

**Replies to Pre-bid Queries for Request for Proposal for procurement of Appliance based Proxy Solution  
NPCI/RFP/2015-16/IT/009 dated 10.07.2015**

S.No	Document Reference	Page No	Clause No	Description in RFP	Clarification sought	Additional Remarks (if any)	NPCI Response
1	Technical Specifications	29	1	The Secure Web gateway offering should be appliance based solution designed for secure proxy and active content caching services. The appliance should have minimum 6 to 10 interfaces upgradable to GE SFP ports.	We assume that active caching is required only for dynamic content and not static content. Kindly clarify. Also request you to restrict the port count to Minimum 4 no's of RJ45 Ports.		The appliance should support caching and Appliance should have Minimum 4 GE Interfaces for data/user traffic excluding a dedicated management interface.
2	Technical Specifications	29	3	The appliance management console should have a single control mechanism in form of 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.)	We can create an access policy that is set to block all, and then just keep it disabled until the time is needed (then enable). Or... just disable the web proxy and https proxy service temporarily. Is that Ok with NPCI. Please clarify. Does NPCI need very aggressive web access policy for their users or not. Such type of configurations may also lead to a lot of false positives in the environment and user complaints.		Understanding is correct and control mechanism should be achieved through proxy.
3	Technical Specifications	29	6	The Solution should have the capability to decrypt the SSL traffic and subsequently feed decrypted traffic to one passive device (IDS, Security Analytics etc) for further analysis	The logs can be passed onto the SIEM for further analysis. What is the need to have capability to decrypt the SSL traffic on the device and then send it to One Passive device. ?		All the logs including SSL logs should be passed though SIEM for further analysis.
4	Technical Specifications	29	8	The solution should support content pre-population. The administrator should have the ability to download the content beforehand and make it available for the user from the proxy appliance	Require more details - what does NPCI want to achieve with the requirement in this clause. We see a security risk if the administrator has the ability to download the content before or even after.		It's an optional feature and not an mandate requirement.
5	Technical Specifications	29	11	The Proxy solution should generate alerts to designated administrator and senior management via email, and SMS.	For SMS - All solutions require a third party SMS gateway solution which works on email alerts sent to it. Please confirm whether NPCI has a sms gateway in place.		Solution should have the capability to integrate with the third party SMS gateway solution if required in future. Email solution is a must.
6	Technical Specifications	29	12	Should have capability to integrate with SIEM tool, also should report alerts via sms.			Same as the response of clause no11.
7	Technical Specifications	30	15	It should also have feature of Reverse proxy and also support Terminal services /Citrix Client.	Qwhy does customer want to use the same appliance for reverse proxy purposes. Does NPCI have a REAL need for reverse proxy. Also why does NPCI wants support for Terminal services/citrix client		Reverse proxy is a mandatory requirement.
8	Technical Specifications	30	17	The proposed solution should support user/ip/mac binding functionality	user and IP binding functionality is possible on proxy. Mac binding is not a proxy feature. Request you to remove the same.		The proposed solution should able to group the users based on IP or user credentials.
9	Technical Specifications	30	19	The proposed solution should support 3G/Wimax/Datacard support to be used as dedicated internet link.	does the customer want to terminate Internet link directly on the Proxy appliance.		No and support 3G/Wimax/Datacard support is not required

10	Technical Specifications	30	20	Both the proxy solution should provide regulatory compliance reports for PCI, ISO, SOX, FISMA, GLBA as applicable.	This clause looks to be incomplete as it says "Both" - what is this both - what is NPCI trying to refer as a second solution along with proxy?		Proxy solution should provide regulatory compliance reports for PCI, ISO, SOX, FISMA, GLBA as applicable.
11	Technical Specifications	30	21	The proposed solution should support scanning of SMTP, SMTPS , POP3, IMAP, FTP over HTTP protocols.	What is the need to include email related protocols on a Web Gateway solution. Request you to remove this point.		The proxy should support RPC over HTTPS and HTTP.
12	Technical Specifications	31	32	The solution should be integrated with existing DLP and APT solution.	Since NPCI is using Fireeye APT, Integration is not possible. Request you to remove integration with APT Solution.		Vendor should ensure after placing their solution there should not be any compatibility issue in the existing APT & DLP solution.
