forevalls and the management tool should be of same OEM for tight integration with firewall.	NICI is not a university but an etherprise customer, pis pis remove the word University from the specification. Also the proposed solution should have management tool which should manage alleas 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. The proposed solution must	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	monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, University should have visibility of all its external facing server/applications/iP addresses directly exposed to internet so that appropriate action can be taken on the application/network/lirewall to miligate misconfiguration and winerability of assets.	The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, NOU should have vulnerability of all assettman faring servers/application/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 etherprise 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	The solution must have service which scans for university's credential leaked in the dark web	Delete	Pls delete this clause.	Duplicate-Refer Response at Cons. S. No 75
110	VENDOR-6	17	76	29 2. Firewall / Performance & Scalability / SN 30	and report to stake holders. 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	Frewall 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	Should have the IPS capability to inspect SSL traffic and SSL	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
			<u> </u>	35	throughput of 9 Gbps.	and the concernment of a dups.		

					RES	PONSES TO THE QUERIES RECEIVED AGAINST TEND	ER 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 second) 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	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	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. 5. 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. 5. No 19
121	VENDOR-6	28	77	2. Firewall / Performance & Scalability / SN S7	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 on 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 or any kind on analysis) sand box solution, detecting VM-aware or memory based malware and protect from virtual sandbox exading 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 RI45 interface and minimum throughput of 500 files/hour process across 6VMs or more. All VMs should be included from day	Local malware analysis appliance should be of same OEM with 4x IGE RMS interface and minimum throughput of S00 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. 5. 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	Pis delete this clause, as this is not relevant in this specification.	Duplicate-Refer Response at Cons. S. No 92
127	VENDOR-6	34 51 No.	8 Dage Number	Eligibility Criteriaa Section	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. Original Content in RFQ	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. Chance sought/ Clarification	Pis aamend this clause, as this will help maany of the perspective serious bidders.	No Change
128	VENDOR	31. NO.	Page Number	Section	Original Content in RFQ Firewall appliance should be	change soughty clarification	Remarks	CCA/NIXI Response
129	VENDOR-7	1	75	2. Firewall / SN 2	supplied with at least 4 x 1GE RI- 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 R1-45, 4x1G SFP, 2x10G SFP+) for fibre ports from day 1.	Firewall appliance should be supplied with at least 16 x IGE RI-45 6 x 106/IC STP- ports. Solution should include all transceivers of populated modules (IACL6 B-45, AxIC STP, 2x10G STP-1) for faire ports (MMF) from day 1.	The interface requirement of expansion modules is specific to DEM, 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 2. Firewall /	Should support Active:Active & Active:Passive modes Firewall Throughput: Minimum 10	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	Performance & Scalability / SN 7	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 2. Firewall /	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 VIANs is a huge ask, and we think that 500 + VIANs 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	Pis remove ESMTP as this is a email protocol and this is not the requirement in the current scenario of NDL, as NDL 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

					PEC	PONSES TO THE QUERIES RECEIVED AGAINST TENDI	58 No CCN /02/11,2023-NIVI Dates 22,02,2023	
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 of failure in central management tool.	Ability to configure, manage and monitor NGFW using CLJ CJU with / without central management solution. NUX would like to have full fature parity with centralized management to manage the Next Generation Firewall in case there is any connectivity issues between Next Generation Treewall and central management too of hane in central 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 astim 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 frewall 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 Ught integration with firewall.	The proposed firewall should be included with a solution to monitor and alert about the health of tervers at NOI like CPU, memory, disk, performance metrics etc. The solution should mol mode the 10 firewalls and the management to all mode be of same OCM for tight integration with firewalt.	NIXI is not a university but an etherprice customer, pit pit remove the word University from the specification. Also the proposed solution should have management tool which should manage attess 10 firewalls as per the requirement and not the servers. Hence request change.	Duplicate-Refer Response at Cons. 5. 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. The proposed solution must	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	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, NO3 should have valishity of all its external facing servers/happlication/iP addresses directly exposed to internet so that appropriate action can be taken on the application/network/tirewall to mitigate misconfiguration and vulnerability of assets.	NRI is not a university but an etherprise 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	The solution must have service which scans for university's credential leaked in the dark web and report to stake holders.	Delete	Pis delete this clause.	Duplicate-Refer Response at Cons. S. No 75
145	VENDOR-7	17	76	29 2. Firewall / Performance & Scalability / SN 30	and report to stake holders. 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	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 second) 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 943-825 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 suppet 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 2. Firewall /	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	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	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 classes.	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. 5. 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. 5. 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 premiets sandbox soluton to be provided to assure no traffe go on cloud for any kind of analysis) sand box solution, detecting WV-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	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	59 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 OVMs or more. All VMs should be included from day 1	Local malware analysis appliance should be of same OEW with 4x LGE RAIS 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	Pis delete this clause, as this is not relevant in this specification.	Duplicate-Refer Response at Cons. S. No 92
162	VENDOR	SI. No.	RFP Page No.	RFP Section	Content of RFP requiring clarification(s)	Points of clarification	Remarks / Suggestions (If Any)	CCA/NIXI Response

					DEC	PONSES TO THE QUERIES RECEIVED AGAINST TENDI	ER No CCA (02(1) 2022 NIVI Dated 22 02 2022	
					RES	PONSES TO THE QUERIES RECEIVED AGAINST TENDI	EN NO. : CCA/U2(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
				specification				
				4. HSM Module:	Host Interface: Should have inbuilt Dual Gigabit Ethernet ports with			Host Interface: Should have inbuilt Dual Gigabit (or Higher
164	VENDOR-8	2	79	Minimum	port bonding and Dual 10G network port with port bonding.	As per the industry standard, an HSM comes with Dual Gigabit network interface with port bonding	Please revise it to Dual Gigabit or Dual 10G network interfaces.	Gigabit ) port with port bonding and should be ready from day 1.
				Technical Specification	All four NICs should have IPv4 and IPv6 support. Capabilities	support. 10 network ports is not mandatory.		All NICs should have IPv4 and IPv6 support capabilities from day 1.
				opeentation	should be from day 1			nom ouy 1.
				4. HSM Module:				
165	VENDOR-8	3	79	Minimum	Support for Hash Message Digest HMAC, SHA1, SHA2 (512), SM3	Please note that SM3 and SM4 are Chinese hashing algorithms required for Chinese regulations. This	Request you to kindly remove the clause.	Duplicate-Refer Response at Cons. S. No 2
				Technical Specification	and SM4	does not apply to Indian regulations.		
					HSM should have simulator	Please note that an HSM simulator should not be		
				4. HSM Module:	capabilities to provide	used for development and integration, primarily because the keys are stored in the application		
166	VENDOR-8	4	79	Minimum Technical	development , integration and Testing of applications in	itself. Moreover, the test results on a HSM simulator will differ drastically with a real HSM.	Request you to kindly remove the clause.	Deleted
				Specification	restricted network with no outside connectivity to internet .	Instead a low performance should be used for test and integration purposes.		
				4. HSM Module:		Could someone please confirm the rationnale		
167	VENDOR-8	5	79	Minimum	HSM should have unlimited client Licenses (Should not have separate	behind the ask. Unlimited client licenses suggest that any no. of client applications can connect to	Request you to kindly remove the clause.	No change
				Technical Specification	cost of any client License)	the HSM. This makes the HSM more vulnerable and the performance of the HSM will degrade.		
				specification		the performance of the risk will degrade.		
				4. HSM Module:	HSM should be FIPS 140-2 Level 3			
168	VENDOR-8	6	79	Minimum	certified and certification should be in OEM Name.	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
				Technical Specification	Certification Copy needs to be submitted			
								The quantity is as per the Tender indicative design. Bidder will offer their design meeting all the requirements of the
					BOM	Can we assume there are 3 environments - PDN.		Tender. However for cost comparisions, the tender indicative quantities will be considered if the proposed
169	VENDOR-8	7	61	Section IV	Root CA: 4x network HSM, 2x PCI	DR and UAT(QA)?. Can we know how is the HSM		design carry less no of items as compared to the tender
1					HSM	quantity derived?		indicated items. Howeever, if the requirements as per the bidder's design, are more, then actual numbers of items
1								will be considerd (based on the unit rates) for comparisions.
				1	1			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
170	VENDOR-8	8	63	Section IV	BOM Issuing CA: 10x network HSM, 2x	Can we assume there are 3 environments - PDN, DR and UAT(QA)?. Can we know how is the HSM		indicative quantities will be considered if the proposed design carry less no of items as compared to the tender
1/0		0	03	accessi iv	ISSUING CA: 10x network HSM, 2x PCI HSM	DR and UA1(QA)?. Can we know how is the HSM quantity derived?		indicated items. However, if the requirements as per the
1								bidder's design, are more, then actual numbers of items will be considerd (based on the unit rates) for
					-			comparisions.
				4. HSM Module:	FIPS 140-3 Level 3. NIST SP 800-	As of today. FIPS 140-3 level 3 certification is in		Clause may be read as "FIPS 140-2 Level 3" or higher,
171	VENDOR-8	9	80	Minimum Technical	131A with valid certification	progress and should be available in near future.	Please confirm if FIPS 140-3 Level 3 is the ask.	with valid certification in the name of OEM".
				Specification				
						Usually auditors are engaged by the CA owner, as it will be a multi year project to get into the broswer		
					The Bidder shall perform the WebTrust certification program	and is costly. Suggestion is for CA Vendor to provide PKI	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	
172	VENDOR-8	10	9	1	including incorporation of CA root in Major	discovery workshop, steps, governance	take more than 5 years.	No change
					Web Browsers	consultancuy for NIXI to get into Webtrust and browser program. Audit should be taken up by NIXI	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	
					The Bidder shall perform the	with the support of CA Vendor.	manage the compliance program	
173	VENDOR-8	11	44	6	WebTrust certification program including	Current broswers under CA/B forum are Mozilla, Microsoft, Google, Apple. What is the priority of		There is no priority as per NIXI is concerend.
					incorporation of CA root in Major Web Browsers	broswers to be recognized?		
					Contractor will carry out Vulnerability assessment (VA) and			
174	VENDOR-8	12	48	6.1	Penetration Testing (PT) using	Under what situation are the 2 tests required?		This is a security norm and needs to be followed as per the Audit Requirements.
			-		certified tool through a Third- party certified agency before			the Audit Requirements.
					acceptance, if required.			
					compliance requirements set forth by the CA/Browser Forum for			
					publicly-trusted CAs (i.e. Baseline Requirements, Network Security	Other than DV, EV and OV TLS certs, is Code-signing cert required? It was not mentioned in page 43		The requiremnt is a generic one and even if it is not
175	VENDOR-8	13	49	6.2	Requirements, Code Signing, Extended Validation, etc.) in the	"solution should mean for Organization Validation		required in the first year, it will be required in the subsequently.
					conduct of any assurance	(OV) and Domain Validation (DV)"		subsequentry.
					engagement or internal audits for Public PKIs.			
					There should be a powerful API			
					that supports certification, revocation for any end entity		I	
176	VENDOR-8	14	68	Section V	as well as to retrieve user and			The clause is calf evolutions and for further inform
					certificate information. The API	What needs to be integrated with the CA?		The clause is self explanatory and for further information, WebTrust requirements may be referred.
177	i i				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.
	VENDOP-9	15	71		should be access controlled Suggested Architecture for Root	Can we propose other architecture e.g. offline		WebTrust requirements may be referred. The Root may be offline and design may accordingly be
1	VENDOR-8	15	71	Section B	should be access controlled	······		WebTrust requirements may be referred.
		15	71		should be access controlled Suggested Architecture for Root SSL CA The CA follows a CA key migration	Can we propose other architecture e.g. offline Root, based on best practices instead?		WebTrust requirements may be referred. The Root may be offline and design may accordingly be
178	VENDOR-8	15	71 141		should be access controlled Suggested Architecture for Root SSL CA The CA follows a CA key migration script for key migration events that	Can we propose other architecture e.g. offline		WebTrust requirements may be referred. The Root may be offline and design may accordingly be
	VENDOR-8	16	141	Section B Checklist	should be access controlled Suggested Architecture for Root SSE CA The CA follows a CA key migration script for key migration events that includes the following	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system?		WebTrust requirements may be referred. The Root may be offline and design may accordingly be proposed. Checklist Point is self explainatory
178 179		16		Section B	should be access controlled Suggested Architecture for Root SSL CA The CA follows a CA key migration script for key migration events that includes the following Original Content in RPQ	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from	Remarks	WebTrust requirements may be referred. The Root may be offline and design may accordingly be proposed.
	VENDOR-8	16	141	Section B Checklist	should be access controlled Suggested Architecture for Root SSL CA The CA follows a CA key migration script for key migration events that includes the following Orginal Content in RPQ Firewall applance should be	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system?	Remarks	WebTrust requirements may be referred. The Root may be offline and design may accordingly be proposed. Checklist Point is self explainatory
	VENDOR-8	16	141	Section B Checklist	should be access controlled Suggested Architecture for Root SSL CA The CA follows a CA key migration script for key migration events that includes the following Orginal Content in RPQ Firewall applance should be supplied with at least 4 x JGC RJ- 65 (expandable to total 8 ports)	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification	Remarks	WebTrust requirements may be referred. The Root may be offline and design may accordingly be proposed. Checklist Point is self explainatory
	VENDOR-8	16	141	Section B Checklist	aloud be access controlled Sagestead architecture for floot Sa. CA. The CA follows a CA key migration acrigit for key migration events that includes the following Original Context in 847 Merchail agalance 810cd Merchail angolied much at loss 4.10 EF (equinabile to call a point) interface, 4.10 SFP aloss (equinabile to call a point).	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Firewall appliance should be supplied with at least 16x XGER.445 6x XD0/1G SPP.ponts. Solution hould include all transceivers of populated	The interface requirement of expansion modules is specific to OEM, hence request to change the	WebTrust requirements may be referred. The Root may be offline and design may accordingly be proposed. Checklist Point is self explainatory
179	VENDOR-8	16 Sr. No.	141 Page Number	Section B Checklist Section	aloud be access controlled Suggested Architecture for Root SSL GA The CA follows a CA key migration acrigit for key migration events that includes the following Original Content in BFQ Finewall appliance include in Prevention in the sol & a SE B (includes the following Original Content in BFQ Finewall appliance include in the solution of the solution of the interface, 4 = 10 SFP sides (expandiable to total B ports), z100 SFP (expandiable to total B port), z105 SFP (expandiable to total B port),	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Firewall appliance should be supplied with at least 16 x 1GE RI-45 G x 100/1/G SPP- ports. Solution should include all transceivers of populated modules (16:10B net 5, sd. 1GS PP, 100 SPP) for		WebTrust requirements may be referred. The Root may be offline and design may accordingly be proposed. Checklist Point is self explainatory CCA/NUXI Response
179	VENDOR-8	16 Sr. No.	141 Page Number	Section B Checklist Section	aloud be access controlled Suggested Architecture for Root SB. CA De CA Nellows a CA key migration acrigt for key migration events that includes the following <b>Dorginal Contentin INFO</b> Firewall appliance should be applied with at least 4 a LGR Rh- d's (ensure), a LGR Rh- d's (ensure), a least 4 a LGR Rh- d's (ensure), a least 4 a LGR Rh- d's (ensure), a least 4 a LGR Rh- d's	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Firewall appliance should be supplied with at least 16x XGER.445 6x XD0/1G SPP.ponts. Solution hould include all transceivers of populated	The interface requirement of expansion modules is specific to OEM, hence request to change the	WebTrust requirements may be referred. The Root may be offline and design may accordingly be proposed. Checklist Point is self explainatory CCA/NUXI Response
179	VENDOR-8	16 Sr. No.	141 Page Number	Section B Checklist Section	aloud the access controlled Segretal Architecture for Root SR CA De CA Allows a CA key migration scrigt for key migration events that includes the following <b>Original Content in BFC</b> Frewall appliance should be applied with at teas 4 a LER Bi- d's (expandiable to total 8 parts) (expandiable results) (expandiable resul	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Firewall appliance should be supplied with at least 16 x 1GE RI-45 G x 100/1/G SPP- ports. Solution should include all transceivers of populated modules (16:10B net 5, sd. 1GS PP, 100 SPP) for	The interface requirement of expansion modules is specific to OEM, hence request to change the	WebTrust requirements may be referred. The Root may be offline and design may accordingly be proposed. Checklist Point is self explainatory CCA/NUXI Response
179	VENDOR-8	16 Sr. No.	141 Page Number	Section B Checklist Section	about the access controlled Segretal Architecture for Root SR CA Tes CA follows a CA key migration end of the migration events and includes the following Original Content in BPC Firewall appliance should be supplied with at least 4 a LOE RI- 45 (expandiable to total 8 ports), 20 (50 GFP (expandiable to total 8 ports), end 5 GFP (expandiable to total 8 ports), parameters of proportied models to total parameters of proportied models to total parameters of proportied models to total strates of the parts from day 1. Each applicates that we can solve the SR Calcito RH-4 Calcitor RH-2 Calcitor SR - for fibre parts from day 1. Each applicates should have located analiable scorage of 200 GG SSD	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Firewall appliance should be supplied with at least 16 x 106 R 14-5 x 100/16 SPP, ports. Solution indue and incomesers of populated modules (10x100 IN-45, Ax10 SPP, bit) for fibre ports (pMH) from day 1. Each appliance should have local available storage	The interface requirement of expansion modules is specific to OEM, hence request to change the expansion modules to fixed port from day 1.	WebTrust requirements may be referred. The Root may be offline and design may accordingly be proposed. Checklist Point is self explainatory CCA/NUXI Response
179 180 181	VENDOR-8 VENDOR VENDOR-9	16 Sr. No. 1	141 Page Number 75 75	Section B Checklist 2. Firewall / SN 2. Firewall / SN 2. Firewall / SN	aboul the access controlled Suggested Architecture for Root SD, CA The CA follows a CA key migration exerts that indues the following Original Content in BVQ Freewall appliance thould be sopplied with at least 4 J CE Bi- da (equandable to total 8 ports). Soughed with at least 4 J CE Bi- da (equandable to total 8 ports). Col GSPP (equandable to total 8 ports). Col GSPP (equandable to total 8 ports). Souton should include all ports). Solution should in clude all ports). Solution should in clude all ports). Solution should in clude all ports). Solution should include all ports). Solution should be to ports). Solution should be to ports). Solution should include all ports). Solution should include all ports). Solution should be to ports). Solution should be to ports). Solution should be to ports). Solution should be to ports). Solution should be to ports). Solution should be to ports). Solution should be to ports). Solution should be to ports). Solution should be to ports). Solution should be to ports). Solution should be to ports). Solution should be to ports). Solution should be to ports). Solution should be to ports). Solution should be to ports). Solution should be to ports). Solution should be t	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Firewall appliance should be supplied with at least 16× 10E R.445 6× 100/16 SPP, ports. Solution include intracekers of populated modules (16x10b Ri-45, ex10 SPP, brit) for fibre ports (MMF) from day 1. Each appliance should have local available storage of 1 TB SSD in-built in the firewall 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. NOI should have min 1.18 storage in-built in the firewall for storing config data and logs in case of management server failure.	WebTrust requirements may be referred.         The Root may be offline and design may accordingly be proposed.         Checklist Point is self explainatory         CCA/NUXI Response         Duplicate-Refer Response at Cons. S. No 60         Duplicate-Refer Response at Cons. S. No 61
179	VENDOR-8 VENDOR VENDOR-9	16 Sr. No. 1	141 Page Number 75	Section B Checklist Section 2. Firewall / SN 2	aboul the access controlled Suggested Architecture for Root Sa, CA The CA follows a CA key migration script for key migration events that induces the following Original Content in BFQ Firewall appliance should be supplied with at least 4 J CE Ri- ds (expandiable to total 8 ports). Supplied with at least 4 J CE Ri- ds (expandiable to total 8 ports). Supplied with at least 4 J CE Ri- ds (expandiable to total 8 ports). SubJiolin Should in clude at ports). SubJiolin Should in clude at ports). SubJiolin Should in clude at parts 1 Auto Should storage of 200 GB SSD Should support Active-Active & Risk	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Firewall appliance should be supplied with at least 16 x 106 R 14-5 x 100/16 SPP, ports. Solution indue and incomesers of populated modules (10x100 IN-45, Ax10 SPP, bit) for fibre ports (pMH) from day 1. Each appliance should have local available storage	The interface requirement of expansion modules is specific to OEM, hence request to change the expansion modules to fixed port from day 1.	WebTrust requirements may be referred.
