Sr. No.	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	Additional Remarks (if any)	Response
1	Section 9 - Technical Specifications	37	1.1	A solution must support 2 10GE Gigabit Ethernet (GBE) (Optical/Copper) and 2 or more 1GE.	Must Have	Requesting to change the Interface requirement as 4*10G (Optical/Copper).	Minimum 2*10 GE are required.
2	Section 9 - Technical Specifications	37	1.11	The solution should integrate with LDAP directory like Active Directory, for user authentication and authorization. Integration with PIM/PAM solution	Must Have	Please suggest which is existing PIM Solution	ARCON/custom build PAM solution
3	Section 9 - Technical Specifications	37	1.13	Solution should integrate with existing DLP, APT/SSLVA solution	Must Have	Cisco WSA Proxy solution Support both SSL Inspection as well as Malware Protection. Hence requesting to modify the clause as "Solution should integrate with existing DLP, and must support SSL Inspection"	This point is related to Integration of Proxy with 3rd party SSLV or APT solution. SSL inspection is must have requirement otherwise. (Section-)
4	Section 9 - Technical Specifications	40	2.9	Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?	Good to Have	3DES, DES, Camellia and AES are supported	OK
5	Section 9 - Technical Specifications					RC4 has know Vulnerablity and has weak cipher hence requesting to remove the RC4 Encryption requirement	OK
6	Section 9 - Technical Specifications	41	2.12	Protocol Support – SPDY, HTTP/2 and HTTP/3	Good to have	Requesting to Modify the clause as "Protocol Support – SPDY, HTTP/2 / HTTP/3" Cisco WSA Currently supports SPYD,HTTP2 but HTTP3 is in Roadmap.	Okay
7	Section 9 - Technical Specifications	41	2.14	Support passing Jumbo Frame IP traffic	Good to Have	Proxy Solution works on L7, hence not relevant for Web Proxy Requirement. Request for removal of this Clause from the specs.	This is for network setting for troubleshooting purposes to modify MTU size if required
8	Section 9 - Technical Specifications	41	2.18	Ability to support network HSM?	Good to have	Requesting to Please Brief on the Use Case for Integration with HSM	This is a good to have requiement if Key management can be offloaded to a HSM device
9	Section 9 - Technical Specifications	41	2.22	Maximum supported concurrent SSL sessions on single device should be 200K concurrent SSL flow states	Good to have	Solutions Support SSL session . Requesting to Modify it as " Solution Must support SSl Inspection "	this point is about capacity requirement, ssl inspection is a must have point
10	Section 9 - Technical Specifications	43	5.2	24x7 remote support including any holidays. Support to include version upgrades, patch updates, including availability of on-site resource if required for troubleshooting and resolution of technical issues Back-to-Back support from OEM/Bidder	Must to Have	Cisco will be provide 24*7 TAC Support and also includes version upgrades, patch updates availability . For on-site resource if required for troubleshooting and resolution of technical issues Back-to-Back support will be Provided by Bidder	Okay
11	Section 9 - Technical Specifications	42	4.6	The solution should support Client Certificate Authentication (Content Gateway) Certificate authentication for use with mobile and other personal devices	Good to Have	Not supported for Mobile device , Requesting to Removal of this Specification	This is a good to have requiement
12	Section 3 – Scope of Work	11	3.1	Solution provider should have at least 2 data centers with at least 1 primary data center being in India.		What is the maximum expected internet bandwidth required for Data Center in India (can't be unlimited)	Subjected to the solution provider
13	Section 3 – Scope of Work	11	3.1	Propose Web proxy hardware appliance for DC & DR. Appliance – 04 Nos. as active-active for two DC. user license for the appliance is required to support 3000 Users in DC-DR Model with complete failover to 100% capacity. (With Hybrid support		Requesting to brief on the device placement with respective to DC & DR . Please suggest if Understanding is correct , the Requirement is of 4 appliance for two DC for 3000 Users	4 appliances, 2 at DC, 2 at DR with Active-Active support. 1 individual device should support 3000 users.

15	Warranties	26	8.13	End of Sale - The bidder is required to quote components of the Solution offered of the latest technology, version, make, model, etc. The bidder should not quote any component of the solution that has been declared as End of Sale (EOSL) or would become EOSL during the contract period. Further, if any of the components is declared EOSL during the contract period commencing from the submission of bid, it must be replaced by bidder with another of equivalent or higher configuration at no extra cost to NPCI.		As a general practice followed by all the NPCI we have seen RFP clause related to End Of supprot timelines and not on End of Sale, since End of Sale of any product line will not impact NPCI existing deployment. Also wanted to clarify that there is no plans of declaring End of Sale of any of the product line which is being proposed but we request to follow standard practice. Requesting to Change the Clause to " If solution goes EOS - END of support " , the during the contract period commencing from the submission of bid, it must be replaced by bidder with another of equivalent or higher configuration at no extra cost to NPCI	Okay, End of Support
16	8.8 Key Deliverables	25	6	OEM Technical Training for NPCI officials (Detailed technical training before Project Kick off and 5 Days Post Implementation Training		Detail techinical Training:Pls share us number of Participants join for training from NPCI. Pls allow Virtual instructor-led training for 2 days of web-based classes with hands-on lab practice. Since Post implementation training is generally about solution deployed by Bidders therefore we would request NPCI to change 5 Days Post Implementation from OEM training to Bidders training. Where Bidders deployment team will train NPCI operation team on solution deployed. Delivery of any on-site Services will be subject to the Parties respective policies and guidance regarding COVID-19 in effect at the time. If needed, the parties will mutually agree upon any required changes to the SOW, such as Services schedule, scope and method of delivery.	5-7 members from NPCI site would be attending training program.
17	8.8 Key Deliverables	25	7	Post Implementation: OEM is annually required to review the deployment and suggest fine tuning, a minimum 7-10 days per year review & fine tuning effort of the OEM needs to be factored for implemented solution		Since NPCI operation team will manage and operate the solution, therefore we would request NPCI to keep only Annual review under OEM scope. OEM will conduct Annual review and submit the report to NPCI operation team. NPCI operation team will execute the changes suggested by OEM Annual review report. Delivery of any on-site Services will be subject to the Parties respective policies and guidance regarding COVID-19 in effect at the time. If needed, the parties will mutually agree upon any required changes to the SOW, such as Services schedule, scope and method of delivery.	Okay
18	Section 9 - Technical Specifications	37	1.6	The Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for Secure Web Gateways solution, or Forrester wave report consecutively for last Two years (Two of last 3 years).	Request to remove this clause from the RFP because it restricts other vendors / OEM to participate in RFP.		This is a Policy requirement of NPCI.

19	Section 9 - Technical Specifications	37	1.8	Solution/appliance to provide High Availability (HA) and Load Balancing functionality and must have RAID redundancy (for hard drives), Network redundancy (for management network interfaces) and Power-Supply module redundancy.	1) we don't support Raid redundancy (for hard drives). Also, the proposed solution will be in a HA. And hence Raid redundancy is not applicable here. So request you to remove the RAID redundancy clause from the RFP. 2) what is Load balancing functionality? Do you require to Integrate a Proxy solution with an External Load balancer?		1) RAID is not required for appliance based solution, but for software based solution should be having RAID as server is to be provided by bidder. 2) We require to Integrate proxy with external load balancer.
20	Section 9 - Technical Specifications	38	1.16	Roaming user and Onsite user policy access management will be done from single Policy Management console. (The solution should be capable of applying 2 different types of disposition and action for a specific Web category with 1 single policy and this should be applied on the fly for both roaming-off site and on premise users.)	Which is the existing web gateway solution deployed at NPCI? We can achieve Roaming user and Onsite User Policy access management via two different solutions, and hence two diff consoles are required. Therefore request you to either remove this clause or modify this clause as "Roaming user, and Onsite user policy access management will be done from single Policy Management console or Dual Policy management console."		Existing solution is Broadcom SWG. Requirement to have Hybrid management console which can manage both on-prem & cloud console from single GUI.
21	Section 9 - Technical Specifications	38	1.12	The solution should have support two factor Authentication for Management Server	At present, we don't have a centralize management server for a secure web gateway. But we can integrate two-factor authentication with individual secure web gateway appliances. And hence request you to remove this clause or modify this clause as "The solution should have support two-factor Authentication for Management Server or Individual Secure web gateway appliance/solution."		Centralized management server requirement is to manage roaming and on-prem users from single console and it should have two factor authentication.
22	Section 9 - Technical Specifications	38	1.22	Solution should have centralized architecture with web or GUI based dashboard console to monitor, reporting, notification, maintaining and policy push for the registered users centrally for multiple boxes/ appliances	We don't have centralize management for policy push for the registered users centrally for multiple boxes/appliances. Hence request you to remove this clause or modify this clause as "Solution should have dedicated management port with web or GUI based dashboard console to monitor, reporting, notification, maintaining and policy push."		This is required for ease of operations for multiple proxy modules.
23	Section 9 - Technical Specifications	38	1.24	Solution shall support role-based administration such as Administrator, Malware Analyst, Database Reader, and Read-only access user	Malware Analyst, Database readers are other vendors/OEM terminology. Kindly make it Generic, i.e. "Solution shall support role-based administration."		Given terminologies are example purpose only. Need to have role based administrations.
24	Section 9 - Technical Specifications	41	2.2	Ability to support OCSP stapling?	Kindly clarify the use case for having an OCSP stapling in a secure web gateway. OSCP stapling is a Reverse Proxy/Server load balancer function and not a secure web gateway function. We don't support the OCSP stapling and Hence request you to remove this clause from the RFP		Point is to support CRL check and OCSP calls through proxy
25	Section 9 - Technical Specifications	41	2.21	Is the device FIPS 140-2 certified?	Kindly clarify the use case for having a FIPS 140-2 certification in secure web gateway/Proxy. FIPS certification is required in Reverse Proxy/Server load balancer and not in a Secure web Gateway. Not all vendors are providing FIPS 140-2 certification in Secure web gateway and Hence request you to remove this clause from the RFP		Need more clarity on question
26	Section 9 - Technical Specifications	42	4.6	Both the proxy solution should provide regulatory compliance reports for PCI ,ISO,SOX,FISMA,GLBA as applicable.	Apart from PCI compliance, What is the relevance of having ISO, SOX, FISMA, GLBA certification in the NPCI environment. Hence request you to modify this clause and only mention PCI compliance. We don't comply with another certification clause apart from PCI.		Solution should be complaint to the standards, PCI compliance will suffice