13	Technical Specifications	31	33	The bidder should ensure that the appliance based solution is sized accordingly for 70% SSL Traffic	Query - 70% SSL traffic is huge. SSL Traffic typically is in the range of 30-40%.what is the criteria used by NPCI to achieve this percentage of SSL traffic.		Considering the future requirements this percentage is expected anything more than 40%
14	Technical Specifications	31	35	The solution should ensure capabilities of caching to be quantified upto 25%.	Pl. elaborate on the requirement here.		No change in RFP
15	Technical Specifications	31	30	The solution should ensure reverse proxy functionality with web acceleration feature including security and anonymity	why does NPCI want to use the same appliance for reverse proxy purposes.		Reverse proxy is a mandatory requirement
16	Technical Specifications	32	44	The solution should provide decryption of unverified encrypted traffic for scanning and then re-encrypt it before sending (SSL decryption).	What is the need to re-encrypt the traffic again before sending.		For AV inspection we require this .No change in RFP
17	Technical Specifications	32	45	The appliance should have Capability to restrict internet usage for end-users with ability to set limits in terms of daily/Weekly/Monthly download limits	Pl Keep the capability to restrict as per Daily and Weekly. Remove Monthly.		No Change in RFP
18	Technical Specifications	32	50	It should have capability to maintain records for 126 Months. Ability to take backup of logs and also d generate Monthly Reports and trend reports for 6 -12 months.	Kindly confirm what type of records and logs will be required to be maintained for 126 months and what is the transactions per second.		126 months is a typo so ignore it. It should have capability to maintain records for 4 Months. Ability to take backup of logs and also generate Monthly Reports and trend reports for 6 -12 months.
19	Technical Specifications	32	51	Policies based on Geo locations as destination.	why this is required. Pls clarify		Irrespective of any locations user polices should be enforced .

20		29	8	The solution should support content pre-population. The administrator should have the ability to download the content beforehand and make it available for the user from the proxy appliance	Content Pre Population is true for IPS, which is not a part of the RFP. Content Filtering generally takes updates from the cloud which works in a real time update scenario		It's an optional feature and not an mandate requirement.
21		29	11	The Proxy solution should generate alerts to designated administrator and senior management via email, and SMS.	Since the Proxy Solution would be integrated with SIEM, which usually has the feature of SMS alert. Request you to make it as email notification only.		Solution should have the capability to integrate with the third party SMS gateway solution if required in future.Email solution is a must.
22		29	12	Should have capability to integrate with SIEM tool, also should report alerts via sms.	Since the Proxy Solution would be integrated with SIEM, which usually has the feature of SMS alert. Request you to make it as email notification only.		Same as the response of clause no11.
23		31	31	The solution should provide file filtering for upload/download.	Does this point include understanding the content of the file attached and block it by keywords?		The solution should have the capacity to control the content of download and upload .
24		31	32	The solution should be integrated with existing DLP and APT solution.	Proxy can be integrated with different DLP solutions using ICAP protocol. Request more clarification for APT's and if the expected integration is through ICAP		Vendor should ensure after placing their solution there should not be any compatibility issue in the existing APT & DLP solution.
25		32	40	The solution should ensure reverse proxy functionality with web acceleration feature including security and anonymity	Web acceleration is generally used on the gateway appliance where Multiple ISP's are connected. Request you to make it only as a Reverse Proxy		Mandatory requirement
26		32	46	The solution should block users when multiple (configurable) numbers of policy violations are triggered simultaneously.	Proxy Generate indept report of the blocked web attempts, which can be analyzed and policies for the same can be applied in case if required. Automatic Blocking might result in dummy calls which would not necessarily because of users accessing sites which are non productive. request to make it as block users with manual intervention by the administrator		OK
27		32	49	The solution should be able to generate, export reports in below mentioned formats i.e. PDF, Word, excel, html .Also it should be able to alerts via sms.	Since the Proxy Solution would be integrated with SIEM, which usually has the feature of SMS alert. Request you to make it as email notification only.		The solution should be able to generate, export reports in below mentioned formats i.e. PDF, Word, excel, html.
28		23	8.13	Payment Terms	We request 70% on Delivery of Appliance(s)/ Equipment, AND 30% after Installation and Sign-Off from NPCI.		No change in RFP

29	NPCI/RFP/2015-16/IT/009	29	1	The Secure Web Gateway Offering should be appliance based solution designed for secure proxy and active content caching services. The Appliance should have Minimum 6 to 10 Interfaces upgradable to GE SFP Ports	Kind amend this to the Appliance should have Minimum 6 Interfaces		Appliance should have Minimum 4 GE Interfaces for data/user traffic excluding a dedicated mangament interface.