179 180 181 182	VENDOR-8 VENDOR VENDOR-9 VENDOR-9	16 Sr. No. 1 2 3	141 Page Number 75 75 75	Section B Checklist Section 2. Firewall / SN 2. Firewall / SN 2. Firewall / SN 5. Firewall / SN 5. Firewall / SN	aloud be access controlled Sagestead Architecture for foot SSL CA The CA follows a CA key migration script for key migration events that includes the following Original Context in 8700 Freenall applanes in 8700 Freenall applanes and B ports, 2 respondible to total B ports, retraces, 4 10 GFP aloss feegondable to total B ports, ratio GFP, legandable to total B sprojed with at least 4 116 BFP despinalised to and B ports, ratio GFP, legandable to total B straice in 97, solution hour licitude all transcreeves of populated modules available to scale of 97, 2006 SFP-1 for fixe ports from der J Should support Active Active B available totage of 200 GB SSD available totage of 200 GB SSD Artive Passer modes Freevall Throughput. Minimum 10 Freevall Throughput. Minimum 10	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Firewall appliance should be supplied with at least 16 x 167 R-M-56 x 100/16 SPP, ports. Solution bioloil include all manoelvers of populated modules (16x1Gb RI-45, Ax1G SPP, 2x10G SPP+) for fibre ports (MMF) from day 1. Each appliance should have local available storage of 1 TB SSD in-built in the firewall from day 1. Should support Active.Active / Active.Passive modes	The interface requirement of expansion modules is specific to OEM, hence request to change the expansion modules to fixed port from day 1. NOI should have min 1.TB storage in-built in the firewall for storing config data and logs in case of management server failure. Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change.	WebTrust requirements may be referred.
179 180 181	VENDOR-8 VENDOR VENDOR-9	16 Sr. No. 1	141 Page Number 75 75	Section B Checklist Section 2. Firewall / SN 2 2. Firewall / SN 2 5. Firewall / SN 6	about the access controlled Segretal Architecture for Root SR CA De CA Allows a CA key migration scrigt for key migration events that includes the following Original Content in BFC Firewall appliance should be applied with the start 4 x LE RI- 45 (separativation) and the start 4 x LE RI- 40 (separativation) and the start 4 x LE RI- 40 (separativation) and the start 4 x LE start 50 (separativation) and the start 4 x LE RI-10 (separativation) and the start 4 x LE RI-10 (separativation) and the	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Firewall appliance should be supplied with at least 15 L GE R.8.45 & st 100/1/G SP4 ports. Solution should include all transceivers of populated modules (16x16) H.4.5, skc1G SP, 2x10G SPP4) for fibre ports (MMF) from day 1. Each appliance should have local available storage of 1 TB SSD in-built in the firewall 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. NIXI should have min 1 TB storage in-built in the firewall for storing config data and logs in case of management server failure.	WebTrust requirements may be referred.         The Root may be offline and design may accordingly be proposed.         Checklist Point is self explainatory         CCA/NUXI Response         Duplicate-Refer Response at Cons. S. No 60         Duplicate-Refer Response at Cons. S. No 61
179 180 181 182	VENDOR-8 VENDOR VENDOR-9 VENDOR-9	16 Sr. No. 1 2 3	141 Page Number 75 75 75	Section B Checklist Section 2. Firewall / SN 2 2. Firewall / SN 6 2. Firewall / SN 6 2. Firewall / SN 5 5. Scalability / SN 7	about the access controlled Segretal Architecture for Root S2 CA Theor CA follows a CA key migration excipt for key migration events includes the following Original Content in BFQ Firewall appliance should be supplied with at least 4 a CE R- 45 (expandiable to total 8 ports). Source S1 and S1	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Chance sought/ Clarification Friewall appliance should be supplied with at least 16 x 106 R.445 & x 100/16 SPP, ports. Solution induel indue all mancevers of populated module (16x10b II-45, Ast10 SPP, 2x100 SPP-) for fibre ports (MMP) from day 1. Each appliance should have local available storage of 1 TB SD In-built in the firewall from day 1. Should support Active-Active / Active-Passive modes Firewall Throughput: Minimum 9 Gbps or higher	The interface requirement of expansion modules is specific to OEM, hence request to change the expansion modules to fixed port from day 1. NOI should have min 1.TB storage in-built in the firewall for storing config data and logs in case of management server failure. Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change.	WebTrust requirements may be referred.
179 180 181 182	VENDOR-8 VENDOR VENDOR-9 VENDOR-9	16 Sr. No. 1 2 3	141 Page Number 75 75 75	Section B Checklist Section 2. Firewall / SN 2 2. Firewall / SN 2 2. Firewall / SN 6 2. Firewall / SN 6 2. Firewall / SN 7 2. F	aloud the access controlled Segretal Architecture for floot S2.CA The CA follows a CA key migration except for key migration except for key migration actudes the following Original Content in BFO Firewall appliance should be supplied with at least A 1CE BA- dS (expandiable to total B ports). Supplied with a test at A 1CE BA- dS (expandiable to total B ports). Subcommentation of include all ports). Solution mound in ciclude all ports). Solutions mound in ciclude all ports). Solution port Active Active Active Passier modes active processes and port ports and beap provided with Envis is enabled in durate (f) Firewall invocation.	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Firewall appliance should be supplied with at least 16 x 105 R14-5 x 100/16 SPP, ports. Solution induel and an another solution solution induel and another solution solution modules (10x100 II) -45, Ax10 SPP, ports. Solution fibre ports (MMP) from day 1. Each appliance should have local available storage of 1 TB SD III-built in the firewall from day 1. Should support Active-Active / Active-Passive modes Firewall Throughput: Minimum 9 Gbps or higher throughput on 64 byte packets as per RFC 2544. Firewall should support at least 4 million	The interface requirement of expansion modules is specific to OEM, hence request to change the expansion modules to fixed port 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.           Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any entreprise firewall all across the globe. Hence, request change.           Request to change as per RFC 2544 the Firewall throughput for 64 byte packets.           B million concurrent connection is on a very higher side for a 10 Gbps Firewall, hence request to	WebTrust requirements may be referred.
179 180 181 181 182 183	VENDOR-8 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9	16 Sr. No. 1 2 3 4	141 Page Number 75 75 75 75	Section 8 Checklist Section Section 2. Firewall / SN 2 Sirewall / SN 2 Firewall / SN 2 Firewall / SN 2 Firewall / SN 3 Scalability / SN 3 Checklist S Checklist	about be access controlled Suggested architecture for floot SSL GA The CA follows & CA key migration acrigit for key migration events that includes the following Original Content in 872 Thermall ing/inter floot day for instantion in the solution of the solution of the control of the solution of the solution of the control of the solution of the solution interface, 4 10 SPF aloss (expandiable to total B ports), 2100 SPF (expandiable to total B ports), 210 SPF (expandiable to total B por	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Firewall appliance should be supplied with at least 16 x 10E R.445 & x 100/16 SPP, ports. Solution induel at Inacoevers of populated modules (16x10b Ri-45, Ax10 SPP, 2x100 SPP+) for fibre ports (MMF) from day 1. Should support Active-Active / Active-Passive modes Firewall throughput: Minimum 9 Gbps or higher throughput on 64 byte packets as per RFC 2544.	The Interface requirement of expansion modules is specific to OEM, hence request to change the expansion modules to fixed port from day 1	WebTrust requirements may be referred.  The Root may be offline and design may accordingly be proposed.  Checklist Point is self explainatory  CCA/NUXI Response  Duplicate-Refer Response at Cons. S. No 60  Duplicate-Refer Response at Cons. S. No 61  Duplicate-Refer Response at Cons. S. No 63
179 180 181 182 183 184	VENDOR-S VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9	16 <b>Sr. No.</b> 1 2 3 4 5	141 Page Number 75 75 75 75 75 75 75	Section B Checklist Section 2. Firewall / SN 2 2. Firewall / SN 2 2. Firewall / SN 6 2. Firewall / SN 6 2. Firewall / SN 7 2. F	aloud the access controlled Segretal Architecture for floot S2.CA The CA follows a CA key migration except for key migration except for key migration actudes the following Original Content in BFO Firewall appliance should be supplied with at least A 1CE BA- dS (expandiable to total B ports). Supplied with a test at A 1CE BA- dS (expandiable to total B ports). Subcommentation of include all ports). Solution mound in ciclude all ports). Solutions mound in ciclude all ports). Solution port Active Active Active Passier modes active processes and port ports and beap provided with Envis is enabled in durate (f) Firewall invocation.	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Firewall appliance should be supplied with at least 16 x 105 R14-5 x 100/16 SPP, ports. Solution induel and an another solution solution induel and another solution solution modules (10x100 II) -45, Ax10 SPP, ports. Solution fibre ports (MMP) from day 1. Each appliance should have local available storage of 1 TB SD III-built in the firewall from day 1. Should support Active-Active / Active-Passive modes Firewall Throughput: Minimum 9 Gbps or higher throughput on 64 byte packets as per RFC 2544. Firewall should support at least 4 million	The interface requirement of expansion modules is specific to OEM, hence request to change the expansion modules to fixed port 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.           Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any entreprise firewall all across the globe. Hence, request change.           Request to change as per RFC 2544 the Firewall throughput for 64 byte packets.           B million concurrent connection is on a very higher side for a 10 Gbps Firewall, hence request to	WebTrust requirements may be referred.   The Root may be offline and design may accordingly be proposed.  Checklist Point is self explainatory  CCA/NUX Response  Duplicate-Refer Response at Cons. S. No 60  Duplicate-Refer Response at Cons. S. No 61  Duplicate-Refer Response at Cons. S. No 62  Duplicate-Refer Response at Cons. S. No 63  Duplicate-Refer Response at Cons. S. No 63
179 180 181 181 182 183	VENDOR-8 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9	16 Sr. No. 1 2 3 4	141 Page Number 75 75 75 75	Section B Checklist Section 2. Firewall / SN 2. 5. Firewall / SN 2. 5. Firewall / SN 6 2. Firewall / SN 7 2. Firewall / SN 7 7. Firewall / SN 7 7. Firewall / SN 7 7. Firewall / SN 7. 7. Firewall / SN 7. Fir	about the access controlled Segretal Architecture for floot SE CA De CA Allova X CA key migration acrigt for key migration events that includes the following <b>Original Contentin RFQ</b> Firewall appliance should be applied with a test A LG R J- d's (expandiable to total B ports) and the second second second second second second second second second SFP+ for fibre ports from day 1. Each applicance should have local should support Active Active & Active Paraw modes SFP+ for fibre ports from day 1. Each applications of the second SFP+ for fibre ports from day 1. Each application that and the second SFP+ for fibre ports from day 1. Each applications from day 1. Each applications from day 1. Each application to the second application of the second second active Paraw modes found support Active Active Active Active Active Paraw modes found support Active Active & Active Paraw modes found support Active Active Active frewall throughout: Shifter frewall abuild support at heat 6 million concurrent sessions	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Chance sought/ Clarification Firewall appliance should be supplied with at least 15 LGF RA-55 & studio/LGF SFP ports. Solution should include all transceivers of populated modules (1stotic BA-55, actot SFP, 2x100 SFP+) for fibre ports (MMF) from day 1. Each appliance should have local available storage of 1 TB SSD in-built in the firewall from day 1. Each appliance should have local available storage modes firewall Throughput Active-Active / Active-Passive modes firewall Throughput. Minimum 9 Gbps or higher throughput on 64 byte packets as per BFC 2544 . Firewall should support at least 4 million concurrent sessions	The interface requirement of expansion modules is specific to OEM, hence request to change the expansion modules to fixed port from day 1. NOT should have min 1 TB storage in-built in the firewall for storing config data and logs in case of management server failure. Firewall with Active Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change. Request to change as per RFC 2544 the Firewall throughput for 64 byte packets. B million concurrent connection is on a very higher side for a 10 Gbps Firewall, hence request to reduce to 4 million.	WebTrust requirements may be referred. The Root may be offline and design may accordingly be proposed. Checklist Point is self explainatory CCA/NUXI Response Duplicate-Refer Response at Cons. S. No 60 Duplicate-Refer Response at Cons. S. No 61 Duplicate-Refer Response at Cons. S. No 62 Duplicate-Refer Response at Cons. S. No 63
179 180 181 182 183 184 185	VENDOR-8 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9	16 Sr. No. 1 2 3 4 5 6	141 Page Number 75 75 75 75 75 75 75 75	Section 8 Checklist Checklist Section 2. Firewall / SN 2 . Firewall / SN 3 . Firewall / Performance & Scalability / SN 3 . Firewall / Performance & Ferformance & Scalability / SN 3 . Firewall / Performance & Scalability / SN 3 . Firewall / Performance & Scalability / SN 3 . Firewall / SCALABILITY / SN 3 . Fir	should be access controlled Segented Architecture for Root SR CA De CA Allows a CA key migration scrigt for key migration events that includes the following <b>Original Content in BFC</b> Firewall appliance should be upplied with the text 4 LG R- 45 (sepandiable to total 8 port) scrigt for key and the start 4 LG R- 45 (sepandiable to total 8 port) scrigt for Key and the start 4 LG R- 45 (sepandiable to total 8 port) scrigt for Key and the start 4 LG R- 45 (sepandiable to total 8 port) scrigt for Key and the start 4 LG R- 45 (sepandiable to total 8 port) scrigt for Key and the start 4 LG R- 40 (SS PF) (sepandiable to total 8 port) scrigt for Key and the start 8 port (scrigt R-14 Key ACM) Scrigt R-14 (scrigt R-14 K	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Chance sought/ Clarification Firewall appliance should be supplied with at least 15 105 R ± 55 6 × 100/15 SP+ ports. Solution should include all transceivers of populated modules (16x160 ± 45.5, acto SP; 2x100 SP+) for fibre ports (MMF) from day 1. Each appliance should have local available storage of 1 TB SSD in-built in the firewall from day 1. Each appliance should have local available storage modes firewall Throughput on 64 byte packets as per BFC 2544 . Firewall through support at least 4 million concurrent sessions	The interface requirement of expansion modules is specific to OEM, hence request to change the expansion modules to fixed port from day 1.           NOX should have min 1 TB storage in-built in the firewall for storing config data and logs in case of management server failure.           NOX should have min 1 TB storage in-built in the firewall for storing config data and logs in case of management server failure.           Request to change as per RFC 2564 the Firewall throughput for 64 byte packets.           B million concurrent connection is on a very highrer side for a 10 Gbps Firewall, hence request to reduce to 4 million.           SOR ession/connections per secong is also a huge number for a 10 Gbps throughput firewall, hence request to reduce to 110k.	WebTrust requirements may be referred.         Proposed.         Checklist Point is self explainatory         CCCA/NXX Response         Duplicate-Refer Response at Cons. S. No 60         Duplicate-Refer Response at Cons. S. No 61         Duplicate-Refer Response at Cons. S. No 62         Duplicate-Refer Response at Cons. S. No 63
179 180 181 182 183 184	VENDOR-S VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9	16 <b>Sr. No.</b> 1 2 3 4 5	141 Page Number 75 75 75 75 75 75 75	Section B Checklist Section 2. Firewall / SN 2 2. Firewall / SN 4. Firewall / SN 5 2. Firewall / SN 5 5 5 5 5 5 5 5 5 5 5 5 5	should he access controlled Suggested Architecture for Root SL CA The CA follows a CA key migration script for key migration script for key migration control for key migration control for key migration devides the following Original Content in 89/Q Firewall appliance should be supplied with a test and the script for key migration devides the following Displant control for the script script for key migration devides the following Displant control for the script script for the prot script for the script script for the prot script for the script firewall schoold support at tests t firewall schoold support at tests	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Friewall appliance should be supplied with at least 16 x 1GE R.455 & 100/1G SPP. ports. Solution Moduli Indue all mancevers of porty ports. Solution Haracevers of populated module (16x1Cb IK-45, ActO SPP. ports. Solution fibre ports (MMP) from day 1. Each appliance should have local available storage of 1 TB SSO In-built in the frewall from day 1. Should support Active.Active / Active.Passive modes Firewall should support at least 4 million concurrent sessions	The interface requirement of expansion modules is specific to OEM, hence request to change the copansion modules to fixed port from day 1.           NIOS should have min 1 TB storage in-built in the firewall for storing config data and logs in case of management server failure.           NIOS should have min 1 TB storage in-built in the firewall for storing config data and logs in case of management server failure.           Prevail with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change.           Request to change as per RFC 2544 the Firewall throughput for 64 byte packets.           B million concurrent connection is on a very higher side for a 10 Gbps Firewall, hence request to reduce to 4 million.           SOOK session/connections per secong is also a huge number for a 10 Gbps throughput firewall, f	WebTrust requirements may be referred.   The Root may be offline and design may accordingly be proposed.  Checklist Point is self explainatory  CCA/NUX Response  Duplicate-Refer Response at Cons. S. No 60  Duplicate-Refer Response at Cons. S. No 61  Duplicate-Refer Response at Cons. S. No 62  Duplicate-Refer Response at Cons. S. No 63  Duplicate-Refer Response at Cons. S. No 63