27	Section 9 - Technical Specifications	43	5.6	Solution should have flexibility for rule/policy enforcement. i.e. Solution should allow administrator to enforce the policy/rule selectively for remote users and LAN users from the same console. E.g. if Rule A / Policy A should be enforced on LAN users but not on Remote users and vice versa. (Option to choose for where to enforce the policy -for remote users OR LAN users). Additionally if required the same policy/rule should be able enforced for both i.e. remote users and LAN users.	We can achieve Roaming user and Onsite User Policy access management via two different solutions, and hence two diff consoles are required. Therefore request you to either remove this clause or modify this clause as "Solution should have the flexibility for rule/policy enforcement. i.e. Solution should allow the administrator to enforce the policy/rule selectively for remote users and LAN users from the same console or two different console / dual console."		This is mandate requirement from NPCI as Solution should able to manage both roaming and on-prem users from single console.
28	Section 9 - Technical Specifications	43	5.7	Solution should support off the network roaming users (Remote Filtering) and On-the-network (corporate) users. For roaming users connecting to Internet via Data card, WIFI, the corporate proxy policies should be enforced on them.	Would you please clarify the number of Roaming users? And the number of on-the-network users?		There is no spefic count for roaming/on-site users, as NPCI has permitted WFH acros all branches hence count can be any within 3000 of ask.
29	Section 9 - Technical Specifications	43	6.1	Licensing structure proposed considering number of users, scalability & centralized architecture. The bidder has to provide the Enterprise (Premium) level licenses to cover all the features desired in the SOW including functional & technical requirements mentioned in this RFP	At present, we don't have a centralize management / centralized architecture for policy push for the registered users centrally for multiple boxes/appliances. Hence request you to remove this clause or modify this clause as "Licensing structure proposed considering a number of users, & scalability. The bidder has to provide the Enterprise (Premium) level licenses to cover all the features desired in the SOW including functional & technical requirements mentioned in this RFP."		This is a required feature as part of delivery
30	Request for proposal for procurement of Secure Web Gateway solution	11	Section 3 - Scope of Work 3.1 Scope of work:	The user license for the appliance is required to support 3000 Users in DC-DR Model with complete failover to 100% capacity. (With Hybrid support).	Please let us know more details on Hybrid Support. Does NPCI wants Hybrid Web Proxy Architecture i.e. Proxy and Cloud Proxy. Please confirm on our understanding.		Solution should able to manage both on-prem and roaming users from single management console.
31	Request for proposal for procurement of Secure Web Gateway solution	11	Section 3 - Scope of Work 3.1 Scope of work:	Integrate the solution with the NPCI's Active Directory system for authentication & other application based on rest APIs.	Kindly let us know which applications are referred here for integration and Customize use case expectation which may require additional implementation efforts ?		Its an mandate requirement that solution should support rest APIs integration with any third party tool. Application such as SOAR, Strobes (dash board presentations etc).
32	Request for proposal for procurement of Secure Web Gateway solution	13	7.3 Technical Scoring Matrix:	Part – B Vendor Evaluation Matrix Customer BFSI reference in India Please provide at least 1 India References including	Request NPCI to consider below criteria for Vendor Evaluation Customer BFSI/PSU reference in India Please provide at least 1 India References including		Minimum of 5 or more similar project deployment.
33	Request for proposal for procurement of Secure Web Gateway solution	25	8.8 Key Deliverables	4. Integrate Proxy with all existing applications, infra tools such as AD, SIEM, SOAR, etc.	Bidder expect that changes and Any Custom API Development on Solutions like SIEM, SOAR will be done by existing Vendor for integration.		API based integration should be supported by the solution, integration will be done by existing vendor
34	Request for proposal for procurement of Secure Web Gateway solution	26	8.9 Delivery schedule	8.9 Delivery schedule Delivery, installation & commissioning of the proxy solution should be completed within 16 weeks from the date of receipt of purchase order. • Delivery of hardware, software, and license should be within 6 weeks. • Installation & commissioning should be completed in next 10 weeks. • Installation Certificate for each installation should be signed by NPCI and the bidder	Since most of OEM's Hardware delivery is delayed and approimately appliance is delivered in 8 to 10 Weeks. We request NPCI, to please extend delivery timelines as below. • Delivery of hardware, software, and license should be within 10 weeks.		No change

35	Request for proposal for procurement of Secure Web Gateway solution	27	8.14 Service Level Requirements (SLA)	The Bidder shall monitor and maintain the stated service levels to provide quality service. Bidder to use automated tools to provide the SLA Reports. Bidder to provide access to NPCI or its designated personnel to the tools used for SLA monitoring.	Does the NPCI has Availablity monitoring tool in place. Please let us know make for integrations. While Ticket logging and reporting will be manual as per RFP SLA's. Please share more details on ths understanding.		NPCI has its own tools such as BMC for ticketing & Incidents, strobes for dash board presentations.
36	Request for proposal for procurement of Secure Web Gateway solution		8.15 Penalty on non-adherence to SLAs:	8.15 Penalty on non-adherence to SLAs: a) Penalty for Severity 1 Incidents: Any violation in meeting the above SLA requirements which leads to Severity 1 incident, NPCI shall impose a penalty of INR 10,000/- (Indian Rupees Ten Thousand only) for each hour of delay up to 12 hours, beyond 12 hours penalty would be INR 20,000 for each hour with a max cap of 5% of total value .	We request penalties to be capped to quarterly arrears.		No change
37	Request for proposal for procurement of Secure Web Gateway solution	11	Section 3 - Scope of Work 3.1 Scope of work:	Integrate the solution with the NPCI's Active Directory system for authentication & other application based on rest APIs.	Kindly let us know which applications are referred here for integration and Customize use case expectation which may require additional implementation efforts ?		Its an mandate requirement that solution should support rest APIs integration with any third party tool. Application such as SOAR, Strobes (dash board presentations etc).
38	Section 9 - Technical Specifications	37	1.1	A solution must support 2 10GE Gigabit Ethernet (GBE) (Optical/Copper) and 2 or more 1GE.	Must Have	Requesting to change the Interface requirement as 4*10G (Optical/Copper).	Minimum 2*10 GE are required.
39	Section 9 - Technical Specifications	37	1.11	The solution should integrate with LDAP directory like Active Directory, for user authentication and authorization. Integration with PIM/PAM solution	Must Have	Please suggest which is existing PIM Solution	ARCON/custom build PAM solution
40	Section 9 - Technical Specifications	37	1.13	Solution should integrate with existing DLP, APT/SSLVA solution	Must Have	Cisco WSA Proxy solution Support both SSL Inspection as well as Malware Protection. Hence requesting to modify the clause as "Solution should integrate with existing DLP, and must support SSL Inspection"	This is required to provide solution as per existing DC setup requirement
41	Section 9 - Technical Specifications	40	2.9	Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?	Good to Have	3DES, DES, Camellia and AES are supported RC4 has know Vulnerablity and has weak cipher hence requesting to remove the RC4 Encryption requirement	OK
42	Section 9 - Technical Specifications	41	2.12	Protocol Support – SPDY, HTTP/2 and HTTP/3	Good to have	Requesting to Modify the clause as "Protocol Support – SPDY, HTTP/2 / HTTP/3" Cisco WSA Currently supports SPYD,HTTP2 but HTTP3 is in Roadmap.	Okay
43	Section 9 - Technical Specifications	41	2.14	Support passing Jumbo Frame IP traffic	Good to Have	Proxy Solution works on L7, hence not relevant for Web Proxy Requirement. Request for removal of this Clause from the specs.	This is for network setting for troubleshooting purposes to modify MTU size if required
44	Section 9 - Technical Specifications	41	2.18	Ability to support network HSM?	Good to have	Requesting to Please Brief on the Use Case for Integration with HSM	This is a good to have requiement if Key management can be offloaded to a HSM device
45	Section 9 - Technical Specifications	41	2.22	Maximum supported concurrent SSL sessions on single device should be 200K concurrent SSL flow states	Good to have	Solutions Support SSL session . Requesting to Modify it as " Solution Must support SSl Inspection "	this point is about capacity requirement, ssl inspection is a must have point
46	Section 9 - Technical Specifications	43	5.2	24x7 remote support including any holidays. Support to include version upgrades, patch updates, including availability of on-site resource if required for troubleshooting and resolution of technical issues Back-to-Back support from OEM/Bidder	Must to Have	Cisco will be provide 24*7 TAC Support and also includes version upgrades, patch updates availability . For on-site resource if required for troubleshooting and resolution of technical issues Back-to-Back support will be Provided by Bidder	Okay
47	Section 9 - Technical Specifications	42	4.6	The solution should support Client Certificate Authentication (Content Gateway) Certificate authentication for use with mobile and other personal devices	Good to Have	Not supported for Mobile device , Requesting to Removal of this Specification	This is a good to have requiement