30	NPCI/RFP/2015-16/IT/009	29	2	The solution should track and block sharing of Internet access from different IP source. Prevention of concurrent login / sharing of internet access by using same credentials (user id & password) from multiple workstations. E.g. User1 logged in with User1admin; User2 should not be able to log in with User1admin	Kindly note this point is a feature of identity management solutions and your Active directory .however you have clarified that this meant that user based policies should be applicable irrespective of whichever machine the user log in from		The solution should identify request from two different sources with same credential. That means at any given point ,the use should be able to login from single IP.
31	NPCI/RFP/2015-16/IT/009	29	6	The Solution should have the capability to decrypt the SSL traffic and subsequently feed decrypted traffic to one passive device (IDS, Security Analytics etc) for further analysis	Kindly amend this point that the solution should provide feeds to SIEM solutions .Since your earlier requirement of prviding feeds to IDS does not aulify in a proxy requirement		All the logs including SSL logs should be passed though SIEM for further analysis.
32	NPCI/RFP/2015-16/IT/009	29	10	The solution should be able to discover and classify, protect data within all infrastructure of NPCI, in file shares, databases and collaboration tools like SharePoint	This is a pure DLP requirement and can be achieved if DLP license will be activated .However since you do not require DLP this point needs to be removed		It's an optional feature .
33	NPCI/RFP/2015-16/IT/009	29	11	The Proxy solution should generate alerts to designated administrator and senior manager via email and SMS	The Proxy solution should generate alerts to designated administrator via email only .You need to delete the SMS reqt		Solution should have the capability to integrate with the third party SMS gateway solution if required in future.Email solution is a must.
34	NPCI/RFP/2015-16/IT/009	29	12	Should have Capability to integrate with SIEM Tool, also should alert via SMS	Should have Capability to integrate with SIEM Tool.You need to delete the SMS reqt		Same as the response of clause no11.
35	NPCI/RFP/2015-16/IT/009	30	15	It should also have feature of Reverse Proxy and also support terminal Services / Citrix client	Kindly remove the requirement for reverse proxy since yours is a pure forward proxy requirement and the purpose of a reverse proxy is primarily for WAF for which you are already using Imperva in your environment		Reverse proxy is a mandatory requirement.
36	NPCI/RFP/2015-16/IT/009	30	17	The proposed solution should support user/ip/mac binding functionality	This is a SSL VPN functionality and has no prevalence in a Proxy scenario for the endpoints.You are reequested to remove this point		The proposed solution should allow to group the users based on IP or user credentials.
37	NPCI/RFP/2015-16/IT/009	30	18	The proposed solution should support session time out and idle time out facility to forcefully logout the users.	We have time based facility available		OK

38	NPCI/RFP/2015-16/IT/009	30	21	The proposed solution should support scanning of SMTP, SMTPS, POP3, IMAP, FTP over HTTP protocols.	If the Mail is accessed from outlook it will use RPC over Https which is supported by proxy. If the mail is accessed from browser (like https://webmail.npci.com/) as application which would be purely HTTPS and would be supported by proxy. Other than this no proxy would be able to support SMTP/POP3/IMAP Protocols as they are part of Email channel and not Web Channel.		The proxy should support RPC over Https and HTTP.
39	NPCI/RFP/2015-16/IT/009	30	23	The proposed solution should provide option to define different bandwidth and policy.	Sir,this option is a packet shaping option available with your firewall and multiple packet shaping tools .We request you to remove this point		Understanding is correct.
40	NPCI/RFP/2015-16/IT/009	31	31	The Solution should provide file filtering for upload / download	Sir Please change this option to "The Solution should provide file filtering for download".		The solution should have the capacity to control the content of download and upload .
41	NPCI/RFP/2015-16/IT/009	31	32	The solution should be integrated with existing DLP and APT solution.	FireEye can be placed ahead of Websense Proxy (between proxy and internet) in the bridge mode. Having Said that with the help of websense proxy 95% of APTs can be taken care of.		Vendor should ensure after placing their solution there should not be any compatibility issue in the existing APT & DLP solution.