179 180 181 182 183 184 185	VENDOR-8 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9	16 Sr. No. 1 2 3 4 5 6	141 Page Number 75 75 75 75 75 75 75 75	Section 8 Checklist Checklist Section 2. Firewall / SN 2 2. Firewall / Performance & Scalability / SN 10 2. Firewall / Performance & Scalability / SN 10 2. Firewall / Performance & Scalability / SN 10 2. Firewall / Performance & Scalability / SN 10 2. Firewall / Performance & Scalability / SN 10 2. Firewall / Performance & Scalability / SN 10 2. Firewall / Scalability / SN 11 2	aloud be access controlled Segested Architecture for hoot SSL CA The CA follows a CA key migration script for key migration events that includes the following Original Context in 1870 (Renardlang beams should be soppled with at least 4 a 106 fel- de (equandable to total 8 ports). A total 8 ports). A total 8 ports). A start of the soppled with at least 4 a 106 fel- gepandable to total 8 ports). A total 8 ports). A total 8 ports, 4 a 10 SPP alos (Renardlang beams). A total 8 ports). A total 8 ports). A total 8 ports). A total 8 ports). A total 8 ports, 4 a 10 SPP alos (Renardlang beams). A total 8 ports, 4	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Friewall appliance should be supplied with at least 16 x 10E RV45 & x 100/16 SPP, ports. Solution module (10x102) IV-45, Act SPP, ports. Solution modules (10x102) IV-45, Act SPP, ports. Base ports (MMS) from day 1. Each appliance should have local available storage of 1 TB SD IN-built in the firewall from day 1. Each appliance should have local available storage of 1 TB SD IN-built in the firewall from day 1. Firewall should support at least a per RFC 2544. Firewall should support at least 4 million concurrent sessions Firewall should support at least 110K sessions / connections per second	The interface requirement of expansion modules is specific to DEM, hence request to change the expansion modules to fixed port from day 1.           ND0 should have min 1.T8 storage in-built in the firewall for storing config data and logs in case of management server failure.           Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change.           Request to change as per RFC 2544 the Firewall throughput for 64 byte packets.           B million concurrent connection is on a very highter side for a 10 Gbps Firewall, hence request to reduce to 4 million.           SOR session/connections per secong is also a huge number for a 10 Gbps throughput firewall, hence request to reduce to 110K.           In any enterprise network requirement of 10000 VLNs is a huge ack, and we think that 500 + VLNs.	WebTrust requirements may be referred.         Proposed.         Checklist Point is self explainatory         CCCA/NXX Response         Duplicate-Refer Response at Cons. S. No 60         Duplicate-Refer Response at Cons. S. No 61         Duplicate-Refer Response at Cons. S. No 62         Duplicate-Refer Response at Cons. S. No 63
179 180 181 182 183 184 185	VENDOR-8 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9	16 Sr. No. 1 2 3 4 5 6	141 Page Number 75 75 75 75 75 75 75 75	Section 8 Checklat Checklat Checklat Section 2. Firewall / SN 2 Firewall / SN 2 Firewall / SN 2 Firewall / SN 3 2 Firewall / SN 5 Calability / SN 1 2 Firewall / Performance & Scalability / SN 1 2 Firewall / Performance & Scalability / SN 1 2 Firewall / Performance & Scalability / SN 1 2 Firewall / Performance & Scalability / SN 1 2 Firewall / Performance & Scalability / SN 1 2 Firewall / Performance & Scalability / SN 1 2 Firewall / Performance & Scalability / SN 1 2 Firewall / Performance & Per	aloud be access controlled Suggested arXiIIseture for hoot SSL CA The CA follows SCA key migration acrigit for key migration events that includes the following Original Context in 870 memory of the following Status 270 and 280 percent interface, 4 10 SFP alos memory of the following of the following memory of the following of the following memory of the following of the following status 280 percent and the following anallable to total 89 p.2010 SFP alos for the perturbation of the following anallable tota get of 200 GB SSD and Use and the following of the set anallable concernet sessions freewall throudd support at least 2000 K-MsNs. Freewall should support at least 1000 VL/Ms.	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Friewall appliance should be supplied with at least 18 x 106 R/s45 & x 100/16 SPP, ports. Solution induel and an	The interface requirement of expansion modules is specific to DEM, hence request to change the expansion modules to fixed port from day 1. NOI should have min 1 TB storage in-built in the firewall for storing config data and logs in case of management server failure. Firewall with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change. Request to change as per RFC 2544 the Firewall throughput for 64 byte packets. 8 million concurrent connection is on a very higher side for a 10 Gbps Firewall, hence request to reduce to 4 million. 5005 sessions/connections per secong is also a huge number for a 10 Gbps throughput firewall, hence request to reduce to 110K. 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 NOC. PIs remove ESMTP as this is a email protocol and this is not the requirement in the current scenario	WebTrust requirements may be referred.         Proposed.         Checklist Point is self explainatory         CCCA/NXX Response         Duplicate-Refer Response at Cons. S. No 60         Duplicate-Refer Response at Cons. S. No 61         Duplicate-Refer Response at Cons. S. No 62         Duplicate-Refer Response at Cons. S. No 63
179 180 181 182 183 184 185 186	VENDOR-8 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9 VENDOR-9	16 <b>Sr. No.</b> 1 2 3 4 5 6 7	141 Page Number 75 75 75 75 75 75 75 75	Section B Checklist Section 2. Firewall / SN 2 2. Firewall / SN 2 2. Firewall / SN 3. Firewall / SN 4. Firewall / SN 5. Firewall / SN 6. Firewall / SN 7. Firewall / SN 2. Firewall / SN 3. Firewall	should be access: controlled Sagested Architecture for flood Sa CA De Ca Allowa S CA key migration scrigt for key migration events that includes the following <b>Original Contentin HPC</b> Firewall appliance should be applied with at least 4 LG B J- d5 (expandiable to total 3 ports) at 00 SPH Contentin HPC Stress of populated module total 4 and 10 sectors of populated modules SPP-1 for fibre ports from day 1. Each applicance should have local should support Arkine-Active & Active Parkaw modes SPP-1 for fibre ports from day 1. Each applicative that SP 2.210G SPP-1 for fibre ports from day 1. Each applicate while the G is enabled and days while the G is enabled and days while the G is enabled in future. (f) Firewall thould support at least 5 SOK sessions per second Firewall flood support at least SOK sessions per second Firewall flood support at least SOK sessions per second	Can we propose other architecture e.g. offline Root, based on best practices instead? What existing keys need to be migrated, and from what system? Change sought/ Clarification Firewall appliance should be supplied with at least 16 x 10E R.445 & x 100/16 SPP, ports. Solution induel intransexiers of populated modules (16x10b Ri-45, ActG SP, 2x10G SPP) for fibre ports (MMF) from day 1. Each appliance should have local available storage of 17B SSD in-built in the firewall from day 1. Should support Active:Active / Active:Passive modes Firewall should support at least 10K sessions / connections per second Firewall should support at least 10K sessions / connections per second	The interface requirement of expansion modules is specific to OEM, hence request to change the expansion modules to fixed port from day 1.           NOX should have min 1 TB storage in-built in the firewall for storing config data and logs in case of management server failure.           NOX should have min 1 TB storage in-built in the firewall for storing config data and logs in case of management server failure.           Prevail With Advert Seave configuration with state synchronization is the standard configuration mode for any enterprise firewall all across the globe. Hence, request change.           Request to change as per RFC 2544 the Firewall throughput for 64 byte packets.           B million concurrent connection is on a very highrer side for a 10 Gbps Firewall, hence request to reduce to 4 million.           SOOK ession/connections per secong is also a huge number for a 10 Gbps throughput firewall, hence request to reduce to 110ic.           Tit 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 NOC.	WebTrust requirements may be referred.         The Root may be offline and design may accordingly be proposed.         Checklist Point is self explainatory         CEA/NUX Response         Duplicate-Refer Response at Cons. S. No 60         Duplicate-Refer Response at Cons. S. No 61         Duplicate-Refer Response at Cons. S. No 61         Duplicate-Refer Response at Cons. S. No 62         Duplicate-Refer Response at Cons. S. No 63         Duplicate-Refer Response at Cons. S. No 64         Duplicate-Refer Response at Cons. S. No 65         Duplicate-Refer Response at Cons. S. No. 65

					RFS	PONSES TO THE QUERIES RECEIVED AGAINST TENDI	FR No CC4/02(1)-2023-NIXI Dated 22-03-2023	
188	VENDOR-9	9	75	2. Firewall / Performance & Scalability / SN	Should support Static, RIP, OSPF, OSPFv3 and RGP	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) & Nat64 (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	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 blased 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 certain annagement solution. University would like to have full feature parity of centralized management tool on the Kert Generation Firewall Radii, in case there is any connectivity issues between Next Generation Firewall and central management tool. or failure in central amagement tool.	Ability to configure, manage and monitor NGFW using CLJ / GUI with / without central management solution. NUX would like to have full fature parkty 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.	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 astim management is based towards OEM, as every OEM have different mechanism to manage one or multiple or 100s of freevalls.	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 CPM for tight integration with firewall.	The proposed firewall should be included with a solution to monitor and alert about the health of severs at NRIB (Re CPU, memory, disk, performance metrics etc. The solution should monitor at-less II forwalls and the management tool should be of same OEM for tight integration with firewall.	NOO is not a university but an etherprise customer, pis pis remove the word University from the specification. Also the proposed solution should have management tool which should manage atteast 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 montor vulnerabilities of internet exposed assets and report to stakeholders. For example, University should have visibility of all its external facing servers/application//# addresses directly exposed to internet so that appropriate action can be application/network/firewall to mitigate misconfiguration and wulnerability of assets.	The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, NU3 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/lirewall to mitigate misconfiguration and vulnerability of assets.	NIXI is not a university but an etnerprise customer, pis pis 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	Pis delete this clause.	Duplicate-Refer Response at Cons. S. No 75
196	VENDOR-9	17	76	2. Firewall / Performance & Scalability / SN 30 2. Firewall /	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	Frewail with Active-Passive configuration with state synchronization is the standard configuration mode for any enterprise firewail all across the globe. Hence, request change.	Duplicate-Refer Response at Cons. S. No 76
197	VENDOR-9	18	76	Performance & Scalability / SN	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 second) 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	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. 5. 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. 5. 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 S9 2. Firewall /	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 analysais jand box solution, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware.	Advance unknown malware analysis engine with real landnawer (deficiated on premiser sandbox real-diation to be provided to alsure to train.go on cloud for any link of nankpils and bus solution, detecting VM-wave or memory based malware and provect from virtual sandbox evading advance unknown malware.	On-Premixe 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	Performance & Scalability / SN 59	Solution should support OS type - Windows 10, Windows 8.1, Windows 7, Linux, Android. Local malware analysis appliance should be of same OEM with 4x	Solution should support OS type - Windows 7 (32 / 64 bit), Linux 64 Local malware analysis appliance should be of	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	Should be of same UEW with 4x 1GE RI4S interface and minimum throughput of 500 files/hour process across 6VMs or more. All VMs should be included from day 1	Local marware anaryss appliance should be of same OEM with As LGE R4S Interface and minimum throughput of S00 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

					RES	PONSES TO THE QUERIES RECEIVED AGAINST TENDE	R 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	PIs 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 IGE RJ- 45 (expandable to total 8 ports) interfaces, 4 x IG 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, 4xIG SFP-) zx10G SFP-) for filte ports from day 1.	Firewall appliance should be supplied with at least 16 x IGE R445 6 x 100/16 SPP+ ports. Solution should include all mancevers of populated modules (16x1Gb R445, 4x1G SPP, 2x10G SPP+) 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. 5. No 60
				2. Firewall / SN	Each appliance should have local	Each appliance should have local available storage		
215	VENDOR-10	2	75	2. Firewall / SN 2	available storage of 200 GB SSD after 1+1 RAID.	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	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 VIANs is a huge ask, and we think that 500 + VIANs should be sufficient to meet the current requirement of NDU.	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	Pis remove ESMTP as this is a email protocol and this is not the requirement in the current scenario of NIX(, as NIX) 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/I3 switch. Request change.	Duplicate-Refer Response at Cons. S. No 68
223	VENDOR-10	10	75	2. Firewall / Performance & Scalability / SN 19 2. Firewall /	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to- IPv4) & Nat64 (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 CLJ / OUI with / without central management solution. NOI would like to have full feature party with centralizate management to manage the Next Generation Firewall. In case there is any Tiesaal and central management tool of failure in central management tool then firewall should have basic management.	Since there are 9 frewalls 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 blased lowards OEM, as every OEM have different mechanism to manage one or multiple or 100s of firewalls.	Duplicate-Refer Response at Cons. 5. 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 solution 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 NDI like CPU, memory, disk, performance metrics etc. The solution should monitor at-least 10 firewalls and the management tooi should be of same OEM for tight integration with firewalt.	NIXI is not a university but an etherprise customer, pis pis remove the word University from the specification. Also the proposed solution should have management tood which should manage atleast 10 firewalls as per the requirement and not the servers. Hence request change.	Duplicate-Refer Response at Cons. 5. 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	Request change.	Duplicate-Refer Response at Cons. S. No 73
228	VENDOR-10	15	76	2. Firewall / Performance & Scalability / SN 28	amm users access. 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/application/# addresses directly exposed to internet so that appropriate action can be taken on the application/hetwork/firewall to amitgate misconfiguration and vulnerability of assets.	users. The proposed solution must monitor vulnerabilities of internet exposed assets and report to stakeholders. For example, NO3 should have vability of all reserveral facing serveral/application/IP addresses directly exposed to internet to that appropriate action can be taken on the application/network/Interwall 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. 5. 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	Pis 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 uring SHA-256 file-hash or signature (update to be provided in 300 second) 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-25 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
				1	Should cater to reputation and category based URL filtering offering comprehensive alerting	Should cater to reputation and category based URL filtering offering comprehensive alerting and	Inspection of 50+ categories should be enough for and URL Filtering requirement. Hence request change.	Duplicate-Refer Response at Cons. S. No 79
233	VENDOR-10	20	76	2. Firewall / Performance & Scalability / SN 44	and control over suspect web traffic and enforces policies in more than 75 categories from day one.	control over suspect web traffic and enforces policies in more than 55 categories from day one.		