48	Section 3 – Scope of Work	11	3.1	Solution provider should have at least 2 data centers with at least 1 primary data center being in India.		As per various security directives and regulatory organization, Data Center must be in strictly hosted in India and data should not cross Indian Geographic for Service providers. Hence, requesting NPCI to consider below clause and accreditation. "Solution provider should have data centers in India with following accreditation. MEITY Empanelled DC PCI DSS Version 3.2.1,2018 ISO/IEC 27017:2015 ISO/IEC 27018:2014	OK
49	Section 3 – Scope of Work	11	3.1	Propose Web proxy hardware appliance for DC & DR. Appliance – 04 Nos. as active-active for two DC. user license for the appliance is required to support 3000 Users in DC-DR Model with complete failover to 100% capacity. (With Hybrid support		Requesting to brief on the device placement with respective to DC & DR . Please suggest if Understanding is correct , the Requirement is of 4 appliance for two DC for 3000 Users	4 appliances, 2 at DC, 2 at DR with Active-Active support. 1 individual device should support 3000 users.
50	Warranties	26	8.13	The successful bidder(s) should ensure that the equipment proposed in this RFP, should not be declared as End of Life (EOL) or End of Support (EOS) by the OEM within the 3 years contract period		The end of life process consists of a series of technical and business milestones. of which EOL is the "The date the document that announces the end-of-sale and end-of-support of a HW/ SW product is distributed to the general public " . NPCI should put a clause around End of Support of the product HW/ SW sold as part of this RFP. So requesting to Modify the cluase as " The successful bidder(s) should ensure that the equipment proposed in this RFP, should not be declared as End of Support (EOS) by the OEM within the 3 years contract period "	Okay, End of Support
51	Warranties	26	8.13	End of Sale - The bidder is required to quote components of the Solution offered of the latest technology, version, make, model, etc. The bidder should not quote any component of the solution that has been declared as End of Sale (EOSL) or would become EOSL during the contract period. Further, if any of the components is declared EOSL during the contract period commencing from the submission of bid, it must be replaced by bidder with another of equivalent or higher configuration at no extra cost to NPCI.		As a general practice followed by all the NPCI we have seen RFP clause related to End Of supprot timelines and not on End of Sale, since End of Sale of any product line will not impact NPCI existing deployment. Also wanted to clarify that there is no plans of declaring End of Sale of any of the product line which is being proposed but we request to follow standard practice. Requesting to Change the Clause to " If solution goes EOS - END of support " , the during the contract period commencing from the submission of bid, it must be replaced by bidder with another of equivalent or higher configuration at no extra cost to NPCI	Okay, End of Support

52	8.8 Key Deliverables	25	6	OEM Technical Training for NPCI officials (Detailed technical training before Project Kick off and 5 Days Post Implementation Training		Detail techinical Training:Pls share us number of Participants join for training from NPCI. Pls allow Virtual instructor-led training for 2 days of web-based classes with hands-on lab practice. Since Post implementation training is generally about solution deployed by Bidders therefore we would request NPCI to change 5 Days Post Implementation from OEM training to Bidders training. Where Bidders deployment team will train NPCI operation team on solution deployed. Delivery of any on-site Services will be subject to the Parties respective policies and guidance regarding COVID-19 in effect at the time. If needed, the parties will mutually agree upon any required changes to the SOW, such as Services schedule, scope and method of delivery.	OK
53	8.8 Key Deliverables	25	7	Post Implementation: OEM is annually required to review the deployment and suggest fine tuning, a minimum 7-10 days per year review & fine tuning effort of the OEM needs to be factored for implemented solution		Since NPCI operation team will manage and operate the solution, therefore we would request NPCI to keep only Annual review under OEM scope. OEM will conduct Annual review and submit the report to NPCI operation team. NPCI operation team will execute the changes suggested by OEM Annual review report. Delivery of any on-site Services will be subject to the Parties respective policies and guidance regarding COVID-19 in effect at the time. If needed, the parties will mutually agree upon any required changes to the SOW, such as Services schedule, scope and method of delivery.	Okay
55	Section 8 - Terms and Conditions	26	8.9 Delivery schedule	Delivery, installation & commissioning of the proxy solution should be completed within 16 weeks from the date of receipt of purchase order. • Delivery of hardware, software, and license should be within 6 weeks. • Installation & commissioning should be completed in next 10 weeks. • Installation Certificate for each installation should be signed by NPCI and the bidder	As there global chip shortage all OEM in this space have major delivery issues. Can NPCI move delivery of hardware to 16 weeks without any LD and modify the project schedule accordingly. Also request npci to change this to "Delivery, installation & commissioning of the proxy solution should be completed within 24 weeks from the date of receipt of purchase order."		No change
56	Section 8 - Terms and Conditions	26	8.12 End of Sale	The bidder is required to quote components of the Solution offered of the latest technology, version, make, model, etc. The bidder should not quote any component of the solution that has been declared as End of Sale (EOSL) or would become EOSL during the contract period. Further, if any of the components is declared EOSL during the contract period commencing from the submission of bid, it must be replaced by bidder with another of equivalent or higher configuration at no extra cost to NPCI.	Reqeust NPCI to consider the End of Sale (EOSL) period as maximum 1 year only as there will be revision and updage on products every year. Request NPCI to consider the clause as :- "The bidder is required to quote components of the Solution offered of the latest technology, version, make, model, etc. The bidder should not quote any component of the solution that has been declared as End of Sale (EOSL) ~~or would become EOSL during the contract period~~. Further, if any of the components is declared **End of Support** ~~EOSL~~ during the contract period commencing from the submission of bid, it must be replaced by bidder with another of equivalent or higher configuration at no extra cost to NPCI."		Okay, End of Support