42	NPCI/RFP/2015-16/IT/009	31	33	The Bidder should ensure that the appliance based solution is sized accordingly for 70% SSL Traffic	Kindly confirm if NPCI's existing usage of SSL sites are 70%. Websense being the most commonly used proxy we have seen the SSL site access of any organization has not been more than 40 to 50%		Considering the future requirements this percentage is expected anything more than 40 %
43	NPCI/RFP/2015-16/IT/009	31	37	The solution should monitor and block instant messaging (IM) based file transfer	This is a pure DLP requirement and can be achieved if DLP license will be activated .However since you do not require DLP this point needs to be removed		The solution should have atleast a feature to block and allow Peer to Peer or any IM /chat .
44	NPCI/RFP/2015-16/IT/009	31	40	The solution should ensure reverse proxy functionality with web acceleration feature including security and anonymity	Kindly remove the requirement for reverse proxy since yours is a pure forward proxy requirement and the purpose of a reverse proxy is primarily for WAF for which you are already using Imperva in your environment .The web acceleration feature is available in load balancers like Radware/F5 which provide reverse proxy/web acceleration solutions.		Same as clause no 15
45	NPCI/RFP/2015-16/IT/009	32	43	The Available bandwidth is 45 Mbps that is expected to be scaled to 150Mbps at each location.	Is 45Mbps bandwidth used only for Web Traffic alone or is it used for all the traffic like SMTP, Application hosting, etc... Usually we have seen 50 to 60% of the total bandwidth is consumed by Web Traffic and rest for SMTP and application hosting. Websense appliances are sized based on the Web Traffic Bandwidth, and considering each page would at an average would be 10KB, for 100Mbps there could be around 1280 Web Transactions per second.		45 Mbps bandwidth is used by web and other applications .Out of which Web traffic is around 50 %.
46	NPCI/RFP/2015-16/IT/009	32	45	The appliance should have Capability to restrict internet usage for end-users with ability to set limits in terms of daily/Weekly/Monthly download limits	Sir,this option is a packet shaping option available with your firewall and multiple packet shaping tools .We request you to remove this point		No Change in RFP

47	NPCI/RFP/2015-16/IT/009	32	49	The solution would be able to generate, export reports in below mentioned formats i.e. PDF, Word, Excel, Html, Also it should be able to alert via SMS	Kindly amend the staetement to The solution would be able to generate, export reports in below mentioned formats i.e. PDF, Excel, HTML.Kindly delete the SMS statement		The solution should be able to generate, export reports in below mentioned formats i.e. PDF, Word, excel, html.
48	NPCI/RFP/2015-16/IT/009	32	51	Policies based on Geo locations as destination.	This is a NGFW feature not available in proxies. Request you to remove this point		Irrespective of any locations user polices should be enforced .
49	NPCI/RFP/2015-16/IT/009	32	54	Allocation of Volume Quota: Assign download/upload, internet browsing quota limit to user / users / group /groups /client/clients etc.	Sir,this option is a packet shaping option available with your firewall and multiple packet shaping tools .We request yo u to remove this point		No change in RFP
50	NPCI/RFP/2015-16/IT/009	32	55	On reaching the quota limit the internet access should be blocked automatically with notification to users.	Sir,this option is a packet shaping option available with your firewall and multiple packet shaping tools .We request yo u to remove this point		No change in RFP
51	NPCI/RFP/2015-16/IT/009	33	59	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.	Please mention in addition the mentioned statement Remote Filtering option has to be made with a onpremise solution only .Cloud based filtering solutions will not be accepted	Kindly provide the number of users for remote filtering licences	No of roaming users is around 200 at present but future scalability should be taken care.On premises solution is expected.
52	NPCI/RFP/2015-16/IT/009	33	63	The solution should must detect and protect against anonymizing websites, anonymizing tools	Kindly amend the statement to The solution should must detest and protect against anonymizing websites which are being accessed thru the proxy		Understanding is correct it should detect and protect the website access through proxy
53	NPCI/RFP/2015-16/IT/009					Also request you to ask for vendors gartner rleadere quadrant only.	No change in RFP .
54	RFP Ref No. NPCI/RFP/2015-16/IT/009 dated 10.07.2015	11	Section 4-Eligibility Criteria-Point No.6	The bidder should provide reference of 2 clients in BFSI segment who have procured, installed including ongoing support for Appliance based Proxy configured in DC-DR Model during the last 3 years as on date of submission of bid	We would request NPCI to consider "The Bidder solution should have at least 1 live installation of Appliance based proxy solution as on date submission of bids."	The proposed/requested amended clause was the part of the earlier RFP released by NPCI for APT solution RFP Reference No. NPCI/RFP/2014-15/IT/003 dated 10.6.2014	No change in RFP .