233 234	VENDOR-10 VENDOR-10	20	76 77	Performance & Scalability / SN 44 2. Firewall / Performance & Scalability / SN 50	and control over suspect web traffic and enforces policies in		The requirement is for a firewall and not a WAF, hence request change.	Duplicate-Refer Response at Cons. S. No 80
				Performance & Scalability / SN 44 2. Firewall / Performance & Scalability / SN 50 2. Firewall / Performance & Scalability / SN 51	and control over suspect web trafic and enforces policies in more than 75 categories from day one. Web Application Firewall Protection Proposed appliance should have in build WAF with Reverse proxy support,	policies in more than 55 categories from day one. Delete Delete	The requirement is for a firewall and not a WAF, hence request change. This is a WAF feature and hence pls delete this clause.	Duplicate-Refer Response at Cons. S. No 80 Duplicate-Refer Response at Cons. S. No 81
234	VENDOR-10	21	77	Performance & Scalability / SN 44 2. Firewall / Performance & Scalability / SN 50 2. Firewall / Performance &	and control over suspect web traffic and enforces policies in more than 75 categories from day one. Web Application Firewall Protection Proposed appliance should have in- build WAF with Reverse proxy	policies in more than 55 categories from day one.		

					RES	PONSES TO THE QUERIES RECEIVED AGAINST TEND	ER 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 inspection.	Delete		Duplicate-Refer Response at Cons. 5. 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	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
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 is Should has open API option to integrate 3rd Party solution	Delete		Duplicate-Refer Response at Cons. 5. No 19
241	VENDOR-10	28	77	2. Firewall / Performance & Scalability / SN	Solution must offer vulnerability management to verify servers	Delete		Duplicate-Refer Response at Cons. S. No 19
242	VENDOR-10	29	77	57 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 doud 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 traffe go on cloud for any kind of analysis) sand box solution, detecting With-ware 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	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	59 2. Firewall / Performance & Scalability / SN 61	Local malware analysis appliance should be of same OEM with 4x 1GE RI45 interface and minimum throughput of 500 files/hour process across 6VMs or more. All VMs should be included from day 1	Local mahware 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	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	for optimal performance. Solution should have orchestrate, automate incident and response module for SOC operation with at least 2 user licenses from day 1.	Delete	Pis delete this classe, as this is not relevant in this specification.	Duplicate-Refer Response at Cons. 5. No 92
247	VENDOR	<b>S.No.</b>	Page No 22 of 32	Point No		Specification Firewall appliance should be supplied with at least 4x LGE RL-4S (expandable to total 8 ports) interfaces, 4x LGSF9 totic (secondable to total 8 ports), 2x LGG SF9 - (expandable to populated modules (skt/GB xL-4S, skt/G SF9 2x LGG SF9-1) for fibre ports (mom dey 1.Each appliance should have local available storage of	Changes Request Firewall appliance should be supplied with at least 16 x 1GE RI-45 interfaces with 3 x10G SFP+ ports. Solution should have 2 USB 3.0, 1 Conside, 1 MgmL, 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.	CCA/NUR Response Clause should be read as "Tirrevail applicate should be supplied with at least 4 x 1GE RH-G (sepandable to total 8 ports) interfaces. 4 x 1G 579 dots (sepandable to total 8 ports), 210G 57P+ (respandable to total 4 ports), 50ution should include all transcrivers of populated modules (&1GB R-45, &1G 57P, 2x10G 57P+) for fibre ports from day 1."
						200 GB SSD after 1+1 RAID. Firewall Throughput: 50Gbps of throughput on		"Each appliance should have local available storage of 200 GB SSD."
249	VENDOR-11	2	22 of 32	7		64 byte packets. Performance should not degrade while IPv6 is enabled in future.(F)	Firewall inspection throughput: 5Gbps	Incorrect specification/page is being referred.
250 251	VENDOR-11 VENDOR-11		22 of 32 22 of 32	8		IPS Throughput 12 Gbps NGFW Throughput: 9 Gbps	IPS Throughput: 3.3 Gbps NGFW Throughput: 1.5 Gbps	Incorrect specification/page is being referred. Incorrect specification/page is being referred.
251	VENDOR-11 VENDOR-11	5	22 of 32	10		Threat Protection Throughput: 10 Gbps	Threat Protection Throughput: 3 Gbps	Incorrect specification/page is being referred.
							annen an angelen a angel	
253	VENDOR-11	6	22 of 32 22 of 32	11		Firewall should support at least 8 million concurrent sessions Firewall should support at least 55K New sessions	Firewall should support at least 500,000 DPI Connections	Incorrect specification/page is being referred.
	-					Firewall should support at least 8 million concurrent sessions Firewall should support at least 55K New sessions per second Firewall should support at least 1000 VLANs		
254 255 256	VENDOR-11 VENDOR-11 VENDOR-11	7 8 9	22 of 32 22 of 32 22 of 32 22 of 32	12 13 14		Firewall should support at least 8 million concurrent sessions Firewall should support at least 55K New sessions per second Firewall should support at least 1000 VLANs Firewall should support at least 50 Gbps of IPSEC VPN throughput	Firewall should support at least 500,000 DPI Connections Firewall should support at least 21,000 Connections per second Firewall should support at least 25 Logical VLAN Firewall should support at least 2.1 Gbps of IPSEC VPN throughput	Incorrect specification/page is being referred. Incorrect specification/page is being referred. Incorrect specification/page is being referred. Incorrect specification/page is being referred.
254 255	VENDOR-11 VENDOR-11	7	22 of 32 22 of 32	12 13		Firewall should support at least 8 million concurrent sessions Firewall should support at least 55K New sessions per second Firewall should support at least 1000 VLANs Firewall should support at least 50 Gbps of IPSEC	Firewall should support at least 500,000 DPI Connections Firewall should support at least 21,000 Connections per second Firewall should support at least 255 Logical VLAN	Incorrect specification/page is being referred. Incorrect specification/page is being referred. Incorrect specification/page is being referred.
254 255 256 257	VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11	7 8 9 10	22 of 32 22 of 32 22 of 32 23 of 32	12 13 14 25		Freeail should support at least 5 million concrerent sessions Freeail should support at least 55K New sessions Freeail should support at least 1000 VLANs Freeail should support at least 1000 VLANs Freeail should support at least 50 Gbps of IPSEC VPN throughput Should be supplied with 1000 SSL VPN users Ability to configure, manage and monitor NGFW using CL and GL load's without central management tool of the Net Generation Freeail should support to the Street management tool on the Net Generation Freeail should support to failure in central management tool on failure in central management tool on failure in central management tool on failure in central and era about the health of servers in the university like CPU, memory, disk, performance terks set. The solution should monitor at least about the health of servers in the university like CPU, memory, disk, performance dertises tert. The solution should monitor at least 20 servers and should be of same QEM for tight	Firewall should support at least 50,000 DPI Connections Firewall should support at least 21,000 Connections per second Firewall should support at least 21.000 Connections per second Firewall should support at least 21.000 Connections Firewall should support 200 SSL VPN users. Firewall should have the ability to configure, manage and monitor INGTW using Q1 and QUI both whould central management tool on the Next Generation Firewall Intel for the next feature parity of centralized management tool on the Next Generation Firewall should be in control and and entrol Firewalls and the institution is added with a solution to monitor and ater about the health firewalls and her institution wide, performance metrics etc. The solution firewalls and the institutions and solution to monitor and alter about the health firewalls and the institutions and solution to monitor and ater about the health firewalls and the institution and solution to monitor and ater about the health firewalls and the institution and solution to monitor and alter about the health firewalls and the institution and solution to monitor and alter about the health firewalls and the institution and solution to monitor and alter about the health firewalls and the institution and solution to monitor and alter about the health firewalls and the institution and solution to monitor and alter about the health firewalls and the institution and the solution to monitor and alter about the health firewalls and the institution and the solution to monitor and alter about the health firewalls and the institution and the solution to monitor and alter about the health firewalls and the institution and the solution to monitor and alter about the health firewalls an	Incorrect specification/page is being referred. Incorrect specification/page is being referred. Incorrect specification/page is being referred. Incorrect specification/page is being referred.
254 255 256 257 258	VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11	7 8 9 10 11	22 of 32 22 of 32 22 of 32 23 of 32 23 of 32 23 of 32	12 13 14 25 26		Frewail should support at least 5 million concrerent sessions Frewail should support at least 55N New session Frewail should support at least 1000 VLANs Frewail should support at least 1000 VLANs Frewail should support at least 1000 VLANs Alling to configure, manage and monitor NGFW uning CU and CUI both without central management stoluton. University would like to have full feature parity of centralized management stoluton. University would like to the stoluton stolutor at least frewail should support at least 500 Kps of the have full feature parity of centralized management stolen the Next Generation Firewail itself, in case there is any connectivity usues between Next Generation Firewail and central management tool of failure in central and et about the health of servers in the university like CPU, memory, disk, performance test's etc. The solution should menter at least 200 the should be of same the state of the server. In the same statement of the reveal. Should have inbuilt feature for two factor at least two admin users access. The proposed solution must monitor vulnerabilites to internet soluto a the approprise factory exposed internet spoets of assess and report to stakeholders. For example, university should have visibility of a lite scentral facing server/application/lite addresses directly exposed internet spoet and vulnerability of usets	Firewall should support at least 50,000 DPI Connections Firewall should support at least 21,000 Connections per second Firewall should support at least 2.1 Gbps of IPSC VPN throughput Firewall should support at least 2.1 Gbps of IPSC VPN throughput Firewall should have the ability to configure, manage and monitor NGFW using CLI and GUI both without central management toution. Institution would like to have feature parity of centralian management too on the Net Generation Firewall and central management too on the Net Generation Firewall and central management too of not heve the enablity to the included with a solution to monitor and alert about the abudi able to monitor arisest 10 freewalls and should be of same CEM for tight integration with freewall.	Incorrect specification/page is being referred.
254 255 256 257 258 258 259	VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11	7 8 9 10 11	22 of 32 22 of 32 22 of 32 23 of 32 23 of 32 23 of 32 23 of 32	12 13 14 25 26		Frewail should support at least 3 million concurrent essential frewail should support at least 55N New session frewail should support at least 550 Obps of IPSEC VPN throughput Should be support at least 50 Obps of IPSEC VPN throughput Should be supplied with 1000 SSL VPN users Ability to configure, manage and monitor NGFW using CL and CLI both without central management solution. University would like to have full feature parity of centralized frewail itself in case there is any consorting remail. Takel in case there is any consorting management tool failure in central management tool for large in the university like CQU memory, disk, performance metrics act. The solution is monitor and alert about the health of servers in the university like CQU memory, disk, performance metrics act. The solution monitor for and alert about the fature for two factor authentication vito OTP (email or mobile) for alakent data dama users access. The proposed solution must monitor vulnerabilities interest of back appropriate action can be taken on the application/Paddress directly esposed intercify and and vulnerability of sets 1 The solution must have service which sears for university's credental leaked in the dark web	Firewall should support at least 50,000 DPI Connections Firewall should support at least 21,000 Connections per second Firewall should support at least 21,000 Connections per second Firewall should support at least 21. Glop of IPSIC VPN throughput Firewall should support 300 SSI. VPN users.  Firewall should have the ability to configure, manage and monitor INGFW using CLI and GUI both without central management solution. Institution would like to have feature parity of centralised management tool on the Next Generation Firewall litel. In case there is any connectivity issue Howen Next Generation Firewall and central management too of failure in central management tool.  The proposed firewalls should be included with a solution to monitor and afer about the health firewalls.  Should have inbuilt feature like SSD for atleast two admin firewall users.  The proposed firewalls should be able to monitor vulnersbillities of internet exposed assets and report stakeholders. For example, institution vulnersbillities of internet exposed assets and report stakeholders. For example, institution doud have vuisibility of all its external force	Incorrect specification/page is being referred.
254 255 256 257 258 258 259 260	VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11	7 8 9 10 11 11	22 of 32 22 of 32 22 of 32 23 of 32 23 of 32 23 of 32 23 of 32 23 of 32	12 13 14 25 26 27 28		Freeail should support at least 3 million concurrent sessions Freeail should support at least 55K New session Freeail should support at least 50K New Session Freeail should support at least 50K New Session Freeail should support at least 50K New Session Should be supplied with 1000 SSL VPN users Ability to configure, manage and monitor NGFW using CL and GLI both without central management solution. University would like to have full feature parity of centralized management solution. University would like statistical session of the Sec International Section on the Nat Generation Freeail Itself, in case there is any connectivity usus between New Ceneration Firewall and central management tool or failure in central management tool on the Nat Generation intervisity like CPU, menory, disk, performance metrics etc. The solution should monitor at- least 20 servers and should be of same CEM for tight releast 20 servers and should be of same CEM for tight alternation surf freeaall. Should have inbuilt feature for two factor alterative admin users access. The proposed balance mut monitor universibilities of internet epocked assets and report to alternative admin users access. The proposed balance and report to alternative so that appropriate action can be taken to internet so that appropriate action can be taken microfinguration and vulnersibility of assets The solution mut monitor universibility of assets the solution should monitor universibility of and report to state holders Should have the IPS capability to inspect 5Sk traffed do SL throughbut of 9 Gbns.	Rewall should support at least 52,000 DPI Connections Firewall should support at least 52,000 Connections per second Firewall should support at least 52,000 Connections per second Firewall should support at least 52,000 Connections per second Firewall should support at least 52,000 Connections per second Firewall should support 500 551.VPN users. Firewall should have the ability to configure, manage and monitor NGPW 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 alter. In case there is any connectivity issue Heaven Peter Generation Firewall and test. In case there is any connectivity issue management tool. The proposed firewall should be included with a solution to monitor and altert about the solut able to monitor at least 10 freewalls and should be of same GRM. For light integration with freewall. Sloudd have inbuilt feature like SSO for atleast two admin firewall users. The proposed firewall should be able to monitor vulnerabilities of internet exposed assets and report of stakeholders. For example, institution should have subility of all its external facing report of stakeholders. For example, institution should have subility of all its external action to a Application / Network Firewall to mitigate the issue. The proposed firewall Should have facility or have service which cans for Institution	Incorrect specification/page is being referred.