57	Section 8 - Terms and Conditions	29	8.15 Penalty on non-adherence to SLAs:	The following Resolution Service Level Agreement (SLA) would be applicable during Warranty are applicable for critical and non-critical incidents. The reported issue would be classified as Critical or Non-Critical by NPCI only. a) Penalty for Severity 1 Incidents: Any violation in meeting the above SLA requirements which leads to Severity 1 incident, NPCI shall impose a penalty of INR 10,000/- (Indian Rupees Ten Thousand only) for each hour of delay up to 12 hours, beyond 12 hours penalty would be INR 20,000 for each hour with a max cap of 5% of total value. b) Penalty for Severity 2: Any violation in meeting the above SLA requirements which leads to Severity 2 incident, NPCI shall impose a penalty of INR 5,000/- (Indian Rupees Five Thousand only) for each hour of delay up to 12 hours, beyond 12 hours penalty would be INR 10,000 for each hour with a max cap of 5% of total value. c) Penalty for Severity 3: Any violation in meeting the above SLA requirements which leads to Severity 3 incident, NPCI shall impose a penalty of INR 2,000/- (Indian Rupees Two Thousand only) per hour with a max cap of 2% of total value. d) The penalty amount would be calculated and deducted from the performance bank guarantee during warranty period. e) Further if the number of downtime instances during a month exceeds 3 times, an additional 0.50% downtime will be reduced from uptime and the penalty will be calculated accordingly. f) If a breach occurs even after a proper policy in Proxy solution is in place, a penalty of Rs. 10,000/-per event will be deducted or the loss due to the breach whichever is higher. The right to levy the penalty is in addition to and without prejudice to other rights / remedies available to the NPCI such as termination of contract, invoking performance guarantee and recovery of amount paid etc.	Reqeust NPCI to specify the CAP for SLA penalty as 10% of product value.		No change
59	Section 9 - Technical Specifications	37	1.13	Solution should integrate with existing DLP, APT/SSLVA solution	Please confirm the existing DLP, APT/SSLVA solution used by NPCI.		DLP- Forcepoint, SSLV- F5, APT- FireEye NX
60	Section 9 - Technical Specifications	38	1.17	The solution should provide geo-location awareness for security incidents. The solution should provide inbuilt capability malicious content of password and unknown encryption files.	Please confirm the relation of geolocation awareness for security incidents with encryption or malware detection. If a file is encrypted with an 'unknown key' there is no way for any web gateway to examine it for malicious content. Encrypted files can be blocked based on detection of encryption in combination with other criteria. For example you could make exceptions such that encrypted files from certain domains or categories are allowed while all other encrypted files are blocked. Hence, it is requested to amend the specification as follows: *"The solution should provide geo-location awareness for security incidents. The solution should be able to block the encrypted files based on detection of encryption in combination with other criteria."*		Need more clarity on question
61	Section 9 - Technical Specifications	41	2.12	Protocol Support – SPDY, HTTP/2 and HTTP/3	Please note that SPDY is an earlier version of HTTP/2 that is no longer in use. HTTP/3 is/will be UDP based and is not able to be traditionally proxied. Hence, please amend the specificatiosn to as follows: "Protocol Support - HTTP/2, FTP, SOCK(s)."		Requirement is to support SPDY, HTTP/2, HTTP/3 can be consider as future support.

62	Section 9 - Technical Specifications	41	2.14	Support passing Jumbo Frame IP traffic	Please note that 'Jumbo frames' are a network level concept. Web Gateway is an application layer proxy intended to filter traffic between clients on the local network and servers on the Internet. The general Internet does not support Jumbo Frame traffic as it is not defined by the 802.3 specification. This specification is targeted at firewall or IPS type network devices that may operate exclusively on local network traffic where jumbo frames could be used. Hence, in order to promote fair competition, it is requested to remove this clause.		This is for network setting for troubleshooting purposes to modify MTU size if required
63	Section 9 - Technical Specifications	41	2.20	Ability to support OCSP stapling?	Please clarify the expectation from the support for OCSP Stapling, as this requirement is ambiguous.		Point is to support CRL check and OCSP calls through proxy
64	Section 9 - Technical Specifications	42	3.7	The solution should apply security policy to more than 100 protocols in multiple categories more than 15. This includes the ability to allow, block, log, and assign quota time for IM, P2P, and streaming media and solution should provide at least below mentioned security categories as below RIGHT FROM DAY ONE : 1) Advanced Malware Command and Control category 2)Advanced Malware payload detection category 3) Malicious embedded links and iframe detection category 4) Mobile malware category 5) Key logger and Spyware category 6) P2P software database from day 1 to control/block the below P2P protocols.	Our solution is one of the world's best in class Web gateway and it is not intended to be a general purpose multi-protocol firewall. McAfee have announced plans to support multi-protocol firewalling in the cloud but we have no plans to support filtering of protocols other than SOCKs, HTTP/S, and FTP with our on premise appliances. Multi-protocol firewalls do not provide sufficient filtering capabilities for HTTP/S traffic. They are a complementary solution for an enterprise class web gateway. Hence, in order to promote fair competition - it is requested to remove this specification.		Need more clarity on question
65	Section 9 - Technical Specifications	42	3.5	The solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future data leakage by the malware.	Please elaborate on the use case.		Solution should able to provide indepth details of Malicious traffic originated from system such as host details, browser, type of attack etc.
66	Section 2 – Introduction	9	2.2	The objective of the RFP is to procure and deploy a new secure Web Gateway Solution as a replacement of existing device.	Request npci to provide details of existing Web Proxy		Existing solution is Broadcom SWG. Requirement to have Hybrid management console which can manage both on-prem & cloud console from single GUI.
67	Section 3 – Scope of Work	11	3.1	Appliance – 04 Nos. as active-active for two DC.	Request NPCI to elaborate on this requirement		As a part of HA setup, NPCI required to have total of 4 proxy devices, 2 per datacenter.
68	Section 3 – Scope of Work	11	3.1	The user license for the appliance is required to support 3000 Users in DC-DR Model with complete failover to 100% capacity. (With Hybrid support).	Please let us know on the expectation for Hybrid support		Solution should able to manage both on-prem and roaming users from single management console.
69	Section 3 – Scope of Work	11	3.1	Integrate the solution with the NPCI's Active Directory system for authentication & other application based on rest APIs.	Please share the number & details of other application for rest APIs based integration.		Its an mandate requirement that solution should support rest APIs integration with any third party tool. Application such as SOAR, Strobes (dash board presentations etc).

70	Section 3 – Scope of Work	11	3.1	Solution provider should have at least 2 data centers with at least 1 primary data center being in India.	Request NPCI to elaborate on this requirement		For cloud based component, data centre should be hosted in India
71	Section 3 – Scope of Work	11	3.1	Technical Training should be arranged by OEM directly.	Please share the no of participants from npci for the training?		5-7 members from NPCI site would be attending training program.
72	RFP Document (RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021) : 3.1 Scope of work	11	3.1 Scope of work	Integrate the solution with the NPCI's Active Directory system for authentication & other application based on rest APIs.	Need Clarification # Need information on integration components other than Active Direcotry & Syslog		Its an mandate requirement that solution should support rest APIs integration with any third party tool. Application such as SOAR, Strobes (dash board presentations etc).
73	RFP Document (RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021) : 3.1 Scope of work	11	3.1 Scope of work	Bidder should support the migration of the Web proxy security policies and features and building new policies required by organization for the proposed solution during the implementation phase.	Need Clarification # Native migration may not be possible between 02 different solutions (source & destination) hence we understand that manual policy creation based on existing policies inline to supported methods will also do; please confirm		Yes, if native is not supported then existing policies should be migrated to new.
74	RFP Document (RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021) : 3.1 Scope of work	11	3.1 Scope of work	The first monitoring report would be submitted on completion of 1 month from the date of acceptance of the Web Proxy Solution and thereafter every fortnight with suggested / required remediation.	Need Clarification # This is during implementation phase or support phase ?		This is required during end to end implementation phase.
75	RFP Document (RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021) : 7.3 Technical Scoring Matrix	22	7.3 Technical Scoring Matrix	Part – B Vendor Evaluation Matrix : Work experience in past (similar project)	Need Clarification # How many such references are required to have maximum score		Minimum of 5 or more similar project deployment.
76	RFP Document (RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021) : 8.14 Service Level Requirements (SLA)	28	8.14 Service Level Requirements (SLA)	All the infrastructure of Data Center, Disaster Recovery site, Offices/Branches will be supported on 24x7 basis.	Need Clarification # Support for branches / offices other than Mumbai/Chennai/Hyderabad will be remote. Is this correct understanding		Yes
77	RFP Document (RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021) : 8.14 Service Level Requirements (SLA)	30	8.14 Service Level Requirements (SLA)	If a breach occurs even after a proper policy in Proxy solution is in place, a penalty of Rs. 10,000/- per event will be deducted or the loss due to the breach whichever is higher. The right to levy the penalty is in addition to and without prejudice to other rights / remedies available to the NPCI such as termination of contract, invoking performance guarantee and recovery of amount paid etc.	Please put capping on penalty and Penalty shall not be more than contract value		No change
78	RFP Document (RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021) : 3.1 Scope of Work	11	NA	NA	Bandwidth Information required so that we can size the appliance accordingly		Need more clarity on question
79	Additional Query				In case Management and Database servers are can be hosted in virtual envoirnment, will NPCI provide Virstual systems, Operating Systems and Database or need to be provisioned by Bidder		In case of Virtual environment, licenses of OS/DB needs to be factored by bidders.