55	RFP Ref No. NPCI/RFP/2015-16/IT/009 dated 10.07.2015	29	Section 9 - Technical Specifications	The Proxy solution should generate alerts to designated administrator and senior management via email, and SMS	Is NPCI expecting the System integrator to also quote for third party SMS appliace gateway for IT alerts and notifications or Do NPCI will integrate with their current SMS appliance?	Proxy can support alerts via smtp, SNMP. For SMS support the solution needs to be integrated with third party SMS appliance gateway for IT alerts and notifications - A plug and play device that integrates easily with existing applications like email, database and application servers	Solution should have the capability to integrate with the third party SMS gateway soultion if required in future.Email solution is a must.

56	RFP Ref No. NPCI/RFP/2015-16/IT/009 dated 10.07.2015	29	Section 9 - Technical Specifications	Should have capability to integrate with SIEM tool, also should report alerts via sms.	Is NPCI expecting the System integrator to also quote for third party SMS appliance gateway for IT alerts and notifications or Do NPCI will integrate with their current SMS appliance?	Proxy can support alerts via smtp, SNMP. For SMS support the solution needs to be integrated with third party SMS appliance gateway for IT alerts and notifications - A plug and play device that integrates easily with existing applications like email, database and application servers	Solution should have the capability to integrate with the third party SMS gateway solution if required in future. Email solution is a must
57	RFP Ref No. NPCI/RFP/2015-16/IT/009 dated 10.07.2015	30	Section 9 - Technical Specifications	The proposed solution should support user/ip/mac binding functionality	This is not features of Proxy Solution. Request you kindly remove this clause	Proxy should support the traffic flow from source IP/MAC/user binding done using external AAA/LDAP/AD. The Proxy does not support binding of IP to MAC address or IP to username on the Proxy platform itself. This is a AAA functionality. And the proxy does not host any AAA functionality for performance reason but can support any AAA solution like MSAD/LDAP/Novell/Lotus/Oracle Core-id etc.	The proposed solution should be able to group the users based on IP or user credentials.
58	RFP Ref No. NPCI/RFP/2015-16/IT/009 dated 10.07.2015	30	Section 9 - Technical Specifications	The proposed solution should support scanning of SMTP, SMTPS, POP3, IMAP, FTP over HTTP protocols.	Request to remove this clause as this is not functionality of web Gateway/proxy	This is not feature of Proxy solution, this is feature of email gateway and also, This requires integration with out of box solution like SAP(Security Analytics and Global Threat Intelligence).	The proxy should support RPC over Https and HTTP.
59	RFP Ref No. NPCI/RFP/2015-16/IT/009 dated 10.07.2015	30	Section 9 - Technical Specifications	The solution should have multiple Anti- Virus engines for scanning AV and other malwares on the Web traffic. Enabling AV should not degrade the performance of and Proxy solutions.	Should AV engines can be freeware or non branded or NPCI expects the SI to quote top 5 AV engine in the industry. Also Please suggest should the AV engine be of a different brand from the endpoint AV engine?	The solution should have AV engines which are different as compared to the endpoint AV solution of the customer. AV engines should be branded amongst atleast top 5 in the industry and not any freewares	The AV engine should not be a freeware and only from all top AV engine available in industry. A different AV engine is expected which should not be same as existing endpoint AV engine.
60	RFP Ref No. NPCI/RFP/2015-16/IT/009 dated 10.07.2015	31	Section 9 - Technical Specifications	The solution should ensure capabilities of caching to be quantified up to 25%	Please clarify how NPCI will cache large Size objects / Videofile / Streaming content ?	The solution should ensure capabilities of caching to be quantified up to 80% of the disk size and single object cache size should be at least 1GB	We require caching for small objects files

61	RFP Ref No. NPCI/RFP/2015-16/IT/009 dated 10.07.2015	32	Section 9 - Technical Specifications	The solution should provide decryption of unverified encrypted traffic for scanning and then re-encrypt it before sending (SSL decryption).	request to please clarify, in this case what should be the minimum supported Key Size and the public key algorithm and cipher support?	Suggest to mention the key size as minimum 2048 bits and up to 8172 bits with supported public key algorithms like RSA,DH	2048 bits but need to check with the vendor if it will support with lower bit size
62	Table 9.1	29	1	The Secure Web gateway offering should be appliance based solution designed for secure proxy and active content caching services. The appliance should have minimum 6 to 10 interfaces upgradable to GE SFP ports.	Please elaborate NPCI's requirement for multiple interfaces for web gateway solution? This is OEM specific and suggest to be removed.		Appliance should have Minimum 4 GE Interfaces for data/user traffic excluding a dedicated management interface.