254 255 256 257 258 259 260 260 261 262 263	VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11	7 8 9 10 11 11 12 13 13 14 15 16	22 of 32 22 of 32 22 of 32 23 of 32	12 13 14 25 26 27 27 28 29 35 51		Frewall should support at least 3 million concurrent sessions Frewall should support at least 55K New sessions Frewall should support at least 500 VLANS Frewall should support at least 500 goot infSEC VPN throwshould Should be supplied with 1000 SSL VPN users Ability to configure, manage and monitor NGFW using CL and GLI both without central management solution. University would like to have full feature parity of centralized management solution. University would like the solution of the NGC Generation Frewall shud support to least 50 Generation frewall stud; in case there is any connectively related to the NGC Generation management tool of halve is central management tool of halve is central management tool The proposed firewall should metrics to: The solution to monitor and alert about the health of servers in the university like CPU, memory, disk, performance metrics etc. The solution to monitor and alert about the health of servers in the university like CPU, memory, disk, performance metrics etc. The solution monitor and alert about the frevall. Should have inbuilt resture for two factor aleast two admin users access. The proposed solution must monitor vulnerabilities of internet spoted assets and report to aleast two admin users access. The solution must monitor vulnerability of aleast two adminest access. The solution must monitor vulnerability of aleast the solution set monitor vulnerability of aleast the adminest access. The solution must monitor vulnerability of assets of the rest to take headers and solution should monitor vulnerability of advects to take headers and solution should monitor vulnerability of sets that appropring advects advective peoped to internet spote aleast and report to advectority credential leaked in the dark web and report to state headers.	Rewall should support at least 500,000 DPI Connections Firewall should support at least 52,000 Connections per second Firewall should support at least 22,000 Connections per second Firewall should support at least 22,000 Connections per second Firewall should support at least 22,000 Connections per second Firewall should support at least 22,000 Connections Firewall should support 500 SSL VPN users. 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 party of centralized management tool on the Next Generation Firewall attention to or failure in color failure in the between Next Generation Firewall attention to or failure in color failure in the between Next Generation Firewall attention to or failure in color failure in the solution to monitor would also to monitor would also to monitor attents 10, memory, disk, performance metrics left. The solution integration with frewalls and be included with a solution to monitor and allert about the health frewalls in the lostitution like CPU, memory, disk, performance metrics left. The solution integration with frewalls and about the solution to monitor would also to monitor attents 10 firewall should be of same OEM for tight integration with frewall.  Fine proposed frewall should be able to monitor vulnerabilities of internet exposed assets and resport to tabeholders. For example, institution should have visibility of all its external facing reservs / Application / Vis decet generation internet out papropriate action can be taken on the Application / Network Firewall to mitigate the issues.  The proposed frewall Should have facility or have service which scans for institution credential leaked in the dark web.  Should have the IPS capability to inspect SSL traffic and SSL throughput of 800 Mbps. Request to remove (WAF features)	Incorrect specification/page is being referred. Incorrect specification/page i
254 255 256 257 258 259 260 261 262 263 264	VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11	7 8 9 10 11 11 12 12 13 13 14 15 16 17	22 of 32 22 of 32 22 of 32 23 of 32 24 of 32	12 13 14 25 26 27 28 29 35		Frewall should support at least 3 million concurrent sessions Frewall should support at least 55K New sessions Frewall should support at least 500 VLAIs Frewall should support at least 500 VLAIs Frewall should support at least 500 VLAIs Should be supplied with 1000 SSL VPN users Ability to configure, manage and monitor NGFW using CLI and GLI both without central management stolicul. University would like to have full feature parity of centralized management stolicul. University would like to the stole of the stole of the stole management tool on the Nat Generation management tool on the Nat Generation management tool The proposed firewall should monitor and alert about the health of servers in the university like CJM, memory, disk, performance metrics etc. The solution monitor and alert about the health of servers in the university like CJM, memory, disk, performance metrics etc. The solution monitor and alert about the freature for two factor athentication with firewall. Should have inbuilt feature for two factor athentication with firewall. Should have the JPS capability of soles The solution mark monitor vulnerabilities and report to state hodders Should have the JPS capability to inspect Sk tartfield and report to state hodders Should have the JPS capability to inspect Sk tartfield aff sks throngshould of Solin.	Rewall should support at least 500,000 DPI Connections Firewall should support at least 21,000 Connections per second Firewall should support at least 21,000 Connections per second Firewall should support at least 21,000 Connections per second Firewall should support at least 21,000 Connections Firewall should support 500 SSLVPN users. Firewall should have the ability to configure, manage and monitor MGFW using CLI and GUI both whout central management solution. Institution would like to have feature parity of centralized management tool on the Next Generation Firewall alter. In case there is any connectivity issue between Next Generation Firewall and central management tool or failure in central management tool. The Next Generation Firewall should be included with a solution to monitor and arit about the hasht freewalls in the institution like CPU, memory, disk, performance metrics etc. The solution should also monitor arises 10 firewalls and should be of same OEM for tight integration with freewall. Should have inbuilt feature like SSO for atleast two admin firewall users. 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 server / Application / Vie dectly operation the Application / Network Firewall to mitigate the issue. The proposed firewall Should have facility or have service which scans for institution cedential leaked in the dark web. Should have the IPS capability to inspect SSL traffic and SSL throughput of 800 Mlaps. Request to remove (WAF Features)	Incorrect specification/page is being referred. Incorrect specification/page i
254 255 256 257 258 259 260 261 262 263 264	VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11	7 8 9 10 11 11 12 12 13 13 14 15 16 17	22 of 32 22 of 32 22 of 32 23 of 32	12 13 14 25 26 27 27 28 29 35 51	PP Reference Section	Freeal should support at least 3 million concurrent sessions Freeal should support at least 55K New sessions Freeal should support at least 500 VLANS freeal should support at least 500 goot inSEC VM throughout Should be supplied with 1000 SSL VPN users Ability to configure, manage and monitor NGFW using CL and GLI both without central management solution. University would like to have full feature parity of centralized management solution. University would like to the solution of the solution of the solution management solution. University would like to have full feature parity of centralized management tool on the Net Generation frame the solution of the solution of the solution of the included with solution to monitor and alert about the health of servers in the university like CPU memory, disk, performance metrics etc. The solution is should monitor and alert about the health of servers in the university like CPU memory, disk, performance metrics etc. The solution must monitor vulnerabilities of internet exposed axets and report to factor aleast two admin users access. The solution must monitor vulnerabilities of internet exposed axets and report to an the application/rework/firmwill to mitigate micronfiguration and vulnerability of assiss The solution must have service which scans for university's (credential leaked in the dark we bandement four bandship of the server in Proposed application should must have service which servers protection, Cross-site scripting protection, HTTPS (TLS/SSL) encryption affloadine.	Rewall should support at least 50,000 DPI Connections Firewall should support at least 52,000 Connections per second Firewall should support at least 52,000 Connections per second Firewall should support at least 52,000 Connections per second Firewall should support at least 52,000 Connections PESC VPN throughput Firewall should support 500 551.VPN users. 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 party of centralized management tool on the Next Generation Firewall attents. The solution to or failure in control firewall should have the ability to configure, manage and monitor NGFW using CLI and GUI both without central management tool. The Next Generation Firewall attents. Firewall should have the lostitution like CPU, memory, disk, performance metrics etc. The solution intogration at least 10 firewall and should be of same OEM for light integration with frewall. Should have inbuilt feature like SSO for atleast two admin firewall users. The proposed firewall should be able to monitor vulnerabilities of internet exposed assets and report to tableholders. For example, institution should have visibility of all its ceternal facing the Application / Network firewall to mitigate the suse. The proposed firewall should be able to monitor vulnerabilities of internet exposed assets and report to tableholders. For example, institution should have visibility of all its ceternal facing the Application / Network firewall to mitigate the suse. The proposed firewall both should have facility or have service which scans for institution credential leaked in the dark web. Should have the IPS capability to inspect SSL traffic and SSL throughput of 800 Mbps. Request to remove (WAF Features) Pedits of cellefication required Application, the struted Application,	Incorrect specification/page is being referred. Incorrect specification/page i
254 255 256 257 258 258 259 260 260 261 262 263 264	VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11	7 8 9 10 11 11 12 12 13 13 14 15 16 17	22 of 32 22 of 32 22 of 32 23 of 32 24 of 32	12 13 14 25 26 27 27 28 29 35 51	BFP Reference Section E Suggested Specifications: 1. Load balancer	Frewall should support at least 3 million concurrent sessions Frewall should support at least 55K New sessions Frewall should support at least 500 VLAIs Frewall should support at least 500 VLAIs Frewall should support at least 500 VLAIs Should be supplied with 1000 SSL VPN users Ability to configure, manage and monitor NGFW using CLI and GLI both without central management stolicul. University would like to have full feature parity of centralized management stolicul. University would like to the stole of the stole of the stole management tool on the Nat Generation management tool on the Nat Generation management tool The proposed firewall should monitor and alert about the health of servers in the university like CJM, memory, disk, performance metrics etc. The solution monitor and alert about the health of servers in the university like CJM, memory, disk, performance metrics etc. The solution monitor and alert about the freature for two factor athentication with firewall. Should have inbuilt feature for two factor athentication with firewall. Should have the JPS capability of soles The solution mark monitor vulnerabilities and report to state hodders Should have the JPS capability to inspect Sk tartfield and report to state hodders Should have the JPS capability to inspect Sk tartfield aff sks throngshould of Solin.	Exeault should support at least 52,0000 DPI Connections Firewall should support at least 52,000 Connections per second Firewall should support at least 52,000 Connections per second Firewall should support at least 52,000 Connections per second Firewall should support at least 52,000 Connections per second Firewall should support 500 SSLVPN users. Firewall should have the ability to configure, manage and monitor NGPW using CLI and CUI both without central management solution. Institution would like to have feature parity of centraliaed management tool on the Next Generation Firewall alter. It can be re is any connectivity issue between Next Generation Firewall and test. In case there is any connectivity issue between Next Generation Firewall and test. In case there is any connectivity issue between Next Generation Firewall and the induded with a solution to monitor and altert about the have proposed firewall and be induded with a solution to monitor and altert about the should able to monitor at least 1D freewalls and should be of same OEM for tight integration with firewall. Solud have inbuilt feature like SSO for atleast two admin firewall users. The proposed firewall blood de able to monitor vulnerschildlike of intense ergoped assets and sorver/ Applications / IP's directly exposed to internet to that appropriate action can be taken on the Application / Network Firewall to mitigate the issues. The proposed firewall OEM should have facility or have service which iscans for institution credential leaker in the dark web. Should have the IPS capability to inspect SSL traffic and SSL throughput of 800 Mpps. Request to remove (WAF Features) Request to remove (WAF Features) Request to remove (WAF Features) Segueted Gause <b>:</b> Segueted G	Incorrect specification/page is being referred. Incorrect specification/page i
254 255 256 257 258 259 260 260 261 262 263 264 264 265	VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11 VENDOR-11	7 8 9 10 11 12 13 14 15 16 17 <b>S. No</b>	22 of 32 22 of 32 23 of 32 24 of 32 24 of 32 24 of 32	12 13 14 25 26 27 27 28 29 35 51	E. Suggested Specifications:	Firewall should support at least 3 million concurrent sessions Firewall should support at least 3 source of the firewall should support at least 3 source of first firewall should support at least 3 source of the have full feature parity of centralized management tool net Next Generation firewall itself, in case there is any connectivity such such that the source of the source of the nanagement tool the proposed firewall should methy for tight integration with firewall. Should have inbuilt feature for two factor athentic tool of the second of the source of the such and with firewall. Should have inbuilt feature for two factor athentic too admin users acces. The proposed source and report to athentic too admin suces acces. Should have the source of the source of the second supplication must monitor vulnerabilities of internet spoted assets and report to subscholers. For example, University should have wisblity of all its centeral facing severs/application must monitor vulnerabilities of a source application must monitor vulnerabilities and report to stat appropriate action can be taken distantion of sources of should have in-built MAF in the solution must monitor vulnerabilities and report to stat appropriate action can be taken distantion of a source of sources of the sources on the supplication of a source of the application stat sources actes and report to stat appropriate action can be taken distantion of a sources of sources of the sources on	Exeault should support at least 52,0000 DPI Connections Firewall should support at least 52,000 Connections per second Firewall should support at least 52,000 Connections per second Firewall should support at least 52,000 Connections per second Firewall should support at least 52,000 Connections per second Firewall should support 500 SSLVPN users. Firewall should have the ability to configure, manage and monitor NGPW using CLI and CUI both without certral management solution. Institution would like to have feature parity of centraliaed management tool on the Next Generation Firewall alter. It can be the size y connectivity issue between Next Generation Firewall alter. It can be the size y connectivity issue between Next Generation Firewall acted management tool of abilite or include management tool. The proposed firewall be included with a solution to monitor and altert about the proposed firewall be included with a solution to monitor and altert about the solut ability to feature like SSO for atleast two admin firewall users.  Fire proposed firewall feature like SSO for atleast two admin firewall users.  The proposed firewall doubd be able to monitor vulnerabilities of intennet ergoad assets and report to statedwark. Firewall to mitigate the issues.  The proposed firewall Dem should have facility or have service which cans for institution credential leaked in the dark web.  Should have the PS capability to inspect SSL traffic and SSL throughput of 800 Maps.  Request to remove (WAF Features)  Peties of addification required  As pro our experimer from the industry, WRP is the industry standard and widely used protocol for high availability. Based on our index stately composed solution should have fue capability to right stately index y composed solution and regerime form the industry. WRP is the industry standard and widely used protocol for high availability. Based on our understanding from the Clause, proposed solution should not ac private y accord or high Availability in mail time between the pairs. The prop	Incorrect specification/page is being referred. Incorrect specification/page i

					KES	PONSES TO THE QUERIES RECEIVED AGAINST TENDE	EK IND. : CCA/U2(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	Duplicate-Refer Response at Cons. S. No 7
						The server load balancer should cater up to at least	key. 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	
270	VENDOR-12	5	5		E. Suggested Specifications: 1. Load Balancer	NC of higher SSL connections per second on 2K key from day 1	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 4s1GE, 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 x10G) to support number of ports requirements. Additionality solution should have reducing to ut of band management port and decicated console port of configuration and management. Suggested Clause : The sever load balancer should be proposed with 8 Ports populatead/ut clause and solution ports and atleast 5 and 50Fx9 R gorts mody 1 (without Bead/UL Claube support) The proposed appliance should have 2 x 10 decicated management port and 1 R445 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 resourcesincluding (PD), memory, network, acceleration resources, operating system, management is positioned complete separate environment from applications and management. Suggested Clause : The proposed device should have hypervisor (should not use Open Source) Based Virtualization feature that virtualizes the Device resourcesincluding CPU, memory, network, and acceleration resources. The hypervisor used to virtualize the hardware should be a specialized purpose build hypervisor and MOT a commercially available hypervisor (Sile XEN, VMware,RVM etc.). (Public Available Reference link should be shared) Each Virtual Instance contains a complete and separated environment of the Following: b) Configurations, d) Obsequences, d) Operating System The proposed device should support 5 Virtual Instance from Day 1 and support upto 30 Virtual Instandone as well as virtualized mode.	No change
	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 Cause : 1. OEM should have OEM TAC in NRDA (since last 10 years) 2. OEM Should have OEM TAC in NRDA (since last 10 years) 3. The proposed OEM should be Parent Technology OEM only (Should NOT be Whitelabled or Co- branding or 21 dParty Technology or OPM Source of Reselfer Agreement 4. OEM should have in NRDA (Lass-1 compliant pare Government MR) Guidelines & subsequent Amendments. 5. Min CEM (MSMRI) is exempted from OEM turnover and Number of year experience eligibility 6. OEM (MSMRI) is exempted from OEM turnover and Number of year experience eligibility 6. OEM/OEM subsidiary/OEM Sister concern Company should be present in INDIA for more than 15 years	
274	VENDOR-13	5.No.	Document Reference Page 78; Minimum		Content of the RFP HSM should be network based	Justification for change Requested network stack mentioned in the RFP,	Suggested Modification HSM should be network based appliance with inbuilt NIC support for 1 GB or 10 GB network .	CCA/NIXI Response Duplicate-Refer Response at Cons. S. No 163
2/3	VENDOR 13	1	rage 70, Minimum Technical Specification (HSM Module). S No 1		nam should be network to assed	explosion netrotions class immunoted in the en- includes capability of sending data botto at 16 and 106 J.0006 connection are backward compatible to IGBE but in order to reduce & remove network performance issues, devices bloudd only communicate using either 108 or 1068 interface at a given time. Thus ISSMs will only be using either IGBE or 1008E interface. Also adding both options will lead to single vendor participation ,request you to make this generic.	ntan sidou de fectivo kolece applance min moun ne sapon for a de ora da de fectivo k	uopinale neer negulise a. Unis. J. Nº 203
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 1050E connection are backward compatible to 158E but in order to reduce & menvoe network performance issues, devices should only communicate using either 1GB or 105B interface at a given time Thus iSMAs will only be using either	Nost Interface: Should have inbuilt Dual Gigabit Ethernet ports with port bonding of Dual 1DG 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:	1GBE or 10GBE interface 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 1	VENDOR-13	4	Page 78; Minimum Technical Specification (HSM Module). 5 No 22		ISM should have capabilities to increase TFS on same appliance by applying locinose upgrade package. In case of Hardware resecuented to addition of new appliance to increase the TFS, of additional networks the MOM included by HSM OEM in BOM during initial states as per organization's guidelines. OEM must provide Down's Day service whenever needed by client at no additional notice.	In order to include cost, please mention range with minimum and maximum values. Dooms Day service is DOM specific feature and would prevent participation. It essentially means the rSM has a backdoor for key extraction which can be done by the DDM.	KSM 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 narware include be included by ISM COM In BOM in Unit at gas a 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 ITS on same applicance by applying license or upgrade can be applying license of the term of the term of the term package can be charaver exploratement or addition influence hardware evolution be induced by HCM ODB M BDM during initial stage. ODF must provide emergency support of any matter 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 certification sales in the tender for other solutions like CA Software, Digital Certificate Life Cycle Manager, COS Responder & Hac CE CAL4- certification carries scores too as per the RFP.	NSM should be RIPS 140-2 Level 3.8 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
	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 BFP	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
283	VENDOR-13 VENDOR-13 VENDOR-13		Physical Characteristics Host Connectivity		Should Support PCIe with external smart card reader PCIe x4	Different OEM's use different things like tokens instead of smartcards. Recommend to make this 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	Should Support Low profile FOC and with external smart card / token with their own PN or Password for multifactor authentication PC-Express CEM 3.0, PCL PCE Express Base 2.0	Should Support PCIe card with external smart card / token Duplicate-Refer Response at Cons. S. No 5
	VENDOR-13		Key backup		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.		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
	Vendor VENDOR-14		Compliance RFP Page 80	Section 6. Layer 3 Switch	Clause 4. General Requirements- The Ethernet switch being proposed must be a Secure Access switches deliver a Secure, Bingle, Scalable Ethernet solution with outstanding security, performance and manageability for threat	for digital signing use case. Change required Please remove the clause	Justification This is a OEM specific feature and is blocking other OEMs to participate. So, kindly remove for wider OEM participation.	CCA/NIXI Response No Change

					RES	PONSES TO THE QUERIES RECEIVED AGAINST TENDE	ER No. : CCA/02(1)-2023-NIXI Dated 22-03-2023	
289	VENDOR-14	-	81		<ol> <li>Authentication Requirements- Switch should support DHCP supports (BHC) HPG, IP source guard, IP sourceguard violation lug, Dynamic ARB inspection, IP-G RA guard, ISMP supports (BHC), Should have management protocol that allows NGW Security Appliance to seamlessly manage any Ethernet Switch</li> </ol>	Switch should support DHCP snooping IPv4 / IPv6, IP source gund, IP sourcegund violation leg/counters, Dynamic AAP inspection or equivalent feature, IPv6 RA guard or equivalent feature, IKMP snooping/roxy/querier, VLMN staching (Dn() , MCAG, GCB mraing (Pv4/Pv6,) <u>Brould have-</u> management protocol that allows- NGCFW-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 DIPC shouling IPvA ( IPvG, IP source guard, IP sourceguard violation IG, Dynamic ARF Impection, IPv6 RA guard, ISMP snooping (IPvrv) (querier, VLAN stacking (IDQI), INCLAS, Gommann, (IPvA/PVI), should have single panel of management via KGPW or through lesparte management tool along with requires hardware to manage the proposed ethernet switches.