80	Section - 9.Technical Specification . 1. General Features and Policies, Point 1.9	37	1.9	The appliance management console should have a single control mechanism in form of Configuration/master button to DENY ALL TRAFFIC control to deactivate all internet services. (This specific option to be used only in case of an outbreak, hacking attempt, etc.)	This is achived by a config and no single button , I hope this shall meet the requirement		Okay
81	Section - 9.Technical Specification . 1. General Features and Policies, Point 1.13	37	1.13	Solution should integrate with existing DLP, APT/SSLVA solution	We can integrate with DLP as native integration and save on overall TCO however it was informed NPCI is having an idependent APT/SSLVA solution hence integration is not required , kindly confirm if the scenario is same and NPCI doesn't required the proposed proxy to integrate with independent APT/SSLVA		Proposed proxy should be able to integrate with all existing solutions such as DLP, SSLV, APT.
82	Section - 9.Technical Specification . 1. General Features and Policies, Point 1.17	38	1.17	The solution should provide geo-location awareness for security incidents. The solution should provide inbuilt capability malicious content of password and unknown encryption files.	g		Proxy should be able to create file type based policies that can control password protected and unknown encrypted file.
83	Section - 9.Technical Specification . 1. General Features and Policies, Point 1.19	38	1.19	Solution should be able to restrict Users to download certain amount of data, for example a user can be restricted to use not more than 1GB data during a time interval.	Yes, the underlying objective can be achieved by Quota assignment based on time interval on categories and policies		Okay
84	Section - 9.Technical Specification . 1. General Features and Policies, Point 1.2	38	1.2	A solution should support hostname resolution through either NetBios Lookup or reverse DNS. (Asset Identification).	Generally we will see the username in the reports however if the user name is not visibile for some reason then in other transaction logs we can see the IP of the machine , we believe to find out the security incidents username is more important than the hostname so kindly ammend the clause accordingly .		This clause is related to asset identification from where query is getting generated (Hostname/IP address)
85	Section - 9.Technical Specification . 1. General Features and Policies, Point 1.21	38	1.21	The solution should support configuring scheduled automatic backup of system configuration.	This can be leveraged by using windows task scheduler as well		Okay
86	Section - 9.Technical Specification . 1. General Features and Policies, Point 1.27	38	1.27	The solution should have granular control over popular social web applications like Facebook, LinkedIn, Twitter, YouTube, and others. The solution should have social control Video UPLOADS to Facebook and YouTube applications	This is possible and gives more granular controls with Native DLP integration		Okay
87	Section - 9.Technical Specification . 1. General Features and Policies, Point 1.29	38	1.29	The solution should have built-in or custom policies for identifying and segregate You Tube traffic for Education only and Other irrelevant non compliance video, It should simplify design and implementation of policy to ensure user compliance.	This possible with by Individual URL re-categorization, I hope this should address NPCI need , please confirm		Granular control over websites should be supported in Proxy solution without indivitual re-categorization.
88	Section - 9.Technical Specification . 1. General Features and Policies, Point 1.35		1.35	Should capture all activity information as part of audit logging & forward it to SIEM.	Kindly ammend the clause as "Solution should capture all activities under Audit logs and forward the transaction logs to SIEM"		Solution should able to capture every indivutual system, admin, transaction, audit logs in console and should be able to forward the same to SIEM.
89	Section - 9.Technical Specification . 1. General Features and Policies, Point 1.39	39	1.39	The proposed solution should support session time out and idle time out facility to forcefully logout the users.	This is OEM specfic and actually not a proxy use case , I would request you to remove this clause		This is required for management and console session of Proxy GUI.

90	Section - 9.Technical Specification . 1. General Features and Policies, Point 1.41	39	1.41	The proposed solution should provide option to define different bandwidth and policy. (Optimize bandwidth utilization).	Underlying objective can be achieved with Time based Quota		Okay
91	Section - 9.Technical Specification . 1. General Features and Policies, Point 1.45	39	1.45	the solution should support different types of compression algorithms and scan nested compressed files.	Generally we do it however In case NPCI has any ask specific to an algorithm then please higlight .		This is a generic requirement.
92	Section - 9.Technical Specification . 1. General Features and Policies, Point 1.46	39	1.46	The solution should ensure capabilities of caching to be quantified up to 25%.	We have Raw disk for 147 GB is used for caching and only http, please consider this figure as nowdays only 20% of traffic is http amnd rest are https		Requirement is to support caching.
93	Section - 9.Technical Specification . 1. General Features and Policies, Point 1.48	40	1.48	The solution should monitor and block instant messaging (IM) based file transfer	This can achived by category or protocol blocking or also doable with Native DLP integration		Okay
94	Section - 9.Technical Specification . 1. General Features and Policies, Point 1.51	40	1.51	The solution should block users when multiple (configurable) numbers of policy violations are triggered simultaneously.	Such feature can bring in business disruption as in our solution user can be blocked multiple times in real time to deal with real time security threats in such scenario the mentioned ask can cause the complete access block to users which can lead in massive business diruption so we request to remove this clause .		This is requirement in case of breach or attack scenerio. There should be a conffigurable limit for minimum violations before blocking.
95	Section - 9.Technical Specification . 2. SSL , Point 2.1	40	2.1	Solution should inspect https traffic (Full Deep Packet / SSL Traffic) and must provide decryption of unverified encrypted traffic for scanning and then re encrypt it before sending	Https traffic decrytpion , scanning and re-encrytpion is very much possible , kindly confirm if this is the ask		Okay
96	Section - 9.Technical Specification . 2. SSL , Point 2.4	40	2.4	Ability to do certificate resigning	We assume the requirement is inline having the capabilities to import the certification to our proxy and keep a record of all signed CA		Yes
97	Section - 9.Technical Specification . 2. SSL , Point 2.4	40	2.4	support RSA, DHE, and ECDHE public key algorithms?	These are inbuilt Mechanisim and we do support as well but this being an internal mechanisim of proxy we don't have any cross referrence , kindly confirm if this helps		OK
98	Section - 9.Technical Specification . 2. SSL , Point 2.4	40	2.4	Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms	These are inbuilt Mechanisim and we do support as well but this being an internal mechanisim of proxy we don't have any cross referrence , kindly confirm if this helps		OK
99	Section - 9.Technical Specification . 2. SSL , Point 2.4	40	2.4	Support MD5, SHA-1, and SHA-256 hash algorithms?	These are inbuilt Mechanisim and we do support as well but this being an internal mechanisim of proxy we don't have any cross referrence , kindly confirm if this helps		Okay but we should be able to see all Hash details in console in case of any Virus, Malware detection.
100	Section - 9.Technical Specification . 2. SSL , Point 2.4	40	2.4	Full Key length support (full 512-8192 bit key lengths), support at least 2048.	These are inbuilt Mechanisim and we do support as well but this being an internal mechanisim of proxy we don't have any cross referrence , kindly confirm if this helps		Okay
101	Section - 9.Technical Specification . 2. SSL , Point 2.4	41	2.4	Protocol Support – SPDY, HTTP/2 and HTTP/3	Kindly ammend the clause as per the required proxy solutiomn it must support http , https and FTP but the mentioned protocol uses UDP stream as reason proxy face challenges but still these traffic wont face any disruptions once we tunnel the same .		Requirement is to support SPDY, HTTP/2, HTTP/3 can be consider as future support.