63	Table 9.1	29	3	The appliance management console should have a single control mechanism in form of 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 OEM specific and suggest to be removed. There should be other alternative ways/methods to be allowed and accepted to achieve the desired result.		No change in RFP. The control mechanism should be achieved through proxy.
64	Table 9.1	29	8	The solution should support content pre-population. The administrator should have the ability to download the content beforehand and make it available for the user from the proxy appliance	This is OEM specific and suggest to be removed. Allowing administrator to control the content for end users will impact the privacy and confidentiality of the user content. Please elaborate if our interpretation of the requirement is incorrect.		It's an optional feature and not a mandate requirement.
65	Table 9.1	29	10	The solution should be able to discover and classify, protect data within all infrastructure of NPCI, in file shares, databases and collaboration tools like SharePoint	This is OEM specific and related to Data Leakage Prevention solution. It does not come under scope of web gateway security solution. However, Web gateway solution should get integrated with existing DLP solution.		It's an optional feature.
66	Table 9.1	29	11	The Proxy solution should generate alerts to designated administrator and senior management via email, and SMS.	SMS based alert is OEM specific. Suggest SMS part of the requirement to be removed.		Solution should have the capability to integrate with the third party SMS gateway solution if required in future. Email solution is a must.
67	Table 9.1	29	12	Should have capability to integrate with SIEM tool, also should report alerts via sms.	SMS based alert is OEM specific. Suggest SMS part of the requirement to be removed.		Same as the response of clause no11.
68	Table 9.1	30	17	The proposed solution should support user/ip/mac binding functionality	MAC based binding is OEM specific. Suggest MAC part of requirement to be removed.		The proposed solution should be able to group the users based on IP or user credentials.
69	Table 9.1	30	19	The proposed solution should support 3G/Wimax/Datacard support to be used as dedicated internet link.	This is OEM specific. 3G/Wimax/Datacard are unreliable source of internet connectivity in the corporate and enterprise level infrastructure.		Support 3G/Wimax/Datacard support is not required

70	Table 9.1	30	20	Both the proxy solution should provide regulatory compliance reports for PCI, ISO, SOX, FISMA, GLBA as applicable.	Please elaborate the NPCI specific requirement. Generally such type of compliance reports are possible by customization in report.	Proxy solution should provide regulatory compliance reports for PCI, ISO, SOX, FISMA, GLBA as applicable.
71	Table 9.1	30	26	The solution should have multiple Anti- Virus engines for scanning AV and other malwares on the Web traffic. Enabling AV should not degrade the performance of and Proxy solutions.	"Enabling AV should not degrade the performance of Proxy solutions" is practically not feasible as there would be increase in the CPU cycles incase of AV/Malware scanning. However, it should not be significant.	Degradation should not more than 10 %.
72	Table 9.1	31	32	The solution should be integrated with existing DLP and APT solution.	Please elaborate the details of existing DLP and APT solution in NPCI environment.	Vendor should ensure after placing their solution there should not be any compatibility issue in the existing APT & DLP solution.
73	Table 9.1	32	49	The solution should be able to generate, export reports in below mentioned formats i.e. PDF, Word, excel, html .Also it should be able to alerts via sms.	As per industry standard reports are generally exported in PDF,HTML,CSV and XML format. Suggest "Word" format to be removed. "SMS" alert is OEM specific, suggest to be removed.	The solution should be able to generate, export reports in below mentioned formats i.e. PDF, Word, excel, html.