290	VENDOR-14	3	81		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		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	<ol> <li>Authentication Requirements- Switch should prevent direct client- to-client traffic visibility at the layer-2 VLAN.</li> </ol>	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), BFD for OSPF for RIP (IPv4/IPv6), VRRP (IPv4/IPv6), BFD for IS-IS (IPv4/IPv6), BFD for IS-IS (IPv4/IPv6), BFD for IS-IS	Switch should support Layer 3 Policy-based routing, CSPF (IP-4/IP-6), BF1 for Gr SSP (IP-4/IP-6), RBF (IP-4/IP-6), BF1 CF Gr RFI (IP-4/IP-6), NRP (IP-4/IP-6), BF2 (IP-4/IP-6), IS-IS (IP-4/IP-6), BFD for IS-IS (IP-4/IP-6)	As RIP is legacy protocol & obsolete today and also nt asked in router, please remove it for wider ODM 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		82		22. Management - Switch should support in Ault in the should a support in Ault in the should a support of the support of the should and support VAM. And Based on the devices matching with the specified citeria devices device language and a specific VAN. Citeria: a MAC device (a parting system and user group. It bidder not supported in the system and user group. It bidder not supported in the should be assigned to a specific value of the support of the system and support. The support of the system state is the support of the system state is the system and user group. It bidder not support of intel the system and user group. It bidder not support of the system and user system and user group. It bidder not support of the system and user system and user group. It bidder not support of the system and user system and user group. It bidder not support of the system and user system and user group. It bidder not support of the system and user system and user group. It bidder not support of the system and user system and user group. It bidder not support of the system and user system and user group. It bidder not support of the system and user system and user group. It bidder not support of the system and user system and user group. It bidder not support of the system and user system and user group. It bidder not support of the system and user system and user group. It bidder not support of the system and user system and user system and user system and user system and user system and user system and user system and user system and user system and user system and user system and	Please remove the clause	This is a OEM specific feature and it 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		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 CEM don't have inbuilt functionality on their switch, they can provide additional require downave 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 participation.	No Change
298	VENDOR-14 VENDOR-14		77	2. Firewall 2. Firewall	59. Advance unknown mulware indexized on prevines and/ware (dexized on prevines and/ware (dexized on previne) and/ware provided to assure no raffic go on cloud for any kind of mulysis) and hox solution, detecting VM-aware mulware to detect and protect from virtual sandbox evading advance unknown mulware. 60. Solution should support OS type Windows 10, Windows 8.1, to	These specification is specific to OEM. Not all firewall DEM base zero day thread protection appliance. Some OEMs provide this protection in the cloud allo. We would request yourself to create a separate section for zero day protection. This will not only provide extended sendary protection coverage but also prevent vendor loday protection.		Duplicate-Refer Response at Cons. S. No 88 Duplicate-Refer Response at Cons. S. No 89
300	VENDOR-14	13	77	2. Firewall	Windows 7 Linux Andraid 61, Local malware analysis appliance should be of same OEM with 4x IGE R45 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			Duplicate-Refer Response at Cons. S. No 91
302	VENDOR-14	15	77	2. Firewall	ontimum tereformance of S. 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		2. Firewall	42 Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using Sk47-256 file-bash or signature (update to be provided in 300 second) as they transit the network and capability to do dynamic analysis on premise on purpose built-appliance	This is not functionality of Freevall but of Zeo dup thread protection. We would request you to other 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		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/application/# addresses directly exposed to internet so that appropriate action can be taken on the application/network/firewall to militate 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	/0	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 Firewall use authentication methods like RADUIS, Active Directory etc. We regestry to u banend the clause to read "Additionally, external authentication and authorization servers should be integrated with any of these RADUIS, IDAP, IDAP Secure, or TACACS protocols."		Duplicate-Refer Response at Cons. S. No 73

					RES	PONSES TO THE QUERIES RECEIVED AGAINST TEND	R No. : CCA/02(1)-2023-NIXI Dated 22-03-2023	
309	VENDOR-14	22	76	2. Firewall	25 Ability to configure, manage and monitor RoffW using CLI and GUI both without central management colution. Inliversity 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 of failure in central	Seems OFM specific clause Request you to anend the clause to "Ability to configure, manage and monitor NGPW using CLI and GLII both without central management sublicion. NGX should have CLI, in case there is any connectivity issues between tool or failure in central management tool"		Doplicate-Refer Response at Cons. 5. No 71
310	Vendor	S. No	RFP Reference Page	RFP Reference S	Content of RFP requiring		Points of clarification required	CCA/NIXI Response
311	VENDOR-15	1	74	E. Suggested Specifications: 1. Load Balancer	darification 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 or high availability. Kindly Confirm. Suggested Clause : The Load Balancer shall deliver the high availability required by modern data centres. It should upport Athier/Brave or Active / Active Accomparations. The Load Balancer shall automatically synchronize configurations in real time between the pain. The proposed device should use standard VRIP (RFC - 3338) for High Availability purpose (no proprietary protocol).	Duplicate-Refer Response at Cons. 5. 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 Tirewall 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 IB or rewrite the cookie in the response.	Duplicate-Refer Response at Cons. 5. 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 Sidng 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	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		should be scalable to 60 Obp. Aper industry standard, SS. Sising is done of 2K key NDT the 4k Key size Suggested Clause: The serve 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		ECG is the latest cipher sulte used in most the application. ECC allows to provide same or higher loved of Security with a nucls smaller key size as compared to RSA. Hence, we request to include the same. Suggested Clause : The server load balance should cater up to at least 50 K or higher SSL connections per second	Duplicate-Refer Response at Cons. S. No 8
316	VENDOR-15	6	74	E. Suggested	The sever load balancer should be		on 2K key and 25 K CPS on ECC from day 1 As per our experience, some of the vendor just to comply the clause propose break out cable	Duplicate-Refer Response at Cons. S. No 271
				Specifications: 1. Load Balancer	proposed with 8 Ports populated with 4x1G; 4x1G SFP ports and atleast 8 x 10G SFP+ SR ports from day 1		functionality (for eg. 1 x 40G can be converted to 4.10G) to support number of ports requirements. Additionality solutions should have redundant out of band management port and decidated console port of configuration and management. Suggested Gluzes : The sever load balancer should be proposed with 8 Ports populated with 8 slGE, 8 x 1G SPP ports and attest 8 x 100 SFP+5 R ports from day 1 (without Beradout Cable support) The proposed appliance should have 2 x 1G dedicated management port and 1 RMS Serial port.	
317	VENDOR-15	7	74	E. Suggested Specifications:	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,	Duplicate-Refer Response at Cons. S. No 272
							Suggested Clause : The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature that Virtualises the Device resources -including CPU, memory, network, and acceleration resources. The Hypervisor clause to intrustize the hardware should be a specialized purpose build Hypervisor and NOT a commercially available hypervisor (like XEN, VMware,XVM 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) Janagement, c) Janagement, d) Operating System The proposed device schuld support 5 Virtual Instance from Day 1 and support upto 30 Virtual tratances for future schulding on the same hardware. Appliance should have capability to use in standalone as well as virtualized mode.	
318	VENDOR-15	9	74	E. Suggested Specifications: 1. Load Balancer New Solution Re	New Gause Request		Minimum Eligibility Citeria should be mentioned to have a benchmark and healthy competition among the industry Leading Solution. Suggested Claus: 1. OKM should have OEM TAC in NDIA (since last 10 years) 2. OKM/OEM sublishing/OEM Sister Concern Company must have at least 5 successful implementation at INDIAN Government/879/Telecom Organizations in last 3 years 3. The proposed OEM should be Parent Technology OEM only (Should NOT be Whitelabled or Co burning or 3 far Myr Technology or Ogress Source on Academ Agreement 1. OKM/OEM sublishing technology or Ogress Source on Academ Agreement subsequent amondanests. 5. Null 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 NDIA for more than 15 years Cyber Saccurity is very important aspect in the entire datacenter services. As per our industry experience, Solution toud include DOE Softextion and the technologi specification is missing in the RF?	Duplicate-Refer Response at Cons. 5. No 273
320	VENDOR-15	10		New Solution Re	New Solution Request		Application and Server Foods/DDoS Attacks. 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 sequification is insign in the RP. We request to include the same, as the WAF is the major component to protect against Application	No Change.
321	VENDOR-15	11		New Solution Re	New Solution Request		8.0.8 tasks including API protection. (Opti Security is varing 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 specifications in singing in the RP. We request to include the same, as the NPS is the major component to protect against Network, Application, Server, Data center Intrusion based tasks datework.	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	Cantraction The Load Balancer shall deliver the high availability required by modern data certice. It should support Active/Passive or Active / Active HA configurations. The Load Balancer shall automatically synchronice configurations. The Load automatically flationer if any fault is detected with the primary unit		As per our experience from the fuculary, VRIP is the fundarity standard and widely used protocol for high enablishity, stated on our indestanding from the Clause, proposed solution should not use Proprietary protocol for high Availability. Kindy Confirm. Suggested Clause : The Load Balancer shall deliver the high availability required by modern data centres. It should support Active/Passive or Active / Active NA configurations. The Load Balancer shall administratily aprinorities configurations in real time between the pairs. The proposed device should use standard VRIP (REC - 2338) for High Availability purpose (no proprietary protoco).	Duplicate-Refer Response at Cons. 5. No 286
324	VENDOR-16 VENDOR-16	2		E. Suggested Specifications: 1. Load Balancer E. Suggested Specifications: 1. Load	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 The server load balancer should deliver at least 10 Gbps or higher of layer 7 throughput		Hence we request to amend this clause. Suggested Clause:	Duplicate-Refer Response at Cons. S. No 267 Duplicate-Refer Response at Cons. S. No 268
325	VENDOR-16	3	74	Specifications:	deliver at least 10 Gbps or higher		Hence we request to amend this clause.	Duplicate-Refer Response at Cons. S.

					RESP	ONSES TO THE QUERIES RECEIVED AGAINST TEND	DER 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		An end Conjugation Conjugation and a Leo Conjugation 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.	Duplicate-Refer Response at Cons. S. No 8
				bulancer	kcy non day 1		Suggested Clause : The server load balancer should cater up to at least 50 K or higher SSL connections per second	bupicate neter nesponse at cons. s. no o
328	VENDOR-16	6	74	E. Suggested Specifications:	The sever load balancer should be proposed with 8 Ports populated		on 2K kev and 25 K CPS on ECC from dav 1 As per our experience, some of the vendor just to comply the clause propose break out cable functionality (for eq. 1 × 40G can be converted to 4x10G) to support number of ports requirements.	Duplicate-Refer Response at Cons. S. No 271
				1. Load Balancer	with 4x1GE, 4x1G SFP ports and atleast 8 x 10G SFP+ SR ports from		functionality (for eg. 1 x 40c can be converted to 4x10c) to support number of ports requirements. Additionally, solution should have redundant out of band management port and dedicated console port of configuration and management.	
					day 1		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 RI45 Serial port.	
329	VENDOR-16	7	74	E. Suggested Specifications:	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,	Duplicate-Refer Response at Cons. S. No 272
				1. Load Balancer			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	
30	VENDOR-16	8	74	E. Suggested	New Clause Request		standalone as well as virtualized mode. Minimum Eligibility Criteria should be mentioned to have a benchmark and healthy competition	Duplicate-Refer Response at Cons. S. No 273
-				Specifications: 1. Load			among the Industry Leading Solution.	
				Balancer			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 CPM should be Parent Technology OEM only (Should NOT be Whitelabled or Co branding or 3rd Party Technology or Open Source or Reseller Agreement	-
							<ol> <li>OEM must be Make in INDIA Class-1 compliant as per Government MII Guidelines &amp; subsequent amendments.</li> </ol>	
							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	
331	VENDOR-16	9		New Solution R	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	Duplicate-Refer Response at Cons. S. No 319
							technical specification is missing in the RFP. We request to include the same, as the DDoS is the major component to protect against Network,	
332	VENDOR-16	10		New Solution R	New Solution Request		Application and Server Floods/DDoS Attacks. Cyber Security is very important aspect in the entire datacenter services.	Duplicate-Refer Response at Cons. S. No 320
							As per our industry experience, Solution should include Web Application Firewall for Web Application Protection and the technical specification is missing in the RFP.	
333	VENDOR-16	11		New Solution R	New Solution Request		As per our industry experience, Solution should include Web Application Firewall for Web	Duplicate-Refer Response at Cons. S. No 321
333	VENDOR-16	11		New Solution R	New Solution Request		As per our industry experience, Solution should include Web Application Firewall for Web Application Protection and the technical genicification is missing in the RFP. We request to include the same, as the WAF is the major component to protect against Application B 0B attack including AP protection. 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 in missing in the RFP.	
	VENDOR-16 Vendor VENDOR-17		Page No	New Solution R Section 2. Firewall	Clause 59. Advance unknown malware		As per our industry experience. Solution should include Web Application Forewall for Web Application Protection and the technical expectification 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 AP instruction. Code Security is very important aspect in the entire datacenter services. As per our industry experience, Solution should include Intrustry more pression Spectra Application, Server, Data centre Intrusion Integration Spectra Mer Repett to include the same, as the NFS is the major component to protect against Network, Application, Server, Data centre Intrusion based attack prevention. Carification is specific to OEM. Not all Firewall OEM have zero day threat protection	
334	Vendor		Page No 77	Section	Clause 59. Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no		As per our industry experience, Solution should include Web Application Forewall for Web Application Protection and the technical expectitation 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 AP instruction. Debr Security is very important aspect in the entire datacenter services. As per our industry experience, Solution abuild include Intrustry Intervention System for Complete Heaviork protection application. Service Data centre Intrusion based status prevention deprintion. Solution is genericity of the service application service application. Service Data centre Intrusion based status prevention. Catefication is securitic to GMA hourd IP reveal IGMA have zero day threat protection application. Service Clin for and apprecision. This will not only protected ready application. Service Clin for and application. This will only movie and application application. Service Clin for and application. This will only movie and application application. Service Clin for and application. This will not only provide extended tereday	Duplicate-Refer Response at Cons. S. No 321
334	Vendor		Page No 77	Section	Clause 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 malysis) and box solution, detecting		As per our industry experience, Solution should include Web Application Freewall for Web Application Protection and the technical experilication is missing in the RFP. We request to include the same, as the WAF is the major component to protect against Application B B attack including AP protection. Cyber Security is very important aspect in the entire datacenter services. A per our industry experience, Solution tould include intrustrion Prevention System for Complete Network protection and the technical specification is missing in the RFP. We request to include the same, as the NHFS is the major component to protect against Network, Application, Server, Data centre intrusion based attack revention. Clarification These specification is specific to OLM. Not all Freewall OLMs were day threat protection appliance. Some OLMS provide this protection in the doub also. We would request protection appliance.	Duplicate-Refer Response at Cons. S. No 321
334	Vendor		Page No 77	Section	Clause 59. Advance unknown malware analysis engine with real hardware (declicated on premises sandbox solution to be provided to assure no raffic go on cloud for any kind of		As per our industry experience. Solution should include Web Application Freewall for Web Application Protection and the technical secilitation is missing in the RFP. We request to include the same, as the WAF is the major component to protect against Application B B attack including AP lipotetican Cyber Security is very important aspect in the entire datacenter services. A per our industry experience, Solution should include intrusion Prevention System for Complete Network protection and the technical specification in missing in the RFP. We request to include the same, as the NMFS is the major component to protect against Network, Application, Server, Data center intrusion based attack greenetion. Clarification These separate section for zore day protection. In the audia data. We would request yourself or create a separate section for zor day protection in the audia data. We would request zero day protection coverage but also prevent worked toxicin your and a allow doub baset zero day protection.	Duplicate-Refer Response at Cons. S. No 321
334	Vendor	Sno 1	Page No 77 77	Section	Clause 59. Also engine with real hardware (deficited on premises sambox subino to be provided to assure no nurfice go on cloud for any kind of analysis) and box colorion, detecting protect from virtual sambox cualing advance minknown malware. 40. Solution should support OS type Windows 10, Windows 8.1.		As per our industry experience. Solution should include Web Application Freewall for Web Application Protection and the technical secilitation is missing in the RFP. We request to include the same, as the WAF is the major component to protect against Application B B attack including AP lipotetican Cyber Security is very important aspect in the entire datacenter services. A per our industry experience, Solution should include intrusion Prevention System for Complete Network protection and the technical specification in missing in the RFP. We request to include the same, as the NMFS is the major component to protect against Network, Application, Server, Data center intrusion based attack greenetion. Clarification These separate section for zore day protection. In the audia data. We would request yourself or create a separate section for zor day protection in the audia data. We would request zero day protection coverage but also prevent worked toxicin your and a allow doub baset zero day protection.	Duplicate-Refer Response at Cons. S. No 321
<b>334</b> 335	Vendor VENDOR-17	Sno 1	77	Section 2. Firewall	Clause 59. Advance unknown mulware clause and the second		As per our industry experience. Solution should include Web Application Freewall for Web Application Protection and the technical secilitation is missing in the RFP. We request to include the same, as the WAF is the major component to protect against Application B B attack including AP lipotetican Cyber Security is very important aspect in the entire datacenter services. A per our industry experience, Solution should include intrusion Prevention System for Complete Network protection and the technical specification in missing in the RFP. We request to include the same, as the NMFS is the major component to protect against Network, Application, Server, Data center intrusion based attack greenetion. Clarification These separate section for zore day protection. In the audia data. We would request yourself or create a separate section for zor day protection in the audia data. We would request zero day protection coverage but also prevent worked toxicin your and a allow doub baset zero day protection.	Duplicate-Refer Response at Cons. 5. No 321 CCA/NIXI Response No Change