102	Section - 9.Technical Specification . 2. SSL , Point 2.14	41	2.14	Support passing Jumbo Frame IP traffic	Our proxy engine allows cusotmizing the MTU so support junbo frame should not be a challenge but again this being an internal mechanisim we don't have a cross reference to this , please confirm if this fine with NPCI		OK
103	Section - 9.Technical Specification . 2. SSL , Point 2.15	41	2.18	Ability to support network HSM?	We need clarity on HSM use case in a proxy solution because any which our proxy has the certificate and private keys internally and it communicate only to those SSL server whose cert not in CRL and this is an automated process so we feel that this clause is not inline with the proxy solution		This is a good to have requiement if Key management can be offloaded to a HSM device
104	Section - 9.Technical Specification . 2. SSL , Point 2.20	41	2.2	Ability to support OCSP stapling?	By deafult our proxy has does the Revocation check based and CRL and OSCP ,kindly confirm if this suffices your request		Point is to support CRL check and OCSP calls through proxy
105	Section - 9.Technical Specification . 2. SSL , Point 2.22	41	2.22	Maximum supported concurrent SSL sessions on single device should be 200K concurrent SSL flow states	We don't have Separate parameters for SSL , it's the overall Value of WCG proxy appliance i.e shared for V10 K G4 its total concurrent connections 120,000, attached the appliance Datasheet for referrence		Okay
106	Section - 9.Technical Specification . 3. Anti-Virus and Anti-Malware , Point 3.2	41	3.2	Solution shall provide forensic evidence on the infections activity within the network as follow: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviors, malware type, severity, source and destination of attack	Packet capture is not scope of proxy solution however this point is OEM specific so we request to remove this clause in order to keep the competetion netural		This is requirement in case of breach or attack scenerio. Solution should able to do packet capture to verify logs.
107	Section - 9.Technical Specification . 3. Anti-Virus and Anti-Malware , Point 3.3	41	3.3	The solution must support different types of compression algorithms and scan nested compressed files.	Generally we do it however In case NPCI has any ask specific to an algorithm then please higlight .		This is generic ask.
108	Section - 9.Technical Specification . 3. Anti-Virus and Anti-Malware , Point 3.1	41	3.1	Solution to provide inline Anti-Virus and Anti-Malware inspection and prevention	Our proxy engine proxy has an inbuilt AV engine and for dealing with Malware we have ACE engine however if the ask to have core sanboxing thenn we propose our cloud based AMD solution , kindly confirm if then suffices the need		Requirement is only for Anti-Virus and Anti-Malware.
109	Section - 9.Technical Specification . 3. Anti-Virus and Anti-Malware , Point 3.4	41	3.4	The solution should have dual anti-malware engines (Signature and Heuristics based) and should also have capabilities to inspect malware embedded in PDF files.	Basic Malware detection can be done however no sandbxing is part of the proposed solution .		Solution should have dual Anti-Virus, Anti-Malware Engines (Signature and Heuristics). There is no ask for Sanboxing.
110	Section - 9.Technical Specification . 3. Anti-Virus and Anti-Malware , Point 3.5	42	3.5	The solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future data leakage by the malware.	Data leakage can be controlled by native DLP integration .		Solution should able to provide indepth details of Malicious traffic originated from system such as host details, browser, type of attack etc.
111	Section - 9.Technical Specification . 3. Anti-Virus and Anti-Malware , Point 3.6	42	3.6	Solution should provide advanced threat dashboard to track the infection or threat history for User/IP, with the ability to access all forensic evidence for past infections. (6 months)	Kindly ammend the the time period to 30 days.		Requirement can't change considering NPCI policies.
112	Section - 9.Technical Specification . 4.Access logs and Reporting , Point 4.2	42	4.2	The solution should support real time graphical and chart based dashboard for the summary of activities over Web.	Please ammend the clause by adding "graphical/Tabular Real time reports" as both serves the purpose		Okay

113	Section - 9.Technical Specification . 4.Access logs and Reporting , Point 4.6	42	4.6	Both the proxy solution should provide regulatory compliance reports for PCI ,ISO,SOX,FISMA,GLBA as applicable.	Yes this possible once natively integrated with web DLP		OK
114	Section - 9.Technical Specification . 4.Access logs and Reporting , Point 4.6	42	4.6	The solution should support Client Certificate Authentication (Content Gateway) Certificate authentication for use with mobile and other personal devices.	This is OEM specific pointer, request you to kindly remove the clause .		This is a good to have requiement
115	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	11	3	Appliance – 04 Nos. as active-active for two DC.	Will NPCI be providing hardware other than SWG Appliance like management servers and database servers.		Nope, every individual components should be factored by bidder.
116	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	11	4	The user license for the appliance is required to support 3000 Users in DC-DR Model with complete failover to 100% capacity. (With Hybrid support).	Confirmation required if Hybrid support is required for all the users or it is for limited set of roaming users who generally are not in office. In case of limited roaming users, what would be the count of roaming users ? In case NPCI opts for Hybrid Support for all the users then all users having SWG agent on their machine will be eligible for web filtering through OEM's data center when they are not connecting to SWG appliance in NPCI's DC or DR		There is no spefic count for roaming/on-site users, as NPCI has permitted WFH acros all branches hence count can be any within 3000 of ask.
117	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	11	16	Solution provider should have at least 2 data centers with at least 1 primary data center being in India.	OEM's Data Center in India is necessary or OEM's having virtual PoP in India can also participate ? virtual PoP are used to send request to OEM's data center in other countries for web filtering however IP shown to NPCI's users would be of INDIA but processing will happens in country/countries other than India. Do OEM's have to certify with a letter that they have a Data Center in INDIA ?		This will not comply with the requirement, processing of traffic should happen in india
118	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	11	25	Technical Training should be arranged by OEM directly.	Can this training be in association with bidder/authorized partner where person from OEM would be present to clarify on any doubts if required - Joint training with partners help to relate to deployment that was done by the bidder and is more relatable to audience. Also wanted information on how many people are to be trained ?		Pre-training should be arranged by OEM, however post deployment training can be arranged by bidder in presence of OEM personnel.

119	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	37	1.13	Solution should integrate with existing DLP, APT/SSLVA solution	Will NPCI be providing additional hardware other than SWG Appliances needed for ICAP integration between DLP and SWG or is to be quoted by bidder/OEM.		There shouldn't be requirement of additional hardware.
121	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	25	8.8 Key Deliverables (Hardware Software/Li	4. Integrate Proxy with all existing applications, infra tools such as AD, SIEM, SOAR, etc.	Please share the Vendors and current version for existing applications, SIEM, SOAR solution		Microsoft Azure AD, Arcsight SIEM, Custom SOAR & Custom Strobes (dash board presentation).
122	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	25	8.8 Key Deliverables (Hardware Software/Li)	5. Additional User License (OS/ DB)	if any server (along with OS and DB) required to deploy the solution will be provisioed by NPCI. Please clarify. Also User count shall be considered 3000.		Nope, every individual components should be factored by bidder.
123	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	27	8.14 Support	The successful bidder shall provide comprehensive on-site support of the solution for a period of 3 years with back to back support with the OEM,	We understand that warranty and support for 3 years is inclusive of Implementation period. Please clarify.		Yes
124	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	11	3.1 - Scope of Work	Bidder should ensure availability of on-site resource if required for troubleshooting and resolution of technical issues back-to-back support from OEM.	The on-site resource is required on dedciated mode available at NPCI location OR the resource is required on case to case basis only for troubleshooting & resolution of techincal issues. Please clarify.		On site support is required during implementation of tool, once handed over to operation team it can be as and when required basis.

125	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	11	3.1 - Scope of Work	Bidder should support the migration of the Web proxy security policies and features and building new policies required by organization for the proposed solution during the implementation phase.	Please advise on the extent of efforts required/envisaged by NPCI for building new policies		Existing solution should be completely migrated to new with all defined policies and new requirement if any.
126	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	11	3.1 - Scope of Work	The solution should be designed to cater Web proxy solution for both on-site employees and roaming employees.	The count of on-site and roaming employees is under 3000 users. Please clarify.	Suggestion - Hope, the 3000 user count is going to accommodate all the increase/growth in user count for the period of next 3 years.	Current count is 2000 and with future growth it should support upto 3000.
127	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	11	3.1 - Scope of Work	Technical Training should be arranged by OEM directly.	Please elaborate on the nature of technical training expected from OEM along with the numbers of training required and the count of NPCI staff to whom the training need to be given.		Product overview and technical training of the tool. 5-7 members from NPCI would be attending the same.
129	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	27	8.14 - Support	The successful bidder shall provide comprehensive on-site support of the solution for a period of 3 years with back to back support with the OEM	Please elaborate whether the on-site resource is required on dedciated mode available at NPCI location OR the resource is required on case to case basis only for troubleshooting & resolution of techincal issues.		On site support is required during implementation of tool, once handed over to operation team it can be as and when required basis.
130	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	29	8.15 - (a) & (b)	Penalty to non-adherence to SLAs for Severity 1 & Severity 2 incidents	Please clarify the max cap of 5% of total value? Which line item from #1 to #6 of Annexure N of commercial bid format will accounted for arriving at the penalty for max cap of 5% of total value?		of total AMC value