74	Table 9.1	32	53	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	Onsite support will be provided by SI who will proposing our solution.	OK
75	Section 8 - Terms and conditions	20	8.5	Taxes and Duties	"The benefits realized by supplier due to lower rates of taxes, duties, charges and levies shall be passed on by the Supplier to NPCI." <b><u>We request clause be amended to state that "Any changes in taxes shall be on account of NPCI. Any benefit due to reduction in taxes shall be passed on to NPCI and any burden due to increase in taxes shall be reimbursed on actual."</u></b>	No change in RFP
76	Section 8 - Terms and conditions	21	8.8	Penalty for default in delivery	The following clauses are applicable to High, Medium and low priorities incidents. a. Penalty for High priority incidents - Any violation in meeting the above SLA requirements, NPCI shall impose a penalty of INR 10,000/- (Indian Rupees Ten Thousand only) for each 30 minutes delay up to 4 hours, beyond 4 hours penalty would be INR 20,000 for each 30 minutes. b. Penalty for Medium Priority incidents: Any violation in meeting the above SLA requirements which leads to medium priority incident, NPCI shall impose a penalty of INR 5000/- (Indian Rupees Five Thousands only) per hour. c. Penalty for Low Priority incidents: Any violation in meeting the above SLA requirements which leads to low priority incident, NPCI shall impose a penalty of INR 1000/- (Indian Rupees One Thousand only) per hour.  <b>We request that a cap be defined for the penalties above, and they shall be in the aggregate for all the above, at 5% of the value of the respective purchase order value.</b>	No change in RFP

77	Section 8 - Terms and conditions	24	8.16	Indemnity	It is our understanding that the overall liability under the agreement includes any liability arising under Indemnity. Please confirm.		Liability and indemnity are separate independent terms.
78	Section 8 - Terms and conditions	24	8.16	Indemnity	We request that the indemnity shall only be restricted to third party claims for bodily injury death, IPR infringement Indemnity and violation of applicable law.		No change in RFP
79	Section 8 - Terms and conditions	24	8.18	Order Cancellation	We request that the second paragraph which refers to risk purchase upon termination of whole or part of the contract is made subject to certain conditions, i.e. (a) only after expiry of a reasonable cure period (b) NPCI shall have a duty to take reasonable mitigation steps as any person in similar circumstances would do to mitigate its own loss or damage. (c) Any procurement of undelivered services shall be made on the principles of competitive bidding. (d) We request this amount is capped to 5% of the value of the relevant purchase order.  Request confirmation that the refund shall only be made in case the Product is returned to Bidder.	A cure period will enable rectification of services prior to termination.  Mitigation of loss is the duty of the aggrieved party under Indian Contracts.  The request for procurement on principles of competitive bidding is for price discovery.  We request the cap to be at 5% of value of relevant purchase order and not value of impacted services.	No change in RFP
80	Section 8 - Terms and conditions	24	8.17	Bidder's liability	<b>We request the second and third paragraph of the clause to be read as:</b>  The Bidder's aggregate liability in connection with obligations undertaken under the purchase order, regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actual and limited to the annual value of the contract/purchase order, and shall exclude all indirect, consequential and incidental damages and compensation.  The Bidder's liability in case of claims against NPCI resulting from infringement of patents, trademarks, copyrights or such other Intellectual Property Rights or breach of confidentiality obligations shall be unlimited.		No change in RFP
81	Section 8 - Terms and conditions	25	8.2	Force Majeure	We request that it is clarified that the Bidder will be paid for all services upto the date of termination and any stranded costs for any investments made by Bidder.		No change in RFP clause .Clause does not prohibit payment upto occurrence of force majeure or on termination due to it. Payment upto occurrence of force majeure is obvious.
82	Section 8 - Terms and conditions	27	8.25	Intellectual Property Rights	<b>We request the addition of the clause below:</b>  Each party shall own all rights, title and interest in their pre-existing Intellectual Property rights and all modifications, enhancements or derivatives thereto.		No change in RFP. NPCI has not stipulated that it will own IPR in application or its updates.