<b>334</b> 335 336	Vendor VENDOR-17 VENDOR-17	<u>Sno</u> 1 2	77	Section 2. Firewall 2. Firewall	So Advance unknown malware malysis engine with real hardware malysis engine with real hardware within to he growed in assume no unfile go on cloud for any kind of analysis) and how solution, detecting yotect from virtual sandsoc evalues advance unknown malware. O Solution should support OS type Windows 10, Windows 8, 1, Windows 10, Windows 8, 19		As per our industry experience. Solution should include Web Application Freewall for Web Application Protection and the technical secilitation is missing in the RFP. We request to include the same, as the WAF is the major component to protect against Application B B attack including AP lipotetican Cyber Security is very important aspect in the entire datacenter services. A per our industry experience, Solution should include intrusion Prevention System for Complete Network protection and the technical specification in missing in the RFP. We request to include the same, as the NMFS is the major component to protect against Network, Application, Server, Data center intrusion based attack greenetion. Clarification These separate section for zore day protection. In the audia data. We would request yourself or create a separate section for zor day protection in the audia data. We would request zero day protection coverage but also prevent worked toxicin your and a allow doub baset zero day protection.	Duplicate-Refer Response at Cons. 5. No 321 CCA.NEXE Response No Change Duplicate-Refer Response at Cons. 5. No 89
<b>334</b> 335	Vendor VENDOR-17 VENDOR-17	<u>Sno</u> 1 2	77	Section 2. Firewall 2. Firewall	Course     So Advance unknown malware:     So Advance unknown en unknown     course and the source of the source unknown unknown.     Source unknown unknown etc.     Source		As per our industry experience. Solution should include Web Application Freewall for Web Application Protection and the technical secilitation is missing in the RFP. We request to include the same, as the WAF is the major component to protect against Application B B attack including AP lipotetican Cyber Security is very important aspect in the entire datacenter services. A per our industry experience, Solution should include intrusion Prevention System for Complete Network protection and the technical specification in missing in the RFP. We request to include the same, as the NMFS is the major component to protect against Network, Application, Server, Data center intrusion based attack greenetion. Clarification These separate section for zore day protection. In the audia data. We would request yourself or create a separate section for zor day protection in the audia data. We would request zero day protection coverage but also prevent worked toxicin your and a allow doub baset zero day protection.	Duplicate-Refer Response at Cons. 5. No 321 CCA.NUX Response No Change Duplicate-Refer Response at Cons. 5. No 89
334 335 336 337	Vendor VENDOR-17 VENDOR-17	<u>Sno</u> 1 2	77	Section 2. Firewall 2. Firewall	Sa Advance unknown malware malysis engine with real hardware malysis engine with real hardware with real hardware unknown in the second second second traffic go on cloud for any kind of analysis) and hose solution, detecting devine unknown malware. Windows 1, Uma, Android, G. Solution should support CS types Windows 10, Windows 8, 11, windows 7, Linux, Android, 61, Local malware analysis appliance should be of same CMS with 4 VG RJS firstfree and minimum encode of the included from day 1 Ca, Solution should have former to anamally configure on what file types will run in which needfie VII for spaces will run in secific work for the space will run in secific work for the space will run in secific work for the space of the space will the space will run in secific work for an analyze outfigure on what file types will run in secific work for the space of the space will run in secific work for the space of the space will run in the space will run in secific work for the space of the space will run in the space will run in secific work for the space of the space will run in the space will run in secific work for the space of the space will run in the space will run in secific with for the space of the space will run in the space space will run in the space will run in the space will run in the		As per our industry experience. Solution should include Web Application Freewall for Web Application Protection and the technical secilitation is missing in the RFP. We request to include the same, as the WAF is the major component to protect against Application B B attack including AP lipotetican Cyber Security is very important aspect in the entire datacenter services. A per our industry experience, Solution should include intrusion Prevention System for Complete Network protection and the technical specification in missing in the RFP. We request to include the same, as the NMFS is the major component to protect against Network, Application, Server, Data center intrusion based attack greenetion. Clarification These separate section for zore day protection. In the audia data. We would request yourself or create a separate section for zor day protection in the audia data. We would request zero day protection coverage but also prevent worked toxicin your and a allow doub baset zero day protection.	Duplicate-Refer Response at Cons. 5. No 321 CCA.NUX Response No Change Duplicate-Refer Response at Cons. 5. No 89
334 335 336 337	Vendor VENDOR-17 VENDOR-17 VENDOR-17	<b>Sno</b> 1 2 3	77 77 77	Section 2. Firewall 2. Firewall 2. Firewall 2. Firewall	Clause So Advance sunknown malware refelestated on premiers sambox whiten to be provided in source nor traffic groun cloud for any kind of analysis) and box solution, detecting VM searer malware to detect and protect from virtual sambox estaing abase entropy of the sambox of the sambox protect from virtual sambox estaing abase and the sambox of the sambox of 0. Solution abased sambox 61. Lock markers AL VM specific VM searer AL VMA should be included from day 1 C. Solution abase for W with the searer seares 6VMA or more. ALI VMA should be included from day 1 C. Solution abase for W with the searer of VMA or more. ALI VMA should be included from day 1 C. Solution abase for W with the searer of VMA or more. ALI VMA will run in which specific VM for optimal performance.		As per our industry experience. Solution should include Web Application Freewall for Web Application Protection and the technical secilitation is missing in the RFP. We request to include the same, as the WAF is the major component to protect against Application B B attack including AP lipotetican Cyber Security is very important aspect in the entire datacenter services. A per our industry experience, Solution should include intrusion Prevention System for Complete Network protection and the technical specification in missing in the RFP. We request to include the same, as the NMFS is the major component to protect against Network, Application, Server, Data center intrusion based attack greenetion. Clarification These separate section for zore day protection. In the audia data. We would request yourself or create a separate section for zor day protection in the audia data. We would request zero day protection coverage but also prevent worked toxicin your and a allow doub baset zero day protection.	Duplicate-Refer Response at Cons. 5. No 321 CCA/NIXI Response CCA/NIXI Response CCA/NIXI Response Duplicate-Refer Response at Cons. 5. No 89 Duplicate-Refer Response at Cons. 5. No 90
334 335 336	Vendor VENDOR-17 VENDOR-17 VENDOR-17	<b>Sno</b> 1 2 3	77 77 77 77 77 77	Section           2. Firewall           2. Firewall           2. Firewall           2. Firewall           2. Firewall	Clause     So. Advance unknown mulware     mulyins engine with real hardware     mulyins engine with real hardware     mulyins on the provided in assume no     traffic grounded in assume no     mulyins) and how solution, detecting     VM-aware mulware to detect and     protect from virtual sandhore example     Mondows 10, Windows 8, 1,     VM-aware mulware to detect and     protect from virtual sandhore example     Mondows 10, Windows 8, 1,     VM-aware, Markada Markada Markada     Solution though support OS type     Windows 1, Burkada Markada Markada     Solution though support OS type     Mondows 10, Windows 8, 1,     Solution though support OS type     more, All VMs     hould be included from day 1     C. Solution should have fature to     munually configure on what file types     will run a which performance.     O. Local Maharam epilence chandle     how alguing frameware     Mondows 10, Lince Maharam epilence though and or to     multil feature to send alset over     multil feature to send alset over     multil of the send malware point		As per our industry experience. Solution should include Web Application Freewall for Web Application Protection and the technical secilitation is missing in the RFP. We request to include the same, as the WAF is the major component to protect against Application B B attack including AP lipotetican Cyber Security is very important aspect in the entire datacenter services. A per our industry experience, Solution should include intrusion Prevention System for Complete Network protection and the technical specification in missing in the RFP. We request to include the same, as the NMFS is the major component to protect against Network, Application, Server, Data center intrusion based attack greenetion. Clarification These separate section for zore day protection. In the audia data. We would request yourself or create a separate section for zor day protection in the audia data. We would request zero day protection coverage but also prevent worked toxicin your and a allow doub baset zero day protection.	Duplicate-Refer Response at Cons. 5. No 321 CCA/NIXI Response No Change Duplicate-Refer Response at Cons. 5. No 89 Duplicate-Refer Response at Cons. 5. No 90 Duplicate-Refer Response at Cons. 5. No 91
334 335 336 337	Vendor VENDOR-17 VENDOR-17 VENDOR-17	<b>Sno</b> 1 2 3	77 77 77 77 77 77	Section           2. Firewall           2. Firewall           2. Firewall           2. Firewall           2. Firewall	Classe     Solution     So		As per our industry experience. Solution should include Web Application Freewall for Web Application Protection and the technical secilitation is missing in the RFP. We request to include the same, as the WAF is the major component to protect against Application B B attack including AP lipotetican Cyber Security is very important aspect in the entire datacenter services. A per our industry experience, Solution should include intrusion Prevention System for Complete Network protection and the technical specification in missing in the RFP. We request to include the same, as the NMFS is the major component to protect against Network, Application, Server, Data center intrusion based attack greenetion. Clarification These separate section for zore day protection. In the audia data. We would request yourself or create a separate section for zor day protection in the audia data. We would request zero day protection coverage but also prevent worked toxicin your and a allow doub baset zero day protection.	Duplicate-Refer Response at Cons. 5. No 321 CCA/NNX Response No Change Duplicate-Refer Response at Cons. 5. No 89 Duplicate-Refer Response at Cons. 5. No 90 Duplicate-Refer Response at Cons. 5. No 91
134 135 136 137 138	Vendor VENDOR-17 VENDOR-17 VENDOR-17	<b>Sno</b> 1 2 3	77 77 77 77 77 77	Section           2. Firewall           2. Firewall           2. Firewall           2. Firewall           2. Firewall	Classe     Solution control mathematic     Solution to the provided on assure no     traffic grant control of the solution of the provided on assure motivation     to the provided on assure motivation of the provided on assure mathematic     Solution of the provided on assure and assure and assure and assure to a detect and     advance mathematic nucleon assure. A solution of the provided on a solution of the provided		As per our industry experience. Solution should include Web Application Freewall for Web Application Protection and the technical secilitation is missing in the RFP. We request to include the same, as the WAF is the major component to protect against Application B B attack including AP lipotetican Cyber Security is very important aspect in the entire datacenter services. A per our industry experience, Solution should include intrusion Prevention System for Complete Network protection and the technical specification in missing in the RFP. We request to include the same, as the NMFS is the major component to protect against Network, Application, Server, Data center intrusion based attack greenetion. Clarification These separate section for zore day protection. In the audia data. We would request yourself or create a separate section for zor day protection in the audia data. We would request zero day protection coverage but also prevent worked toxicin your and a allow doub baset zero day protection.	Duplicate-Refer Response at Cons. S. No 321 CCA/NXX Response CCA/NXX Response CCA/NXX Response Duplicate-Refer Response at Cons. S. No 89 Duplicate-Refer Response at Cons. S. No 90 Duplicate-Refer Response at Cons. S. No 91
3334 3335 3336 3337 3338 3339 340	Vendor VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	2 3 4	77 77 77 77 77 77	Section 2. Firewall 2. Firewall 2. Firewall 2. Firewall 2. Firewall	Classel     Sin Advances tankown malweit     Sin Advance tankown to detect and     protect from virtual sandhox evading     advance unknown malware.     Sin Advances Si.     Windows Si.     Windows Si.     Windows Si.     Sin Advances Si.     Sin Advances Si.     Sin Advances tankown malware.     Advances malysis appliance     doubt for a same ODM with N i GEI     forughtput of SOM for malysis appliance     doubt for a same ODM with N i GEI     forughtput of SOM for more. All VMs     doubt be included from day 1     C.     Solution should have feature to     manually configure on what file types     will run in which specific VM for     angulation should be notified to     for Losed advances.     Sin Advances		As per our industry experience, Solution should include Web Application Prevention for Web Application Protection and the technical secification is missing in the RFP. We request to include the same, as the WAF is the major component to protect against Application Code Security is very important aspect in the entire datacenter services. As per our industry experience, Solution build include Internor Prevention System for Compate Network protection and the technical specification in missing in the RFP. We request to include the same, as the WAF is the major component to protect against Network, Application, error, Data centre innusion based attab. Reventers, Application, error, Data centre innusion based attab. Reventers, appliance, Some OEMs provide this protection. This will not work only index error any protection coverage but also prevent vendor lockin or you can also allow cloud based zero day protection.	Duplicate Refer Response at Cons. S. No 321 CCA/NUX Response No Change Duplicate Refer Response at Cons. S. No 89 Duplicate Refer Response at Cons. S. No 90 Duplicate Refer Response at Cons. S. No 91 Duplicate Refer Response at Cons. S. No 91
3334 3335 3336 3337 3338 3339 340 340	Vendor VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	5 5 6	77 77 77 77 77 77 77	Section           2. Firewall           2. Firewall           2. Firewall           2. Firewall           2. Firewall	Clause     So Advance unknown malwave     of Advance unknown malwave     of Advance unknown malwave     idealization premiers sambox     white the advance of the adva		As per or industry experience, Solution should include Web Application Freewall 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 Code Security is very important aspect in the entire datacenter services. As per our industry depretinese, Solution Should include Intrum Prevention System for Complete Heaview functions and the technical specification is missing in the RFP. Solution Security is very important aspect in the entire datacenter services. As per our industry depretinese, Solution Data centre Intrusion Interesting Systems and the technical specification is missing in the RFP. These specification is specification is missing in the RFP. Application Security Data centre Intrusion based attack prevention. These specification is specification is the protection in the data data with protection appliance. Some OEMs provide this protection in the doub also. We would request protection appliance. Some OEMs provide this protection. This will convirg protection exceeds and the second protection appliance. Some OEMs provide this protection. The will on evolve provide second zero day protection coverage but also prevent vendor lockin or you can also allow cloud based zero day protection.	Duplicate-Refer Response at Cons. 5. No 321 CCA/NXI Response No Change Duplicate-Refer Response at Cons. 5. No 89 Duplicate-Refer Response at Cons. 5. No 90 Duplicate-Refer Response at Cons. 5. No 91 Duplicate-Refer Response at Cons. 5. No 91 No Change No Change
3334 3335 3336 3337 3338 3339 340 340	VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	5 5 6 7	77 77 77 77 77 77 77 77	Section           2. Firewall	Obstance sensores malwares     So, A-denaces sensores malwares     disdicated on premises sandhose     adulton to be provided to assure no     marking you chood for any kind of     adulton to be provided to assure no     more to detect and     protect from virtual sandhose vanding     advance unknown malware.     Of. Solution should support OS type     Windows 11, Windows 81, 1     Windows 71, Jama, Andreid     D. Local malware analysis applicate     Of. Jocubar Malware analysis applicate     Advance malysis on the same sensore analysis     applicate analysis applicate     Advance malysis on what file types     advance malysis on policitate     Advance malysis applicate     Advance analysis on the same policy     advance malysis on the same policy     advance malysis     applicate the same policy     advance malysis     advance     advance malysis     advance     advance malysis     advance malysis     advance malysis     advance		As per or industry experience, Solution should include Web Application Freewall for Web Application Protection and the technical expericition is missing in the IRP. We request to include the same, is the WAF is the major component to protect against Application Color Society is very important aspect in the entire datacenter services. As per our industry and the technical period and interaction in the SPP. We request to include the same, as the NPF's the major component to protect against Network, Application, Server, Data centre intrusion based attack prevention. Calification is specific to ORA. Not all Firewall ORA have zero day threat protection application. Server, Data centre intrusion based attack prevention. Calification is specific to ORA. Not all Firewall ORA have zero day threat protection application. Server, Data centre intrusion based attack prevention. Calification is specific to ORA. Not all Firewall ORA have zero day threat protection application. Server, Data centre intrusion based attack prevention. Calification is prevent to be able prevent vender locid in or you can also allow doub based zero day protection. Coverage but also prevent vender locid or you can also allow doub based zero day protection.	Duplicate-Refer Response at Cons. S. No 321 CCA/NXI Response No Change Duplicate-Refer Response at Cons. S. No 89 Duplicate-Refer Response at Cons. S. No 90 Duplicate-Refer Response at Cons. S. No 91 Duplicate-Refer Response at Cons. S. No 302 No Change No Change
134 135 136 137 138 139 140	VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	5 5 6 7	77 77 77 77 77 77 77 77	Section           2. Firewall	Clause     St. Advance tanknown malware     St. Advance tanknown malware     St. Advance tanknown malware     St. Advance tanknown malware     St. Advance tanknown contraction to the provided to assure to     and the state of the stat		As per or industry experience, Solution should include Web Application Freewall 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 Code Security is very important aspect in the entire datacenter services. As per our industry depretinese, Solution Should include Intrum Prevention System for Complete Heaview functions and the technical specification is missing in the RFP. Solution Security is very important aspect in the entire datacenter services. As per our industry depretinese, Solution Data centre Intrusion Interesting Systems and the technical specification is missing in the RFP. These specification is specification is missing in the RFP. Application Security Data centre Intrusion based attack prevention. These specification is specification is the protection in the data data with protection appliance. Some OEMs provide this protection in the doub also. We would request protection appliance. Some OEMs provide this protection. This will convirg protection exceed by these protection appliance. Some OEMs provide this protection. This will convirg protection appliance are protection coverage but also prevent vendor lockin or you can also allow cloud based zero day protection.	Duplicate-Refer Response at Cons. S. No 321 CCA/NXI Response No Change Duplicate-Refer Response at Cons. S. No 89 Duplicate-Refer Response at Cons. S. No 90 Duplicate-Refer Response at Cons. S. No 91 Duplicate-Refer Response at Cons. S. No 302 No Change No Change