131	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	29	8.15 - (C)	Penalty to non-adherence to SLAs for Severity 3 incidents	Please clarify the max cap of 2% of total value? Which line item from #1 to #6 of Annexure N of commercial bid format will accounted for arriving at the penalty for max cap of 2% of total value?		of total AMC value
132	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	30	8.20	Migration activities for change of location	Please clarify on the commercial payouts for the bidder for the activities under the migration heading of the RFP	As the activites under the migration heading is one-of in nature, we suggest that the bidder could be paid at actuals.	As migration is planned in january 2022, this will be a component in implementation piece subjected to delivery of device
136	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021	37	Section-9 - Technical specifications	A solution must support 2 10GE Gigabit Ethernet (GBE) (Optical/Copper) and 2 or more 1GE.	Request to kindly amend the clause as "The number of http connection and concurrent users for sizing along with Performancer SLA. Point No 2.2 already mentioned "Maximum supported concurrent SSL sessions on single device should be 200K concurrent SSL flow states.		This requirement is from network port (NIC) presepective for connectivity in DC network
137	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 - Technical specifications	The bidder should have support offices in Mumbai, Hyderabad and Chennai.	Request to Amend the clause as "Bidder must have support center in India and support must be available 24 by 7.		Support offices required in Mumbai, Hyderabad and Chennai as a part of Datacenter support in case of Hardware failure or any other technical issues which cannot be resolved remotely.
138	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 - Technical specifications	Solution should support IPv6 traffic, NTP server time synchronization, DNS configuration, Solution should have usable storage of 1TB+	Kindly Amend the clause as the solution must probvide DNS security and can prevent data exfiltration		This point is related to the system configuration for NTP and DNS servers of NPCI

139	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 Technical specifications	Solution/appliance to provide High Availability (HA) and Load Balancing functionality and must have RAID redundancy (for hard drives), Network redundancy (for management network interfaces) and Power-Supply module redundancy.	Kindly Amend the clause as Solution must provide HA and 99.999 percent uptime		This is related to hardware component of the solution
140	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 Technical specifications	The solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network simultaneously on a single appliance	We have multiple deployment options like IPSEC / JRE Tunneling, PAC Files, and Zscaler Client Connector		OK
141	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 Technical specifications	The solution should integrate with LDAP directory like Active Directory, for user authentication and authorization. Integration with PIM/PAM solution	We can integrate solution with LDAP directory but Need ,ore clarification on integrate with PIM/PAM solution as the solution is hosted on cloud		On-prem solution should be integrated with PIM/PAM solution and access shouldn't be given directly from user's system.
142	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 Technical specifications	Solution should integrate with existing DLP, APT/SSLVA solution	1. Zscaler can forward information about transactions that trigger DLP policies to your third party solution. Zscaler uses secure Internet Content Adaptation Protocol (ICAP) to do this. https://help.zscaler.com/zia/about-data-loss-prevention 2. Zscaler enables endpoint-to-cloud security through integrations with leading Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) solutions. https://www.zscaler.com/partners/technology/endpoint-security 3. Zscaler security solution inspect full SSL across all ports and protocols and never run out of inspection capacity. Integration with SSLVA may required extra hop and may add latency		This is required to provide solution as per existing DC setup requirement
143	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 Technical specifications	Roaming user and Onsite user policy access management will be done from single Policy Management console. (The solution should be capable of applying 2 different types of disposition and action for a specific Web category with 1 single policy and this should be applied on the fly for both roaming-off site and on premise users.)	Need clerification		As part of hybrid requirement, requirment to have single pane of control for cloud based policy and onprem device policy

144	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 - Technical specifications	The solution should provide geo-location awareness for security incidents. The solution should provide inbuilt capability malicious content of password and unknown encryption files.	Need clerification		Need more clarity on question
145	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 - Technical specifications	A solution should support hostname resolution through either NetBios Lookup or reverse DNS. (Asset Identification).	Need clerification		This clause is related to asset identification from where query is getting generated (Hostname/IP address)
146	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 - Technical specifications	Solution shall support role-based administration such as Administrator, Malware Analyst, Database Reader, and Read-only access user	Need clerification		Given terminologies are example purpose only. Need to have role based administrations.
147	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 - Technical specifications	It should support SNMP v2c,V3 and above	Zscaler solution & monitoring for any critical events		what is the question here
148	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 - Technical specifications	The solution should block users when multiple (configurable) numbers of policy violations are triggered simultaneously.	Need more clarity		This is requirement in case of breach or attack scenerio. There should be a conffigurable limit for minimum violations before blocking.

149	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 - Technical specifications	Ability to import server side certificates and private keys for decryption	Zscaler is a forward proxy solution & cannot use as reverse proxy, Need more clarification on use case		Point is to import internal CA signed certificate Proxy server
150	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 - Technical specifications	Ability to do CA revocation management			Point is to support CRL check and OCSP calls through proxy
151	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 - Technical specifications	Ability to support OCSP stapling?			Point is to support CRL check and OCSP calls through proxy
152	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 - Technical specifications	Is the device FIPS 140-2 certified?	https://ir.zscaler.com/news-releases/news-release-details/zscaler-security-cloud-receives-fips-140-2-validation-encryption		Need more clarity on question
153	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 - Technical specifications	Maximum supported concurrent SSL sessions on single device should be 200K concurrent SSL flow states.	Since we do 100 percent SSL, hence may not required		Okay

154	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 Technical specifications	Solution shall provide forensic evidence on the infections activity within the network as follow: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviors, malware type, severity, source and destination of attack	We provide very rich logs in Dashbaord about the source, destination , URL etc		Okay
155	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 Technical specifications	The solution should apply security policy to more than 100 protocols in multiple categories more than 15. This includes the ability to allow, block, log, and assign quota time for IM, P2P, and streaming media and solution should provide at least below mentioned security categories as below RIGHT FROM DAY ONE : 1) Advanced Malware Command and Control category 2) Advanced Malware payload detection category 3) Malicious embedded links and iframe detection category 4) Mobile malware category 5) Key logger and Spyware category 6) P2P software database from day 1 to control/block the below P2P protocols.	Kindly Add/ Amend the clause as " Solution shoud support all ports and protocol and must have IPS fucntion from the day 1.		Need more clarity on question
156	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 Technical specifications	Both the proxy solution should provide regulatory compliance reports for PCI,ISO,SOX,FISMA,GLBA as applicable.	Need more clarification and Use case for this Point		Solution should be complaint to the standards, PCI compliance will suffice
157	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 Technical specifications	The appliance should integrate with the current Active directory for user authentication to access internet.	Kindly Amend the clsur as " Proposed solution must support SAML2.0"		Active directory integration should be supported
158	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 Technical specifications	Solution should have flexibility for rule/policy enforcement. i.e. Solution should allow administrator to enforce the policy/rule selectively for remote users and LAN users from the same console. E.g. if Rule A / Policy A should be enforced on LAN users but not on Remote users and vice versa. (Option to choose for where to enforce the policy -for remote users OR LAN users). Additionally if required the same policy/rule should be able enforced for both i.e. remote users and LAN users.	Policy can be bifurcate basis on Location		Okay

159	Request for proposal for procurement of Secure Web Gateway solution RFP Reference No: NPCI/RFP/2021-22/IT/09 dated 05.10.2021		Section-9 - Technical specifications	The solution should have complete license for Antivirus, SSL, Secure web gateway and content inspection.	Kindly Amend the clause as " The solution must have AV protection , 100 percent SSL inspection wihout performace degradation along NGFW Firewall.		This is specific requirement as per NPCI architecture
160	RFP	29	8.15	Penalty for non-adherence to SLAs	We request that the SLA penalties be capped cumulatively for all instances at 5% of the quartely invoices.		No change in RFP terms
161	RFP	31	8.22	Indemnity	We submit that we shall defend (settle and/or pay damages awarded by the court) NPCI against any third party claims arising from the following: a. Claims for loss or damage to third party tangible property; b. claim by any person in respect of bodily injury or death; c. claims by any third party in respect of any IP infringement; brought against or recovered from NPCI by reasons of any act or omission attributable to us or our agents or employees in the performance of the contractual obligation.		No change in RFP terms
162	RFP	31	8.23	Bidder's Liability	We submit that there are no exceptions to the disclaimer of liability for indirect damages and all exceptions should only apply to overall liability cap. Both parties agree that neither party shall be liable for any indirect, remote, consequential loss or damages including but not limited to loss of profit, loss of anticipated earning, loss of data, revenues, goodwill, or business value whether or not that party was aware or should have been aware of the possibility of such costs, expenses or damages.		No change in RFP terms
163	RFP	32	8.25	Exit option and contract re-negotiation	We understand that in the event of termination, we will be paid for all goods/services delivered till the effective date of termination.		No change in RFP terms
164	RFP	33	8.26	Extension of Contract	We submit that the services shall be provided as per the specifications agreed between the parties. Further, any extension shall be on mutually agreed terms and NPCI cannot unilaterally impose obligations for extension. Further, any change in the scope of work, including quantities, shall follow a change request process.		No change in RFP terms
165	RFP	33	8.27	Order Cancellation	We submit that prior to termination, we are provided with a cure period of at least 30 days. Further, we request deletion of the following portion of the clause: *'In case of order cancellation, any payments made by NPCI to the Bidder for the particular service would necessarily have to be returned to NPCI with interest @ 15% per annum from the date of each such payment .'*		No change in RFP terms
166	RFP	33	8.29	The Bidder agrees that after completion of the Term or upon earlier termination of the assignment the Bidder shall, if required by NPCI, continue to provide facility to NPCI at no less favorable terms than those contained in this RFP. In case NPCI wants to continue with the Bidder's facility after the completion of this contract then the Bidder shall offer the same terms to NPCI.	We request deletion of this portion of the clause.		No change in RFP terms