134 135 136 137 138 139 140	VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	5 5 6 7	77 77 77 77 77 77 77 77	Section           2. Firewall	Clause     Standard and the second seco		As per or industry experience, Solution should include Web Application Freewall 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 Code Security is very important aspect in the entire datacenter services. As per our industry depretinese, Solution Should include Intrum Prevention System for Complete Heaview functions and the technical specification is missing in the RFP. Solution Security is very important aspect in the entire datacenter services. As per our industry depretinese, Solution Data centre Intrusion Interesting Systems and the technical specification is missing in the RFP. These specification is specification is missing in the RFP. Application Security Data centre Intrusion based attack prevention. These specification is specification is the protection in the data data with protection appliance. Some OEMs provide this protection in the doub also. We would request protection appliance. Some OEMs provide this protection. This will convirg protection exceed by these protection appliance. Some OEMs provide this protection. This will convirg protection appliance are protection coverage but also prevent vendor lockin or you can also allow cloud based zero day protection.	Duplicate-Refer Response at Cons. S. No 321 CCL/INIX Response No Change Duplicate-Refer Response at Cons. S. No 89 Duplicate-Refer Response at Cons. S. No 90 Duplicate-Refer Response at Cons. S. No 91 Duplicate-Refer Response at Cons. S. No 91 Duplicate-Refer Response at Cons. S. No 92 No Change No Change
3334 3335 3336 3337 3338 3339 340 340	VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	5 5 6 7	77 77 77 77 77 77 77 77	Section           2. Firewall	Database     Single Advances tankown malweige     Single Advances tankown malweige     diodicated on premises sambox     advances tankown advances     diodicated on premises sambox     advance tankown to discet and     protect from virtual sambox evading     advance tankown malware.     diodicated on a server on     diodicate advances     diodicate advances     diodicate advances     diodicated     diodicate     d		As per or industry experience, Solution should include Web Application Freewall 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 Code Security is very important aspect in the entire datacenter services. As per our industry depretinese, Solution Should include Intrum Prevention System for Complete Heaview functions and the technical specification is missing in the RFP. Solution Security is very important aspect in the entire datacenter services. As per our industry depretinese, Solution Data centre Intrusion Interesting Systems and the technical specification is missing in the RFP. These specification is specification is missing in the RFP. Application Security Data centre Intrusion based attack prevention. These specification is specification is the protection in the data data with protection appliance. Some OEMs provide this protection in the doub also. We would request protection appliance. Some OEMs provide this protection. This will convirg protection exceed by these protection appliance. Some OEMs provide this protection. This will convirg protection appliance are protection coverage but also prevent vendor lockin or you can also allow cloud based zero day protection.	Duplicate-Refer Response at Cons. S. No 321 CCA/NXI Response No Change Duplicate-Refer Response at Cons. S. No 89 Duplicate-Refer Response at Cons. S. No 90 Duplicate-Refer Response at Cons. S. No 91 Duplicate-Refer Response at Cons. S. No 302 No Change No Change
134 135 136 137 138 138 139 140 141 142	VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	5 5 6 7	77 77 77 77 77 77 77 76	Section           2. Firewall	Classe         29. Advances tankown malware         29. Advances tankown malware         20. Advances tankown advances         20. Advances tankown advances         20. Advances tankown advances         20. Advances tankown advances         20. Soliton to the growth advance         20. Soliton advances         20. Soliton         20. S		As per or industry experience, Solution should include Web Application Freewall 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 Code Security is very important aspect in the entire datacenter services. As per our industry depretinese, Solution Should include Intrum Prevention System for Complete Heaview functions and the technical specification is missing in the RFP. Solution Security is very important aspect in the entire datacenter services. As per our industry depretinese, Solution Data centre Intrusion Interesting Systems and the technical specification is missing in the RFP. These specification is specification is missing in the RFP. Application Security Data centre Intrusion based attack prevention. These specification is specification is the protection in the data data with protection appliance. Some OEMs provide this protection in the doub also. We would request protection appliance. Some OEMs provide this protection. This will convirg protection exceed by these protection appliance. Some OEMs provide this protection. This will convirg protection appliance are protection coverage but also prevent vendor lockin or you can also allow cloud based zero day protection.	Duplicate-Refer Response at Cons. S. No 321 CCA/NXI Response No Change Duplicate-Refer Response at Cons. S. No 89 Duplicate-Refer Response at Cons. S. No 90 Duplicate-Refer Response at Cons. S. No 91 Duplicate-Refer Response at Cons. S. No 302 No Change No Change
334 3335 3336 3337 3338 3338 3339 340 341 3442	VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	5 2 3 4 4 5 7 8	77 77 77 77 77 77 77 76	Section           2. Firewall           2. Firewall	Classe     Standard Constraints and Second Sec		As per our industry experience, Solution should include Web Application Prevention Specification instead in the RFP. We request to include the same, as the WAF is the major component to protect against Application Code Statuski include mark aspect in the entire datacenter services. As per our industry experience, Solution abuild include Intromo Prevention Specification Simony application Protection abuild include Intromo Prevention Specification application Specification as a the pill of the same process and per our industry depresses, Solution abuild include Intromo Prevention Specification application, Server Data centre Intrusion based attack prevention. Califications is specific to GMA Not all Firewall GMA have area day threat protection application. Server Data centre Intrusion based attack prevention. These specification is specific to GMA Not all Firewall GMA have area day threat protection application. Server CIMA provide this protection. This will not only provide extended zeroday protection coverage but also prevent vendor lockin or you can also allow cloud based zerod day protection. We understand that the bidder has to provide sequent protection. We would request you to either move it the said section or remove the clause. This is not part of network Tirewall. We would request to have a separate section for this requirement. This is not functionality of Firewall bud 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. 5. No 321 CCA/NXI Response No Change Duplicate-Refer Response at Cons. 5. No 89 Duplicate-Refer Response at Cons. 5. No 90 Duplicate-Refer Response at Cons. 5. No 91 Duplicate-Refer Response at Cons. 5. No 302 No Change No Change
334 335 336 337 338 338 339 340 341 342	VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	5 6 7 8 9	77 77 77 77 77 77 77 76 78 78	Section       2. Firewall	Clause     Standard and the second and a second and a second second a		As per or industry experience, Solution should include Web Application Freewall for Web Application Protection and the technical expectition is missing in the IRP. We request to include the same, is the WAF is the major component to protect against Application Code Security is very important aspect in the entire datacenter services. As per our industry and the solution is simplication in the important protection in the complex the leavest protection application Protect against the IRP. These specification is signific to CMA Net all Freewall CMA have zero day threat protection application. Security Data server intrusion based attack prevention. <b>Cardination</b> Security Data Security Intrusion based attack prevention. <b>Cardination</b> Security Data Security Protection in the data data security as a protection. This is not part of network firewall. We would request to have a separate section for this requirement We understand that the bidder has to provide separate solution independent of Firewall. 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. Not surve what "university" means here. Moreover, it this clause is not functionality of firewall. We request you to remove the dause.	Duplicate Refer Response at Cons. 5. No 321 CCA.NUM Response No Change Duplicate Refer Response at Cons. 5. No 89 Duplicate Refer Response at Cons. 5. No 90 Duplicate Refer Response at Cons. 5. No 90 Duplicate Refer Response at Cons. 5. No 302 Duplicate Refer Response at Cons. 5. No 302 Duplicate Refer Response at Cons. 5. No 302 No Change Duplicate Refer Response at Cons. 5. No 78
334 335 336 337	VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	5 2 3 4 4 5 7 8	77 77 77 77 77 77 77 76 78 78	Section           2. Firewall           2. Firewall	Clause     Standard and the second and a second and a second and a second and a second second a second second a second second a second second a second a second a second a second a second a second		As per or inductly experience, Solution should include Web Application Freewall for Web Application Protection and the technical experification is missing in the IRP. We request to include the same, is the WAF is the major component to protect against Application Color Solutions including Alformatical Color Solutions including Alformatical in the Solution is specification in single in the IRP. We request to include the same, as the NBF's the major component to protect against Network, Application, Server Data centre infrusion based attack prevention. <b>Calification</b> is specific to ORA. Not all Firewall ORA have zero day threat protection application. Server Data centre infrusion based attack prevention. <b>Calification</b> is specific to ORA. Not all Firewall ORA have zero day threat protection application. Server Data centre infrusion based attack prevention. <b>Calification</b> Server Color and a specific to ORA. Not all Firewall ORA have zero day threat protection application. Server DAta centre infrusion based attack prevention. <b>Calification</b> Server Color and a specific to ORA. Not all Firewall ORA have zero day threat protection application. Server DAta provide this protection. This will not only provide extended zerod by protection. This is not part of network firewall. We would request to have a separate section for this requirement. We would based that the bidder has to provide separate solution independent of Firewall. This is not part of network firewall. We would request protection. We would request you to either move it the said section or remove the clause. Not suze what "university" means here. Moreover, it this clause is not functionality of firewall. We	Duplicate Refer Response at Cons. 5. No 321 CCA.NUM Response No Change Duplicate Refer Response at Cons. 5. No 89 Duplicate Refer Response at Cons. 5. No 90 Duplicate Refer Response at Cons. 5. No 90 Duplicate Refer Response at Cons. 5. No 302 Duplicate Refer Response at Cons. 5. No 302 Duplicate Refer Response at Cons. 5. No 302 No Change Duplicate Refer Response at Cons. 5. No 78
334 335 336 337 338 339 340 341 342	VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	5 6 7 8 9	77 77 77 77 77 77 77 76 78 78	Section       2. Firewall	Oracle     Solution     So		As per or inductly experience, Solution should include Web Application Freewall for Web Application Protection and the technical experitation is missing in the IRP. We request to include the same, is the WAF is the major component to protect application application protecting All innerection Color Society is very important aspect in the Prove and Color Society and Color and the technical peritation is insigned in the Pro- magnetization aspectication is insigned in the Pro- Mer request to include the same, as the NPFs to the major component to protect application Application. Specific to ORA. Not all Firewall ORA have zero day threat protection application. Server, Data centre infrusion based attack prevention. Calification is specific to ORA. Not all Firewall ORA have zero day threat protection application. Server, Data centre infrusion based attack prevention. Calification application. Server, Data centre infrusion based attack prevention. Calification application. Server, Data centre infrusion the Data on the product application application. Server, Data centre infrusion based attack prevention. Calification application coverage but also prevent vendor lockin or you can also allow doud based zero day protection. This is not part of network firewall. We would request to have a separate section for this cognition coverage but also prevent vendor lockin or you can also allow doud based zero day protection. We understand that the blidder has to provide separate solution independent of firewall. 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 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. 5. No 321 CCA.NEXE Response No Change Duplicate Refer Response at Cons. 5. No 90 Duplicate Refer Response at Cons. 5. No 90 Duplicate Refer Response at Cons. 5. No 91 Duplicate Refer Response at Cons. 5. No 92 Duplicate Refer Response at Cons. 5. No 78
334 335 336 337 338 339 340 341 342	VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	5 6 7 8 9	77 77 77 77 77 77 77 76 78 78	Section       2. Firewall	Classe     Systematic temperature malveser     Systematic temperature malveser     Systematic temperature malveser     Systematic temperature malveser     Systematic temperature		As per or inductly experience, Solution should include Web Application Freewall for Web Application Protection and the technical experitation is missing in the IRP. We request to include the same, is the WAF is the major component to protect application application protecting All innerection Color Society is very important aspect in the Prove and Color Society and Color and the technical peritation is insigned in the Pro- magnetization aspectication is insigned in the Pro- Mer request to include the same, as the NPFs to the major component to protect application Application. Specific to ORA. Not all Firewall ORA have zero day threat protection application. Server, Data centre infrusion based attack prevention. Calification is specific to ORA. Not all Firewall ORA have zero day threat protection application. Server, Data centre infrusion based attack prevention. Calification application. Server, Data centre infrusion based attack prevention. Calification application. Server, Data centre infrusion the Data on the product application application. Server, Data centre infrusion based attack prevention. Calification application coverage but also prevent vendor lockin or you can also allow doud based zero day protection. This is not part of network firewall. We would request to have a separate section for this cognition coverage but also prevent vendor lockin or you can also allow doud based zero day protection. We understand that the blidder has to provide separate solution independent of firewall. 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 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. 5. No 321  CCA/NUX Response No Change Duplicate-Refer Response at Cons. 5. No 89 Duplicate-Refer Response at Cons. 5. No 90 Duplicate-Refer Response at Cons. 5. No 91 Duplicate-Refer Response at Cons. 5. No 302 No Change No Change Duplicate-Refer Response at Cons. 5. No 78 Duplicate-Refer Response at Cons. 5. No 78
3334 3335 3336 3337 3338 3338 3339 340 341 342 342	VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	5 6 7 8 9	77 77 77 77 77 77 77 76 78 78	Section       2. Firewall	Classe     So, Anascenge with real hardware     So, Anascenge with real hardware     idealized on premises sualibox     solution to be provided to assure no     traffic go on cloud for any kind of     any have engines on advances. Network     protect from virtual suelbox coulding     share malyous malyous.     Construct a support of type     Mindows 10, Windows 8.1,     Windows 7, Linux, Android,     Solution should support OS type     Windows 7, Linux, Android,     Solution should support OS type     Windows 7, Linux, Android,     Solution should support OS type     Windows 7, Linux, Android,     Solution should support OS type     Windows 10, Windows 8.1,     Windows 7, Linux, Android,     Solution should be proved from days     layer any segment of the state of the state of the state     hould be included on adays     The provides markets     the state of the state of the state of the state     hould be included by     with run in which specific VM for     equinal performance.     Solution should be modelle in adays     Solution adays appliance theory     add the state of the state of the state of the state     detected malware by     here inshift frateware, bit which is the state     detected malware by     here inshift frateware.     Solution frameware     detected malware by     hereinshift frateware by     instate the state of the state of the state of the state     detection of malware by     hereinshift frateware.     Solution frameware the edisposition of malware by     hereinshift frateware by     hereinshift frateware by     instate the stateware of the statewa		As per or inductly experience, Solution should include Web Application Freewall for Web Application Protection and the technical expectition is missing in the IRP. We request to include the same, is the WAF is the major component to protect application protection. Solution and the technical performance of the solution of the solution of Complete Helenoity potention and the technical performance of the solution of the solution of the solution of Complete Helenoity potention and the technical performance of the solution of the soluti	Duplicate Refer Response at Cons. 5. No 321 CCA.NEXE Response No Change Duplicate Refer Response at Cons. 5. No 90 Duplicate Refer Response at Cons. 5. No 90 Duplicate Refer Response at Cons. 5. No 91 Duplicate Refer Response at Cons. 5. No 92 Duplicate Refer Response at Cons. 5. No 78
334 335 336 337 338 338 339 340 341 342	VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	5 6 7 8 9	77 77 77 77 77 77 77 76 78 78	Section       2. Firewall	Clause     Standard and the second and a second and a second		As per or inductly experience, Solution should include Web Application Freewall for Web Application Protection and the technical expectition is missing in the IRP. We request to include the same, is the WAF is the major component to protect application protection. Solution and the technical performance of the solution of the solution of Complete Helenoity potention and the technical performance of the solution of the solution of the solution of Complete Helenoity potention and the technical performance of the solution of the soluti	Duplicate Refer Response at Cons. S. No 321  CCA/NUX Response No Change Duplicate Refer Response at Cons. S. No 89 Duplicate Refer Response at Cons. S. No 90 Duplicate Refer Response at Cons. S. No 90 Duplicate Refer Response at Cons. S. No 91 Duplicate Refer Response at Cons. S. No 73 Duplicate Refer Response at Cons. S. No 78 Duplicate Refer Response at Cons. S. No 78
134 135 136 137 138 139 140 141 142	VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	5 6 7 8 9	77 77 77 77 77 77 77 76 78 78	Section       2. Firewall	Classe     Solution     So		As per or inductly experience, Solution should include Web Application Freewall for Web Application Protection and the technical expectition is missing in the IRP. We request to include the same, is the WAF is the major component to protect application protection. Solution and the technical performance of the solution of the solution of Complete Helenoity potention and the technical performance of the solution of the solution of the solution of Complete Helenoity potention and the technical performance of the solution of the soluti	Duplicate-Refer Response at Cons. 5. No 321  CCA/NUX Response No Change Duplicate-Refer Response at Cons. 5. No 89 Duplicate-Refer Response at Cons. 5. No 90 Duplicate-Refer Response at Cons. 5. No 91 Duplicate-Refer Response at Cons. 5. No 302 No Change No Change Duplicate-Refer Response at Cons. 5. No 78 Duplicate-Refer Response at Cons. 5. No 78
334 335 336 337 338 338 339 340 341 342	VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17 VENDOR-17	5 6 7 8 9	77 77 77 77 77 77 77 77 77 78 78 76	Section       2. Firewall	Classe     Solution     So		As per or inductly experience, Solution should include Web Application Freewall for Web Application Protection and the technical expectition is missing in the IRP. We request to include the same, is the WAF is the major component to protect application protection. Solution and the technical performance of the solution of the solution of Complete Helenoity potention and the technical performance of the solution of the solution of the solution of Complete Helenoity potention and the technical performance of the solution of the soluti	Duplicate-Refer Response at Cons. 5. No 321  CCA/NUX Response No Change Duplicate-Refer Response at Cons. 5. No 89 Duplicate-Refer Response at Cons. 5. No 90 Duplicate-Refer Response at Cons. 5. No 91 Duplicate-Refer Response at Cons. 5. No 302 No Change No Change Duplicate-Refer Response at Cons. 5. No 78 Duplicate-Refer Response at Cons. 5. No 78

	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 KMW using CLI and GUI both without central management studioti. University would like to have full feature parity of centralised management tool on the Next Generation Freewall itself, incas there is any control of the studies of the studies of the Next Generation management tool of failure in central management tool	Seems OEM specific clause Request you to amend the clause to <sup>2</sup> Ability to configure, manage and montor WGW using (21 and GU lito thin whose central management solution.NIX 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 ***									