167	RFP	35	8.32	The Bidder confirms to NPCI that it complies with all Central , State, Municipal laws and local laws and rules and regulations and shall undertake to observe, adhere to, abide by, comply with and notify NPCI about compliance with all laws in force including Information Technology Act 2000, or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and for all purposes of this RFP, and shall indemnify, keep indemnified, hold harmless, defend and protect NPCI and its officers/staff/personnel/representatives/agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any defaultor failure on its part to conform or comply with the above and all other statutory obligations arising there from.	We submit that we will indemnify for fines and penalties payable by NPCI as a result of a direct breach by us of the applicable laws.		No change in RFP terms
168	RFP	35	8.34	Intellectual Property Rights	We submit that there will be no transfer of ownership of any intellectual property. NPCI grants us a non-exclusive, worldwide, royalty-free right and license to any intellectual property that is necessary for us and our designees to perform the ordered services. If deliverables are created by us specifically for NPCI and identified as such , we hereby grant NPCI a worldwide, non-exclusive, fully paid, royalty-free license to reproduce and use copies of the deliverables internally. We shall retain ownership of: a. all pre-existing Intellectual Property Rights ("IPR") and; b. all IPR in materials and reports etc. developed during the course of the agreement and remain therefore able to re-use any copyrightable or patentable elements of the materials and report in future engagements.		No change in RFP terms
169	RFP	24	8.4	8.4 Performance Bank Guarantee The Successful bidder shall, within 14 working days of receipt of Purchase Order, submit a Performance Bank Guarantee (PBG) equal to 10% of total value of the Purchase order (exclusive of taxes), valid for 1 year, with a claim period of 12 (twelve) months from the date of expiry of the validity period of the Bank Guarantee (BG)	We request for PBG to be furnished within 30 days from receipt of purchase order. Further we request for PBG claim to be valid for 3 months from date of expiry of contract period.		No change in RFP terms
170	RFP	26	8.11	8.11 Penalty for default in delivery If the successful bidder does not deliver & implement the solution as per the above delivery schedule, or such authorized extension of delivery period as may be permitted in writing by NPCI, NPCI shall impose a penalty as given below: ¤ Non Delivery of above at NPCI - at the rate of 0.5% of the total Purchase Order value for each week's delay beyond the stipulated delivery period subject to a maximum of 5% of the PO value. ¤ In case the delay exceeds 10 days beyond the stipulated delivery period of RFP, NPCI reserves the right to cancel the order without prejudice to other remedies available to NPCI	We request for penalty imposition as below ¤ Non Delivery of above at NPCI - at the rate of 0.5% of the undelivered Purchase Order value for each week's delay beyond the stipulated delivery period subject to a maximum of 5% of the PO value. ¤ In case the delay exceeds 10 days beyond the stipulated delivery period of RFP, NPCI to give 30 days notice period before canceling the order.		No change in RFP terms
171	RFP	26	8.13	8.13 Warranties	Bidder submits that for any replacement warranty shall be extended until expiry of the balance life period for the first replacement only.		No change in RFP terms
172	RFP	30	8.17	8.17 Repeat Order: NPCI reserves the right to place Purchase Orders with the selected bidder(s) for any or all of the goods and/or services included in the Solution at the agreed unit rate for individual categories of purchase order during the period of 3 years from the date of award / 1st Purchase Order.	Bidder submits that pricing for any repeat order will be agreed mutually at the time of repeat order.		No change in RFP terms
173	RFP	30	8.19	Payment Terms	Bidder requests for payment within 30 days from date of issue of invoice.		No change in RFP terms

174	RFP	30	8.2	In case NPCI wishes to shift the devices from one place to another anywhere in the country, adequate support will be made available by the bidder by arranging field engineer for the purpose of dismantling of devices/software/service supplied by Service provider & hand-over to the concerned Officials or Data Center, pre-shifting inspection, post-shifting inspection, re-installation etc. of all devices supplied by Service provider.	Relocation of devices may require planning and reconfiguration. Such activities may be mutually agreed and executed as per additional commercial CR. While all precautions are taken care, NPCI Should Insure the items (end to end) during any kind of relocation / migration.		No change in RFP terms
175	Section 9 - Technical Specifications	37	1.13	Solution should integrate with existing DLP, APT/SSLVA solution	Please confirm the existing DLP, APT/SSLVA solution used by NPCI.		DLP- Forcepoint, SSLV- F5, APT- FireEye NX
176	Section 9 - Technical Specifications	38	1.17	The solution should provide geo-location awareness for security incidents. The solution should provide inbuilt capability malicious content of password and unknown encryption files.	Please confirm the relation of geolocation awareness for security incidents with encryption or malware detection. If a file is encrypted with an 'unknown key' there is no way for any web gateway to examine it for malicious content. Encrypted files can be blocked based on detection of encryption in combination with other criteria. For example you could make exceptions such that encrypted files from certain domains or categories are allowed while all other encrypted files are blocked. Hence, it is requested to amend the specification as follows: *"The solution should provide geo-location awareness for security incidents. The solution should be able to block the encrypted files based on detection of encryption in combination with other criteria."*		Will discuss in Technical Round
177	Section 9 - Technical Specifications	41	2.12	Protocol Support – SPDY, HTTP/2 and HTTP/3	Please note that SPDY is an earlier version of HTTP/2 that is no longer in use. HTTP/3 is/will be UDP based and is not able to be traditionally proxied. Hence, please amend the specificatiosn to as follows: "Protocol Support - HTTP/2, FTP, SOCK(s)."		Requirement is to support SPDY, HTTP/2, HTTP/3 can be consider as future support.
178	Section 9 - Technical Specifications	41	2.14	Support passing Jumbo Frame IP traffic	Please note that 'Jumbo frames' are a network level concept. Web Gateway is an application layer proxy intended to filter traffic between clients on the local network and servers on the Internet. The general Internet does not support Jumbo Frame traffic as it is not defined by the 802.3 specification. This specification is targeted at firewall or IPS type network devices that may operate exclusively on local network traffic where jumbo frames could be used. Hence, in order to promote fair competition, it is requested to remove this clause.		This is for network setting for troubleshooting purposes to modify MTU size if required (Good to have).
179	Section 9 - Technical Specifications	41	2.20	Ability to support OCSP stapling?	Please clarify the expectation from the support for OCSP Stapling, as this requirement is ambiguous.		Point is to support CRL check and OCSP calls through proxy

180	Section 9 - Technical Specifications	42	3.7	The solution should apply security policy to more than 100 protocols in multiple categories more than 15. This includes the ability to allow, block, log, and assign quota time for IM, P2P, and streaming media and solution should provide at least below mentioned security categories as below RIGHT FROM DAY ONE : 1) Advanced Malware Command and Control category 2) Advanced Malware payload detection category 3) Malicious embedded links and iframe detection category 4) Mobile malware category 5) Key logger and Spyware category 6) P2P software database from day 1 to control/block the below P2P protocols.	Our solution is one of the world's best in class Web gateway and it is not intended to be a general purpose multi-protocol firewall. McAfee have announced plans to support multi-protocol firewalling in the cloud but we have no plans to support filtering of protocols other than SOCKs, HTTP/S, and FTP with our on premise appliances. Multi-protocol firewalls do not provide sufficient filtering capabilities for HTTP/S traffic. They are a complementary solution for an enterprise class web gateway. Hence, in order to promote fair competition - it is requested to remove this specification.		Will discuss in Technical Round
181	Section 9 - Technical Specifications	42	3.5	The solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future data leakage by the malware.	Please elaborate on the use case.		Solution should able to provide indepth details of Malicious traffic originated from system such as host details, browser, type of attack etc.