83	Annexure Z - Non Disclosure Agreement	58	Article 12	Term	We request the clause in the NDA to be read as, since there is no term defined in the NDA:  This term of this Agreement shall be coterminous with the term of the main Contract. The obligations of each Party hereunder will continue and be binding irrespective of whether the termination / expiry of the Agreement for a period of one year after the termination / expiry of this Agreement.		No change in RFP
84	Section 8 - Terms and conditions	27	8.29	No Damage of NPCI Property	We request that the clause be read as:  Bidder shall ensure that there is no loss or damage to the property of NPCI while executing the Contract. In case, it is found that there is any such loss/damage due to direct negligence/non-performance of duty by any personnel, the amount of loss/damage shall be mutually agreed between the parties.		No change in RFP
85		23	8.13	8.13 Payment Terms	We request that the payment terms for hardware and software delivered be changed to 70% on delivery of all the material on site and 30% after installation.		No change in RFP
86				The Proxy solution should generate alerts to designated administrator and senior management via email, and SMS	The Proxy can support alerts via smtp, SNMP. For SMS support the solution needs to be integrated with third party SMS appliance gateway for IT alerts and notifications - A plug and play device that integrates easily with existing applications like email, database and application servers	Is NPCI expecting the System integrator to also quote for third party SMS appliance gateway for IT alerts and notifications or Do NPCI will integrate with their current SMS appliance?	Solution should have the capability to integrate with the third party SMS gateway solution if required in future.Email solution is a must
87				Should have capability to integrate with SIEM tool, also should report alerts via sms.	The Proxy can support alerts via smtp, SNMP. For SMS support the solution needs to be integrated with third party SMS appliance gateway for IT alerts and notifications - A plug and play device that integrates easily with existing applications like email, database and application servers	Is NPCI expecting the System integrator to also quote for third party SMS appliance gateway for IT alerts and notifications or Do NPCI will integrate with their current SMS appliance?	Solution should have the capability to integrate with the third party SMS gateway solution if required in future.Email solution is a must
88				The proposed solution should support user/ip/mac binding functionality	As per our understanding the Proxy should support the traffic flow from source IP/MAC/user binding done using external AAA/LDAP/AD. The Proxy does not support binding of IP to MAC address or IP to username on the Proxy platform itself. This is a AAA functionality. All OEM's do not host any AAA functionality for performance reason but can support any AAA solution like MSAD/LDAP/Novell/Lotus/Oracle Core-id etc.	This is a feature not supported by all OEM's. Request NPCI exclude this point from RFP?	The proposed solution should able to group the users based on IP or user credentials.
89				The proposed solution should support scanning of SMTP, SMTPS, POP3, IMAP, FTP over HTTP protocols.		Can SMPT and SMTPS be excluded from this RFP point since it has to integrate with Blucoat Security Analytics Platform or the SI should propose with security analytics platform at additional cost over Secure web Gateway?	The proxy should support RPC over Https and HTTP.

90				The solution should have multiple Anti- Virus engines for scanning AV and other malwares on the Web traffic. Enabling AV should not degrade the performance of and Proxy solutions.	The solution should have AV engines which are different as compared to the end-point AV solution of the customer. AV engines should be branded amongst atleast top 5 in the industry and not any freewares	Should AV engines can be freeware or non branded or NPCI expects the SI to quote top 5 AV engine in the industry. Also Please suggest should the AV engine be of a different brand from the endpoint AV engine?	The AV engine should not be a freeware and only from all top AV engine available in industry. A different AV engine is expected which should not be same as existing endpoint AV engine.
91				The solution should ensure capabilities of caching to be quantified up to 25%	The solution should ensure capabilities of caching to be quantified up to 80% of the disk size and single object cache size should be at least 1GB	How NPCI will cache large Size objects / Videofile / Streaming content ?	We require caching for small objects files
92				The solution should provide decryption of unverified encrypted traffic for scanning and then re-encrypt it before sending (SSL decryption).	OK but need to mention the key size as minimum 2048 bits and up to 8172 bits with supported public key algorithms like RSA,DH	In this case what should be the minimum supported Key Size and the public key algorithm and cipher support?	2048 bits but need to check with the vendor if it will support with lower bit size
93	Annexure - H	45	6	The Bidder should provide reference of 2 clients in BFSI segment who have procured, installed including ongoing support for Appliance based Proxy configured in DC-DR Model during the last 3 years as on the date of submission of the bid.	Please confirm if the reference can be from an OEM solution which is not necessarily the proposed OEM. Also allow to provide 2 references from non-BFSI segment also.		Any reference of past implementation should be regarding the Bidder and not the OEM.
94	Section 9 - Technical Specifications	29	11	The Proxy solution should generate alerts to designated administrator and senior management via email, and SMS	As discussed the Proxy can support alerts via smtp, SNMP. For SMS support the solution needs to be integrated with third party SMS appliance gateway for IT alerts and notifications - A plug and play device that integrates easily with existing applications like email, database and application servers	Is NPCI expecting the System integrator to also quote for third party SMS appliance gateway for IT alerts and notifications or Do NPCI will integrate with their current SMS appliance?	Solution should have the capability to integrate with the third party SMS gateway solution if required in future. Email solution is a must.
95	Section 9 - Technical Specifications	12	12	Should have capability to integrate with SIEM tool, also should report alerts via sms.	Same as above -answer to point number 11.	Is NPCI expecting the System integrator to also quote for third party SMS appliance gateway for IT alerts and notifications or Do NPCI will integrate with their current SMS appliance?	Same as the response of clause no11.
96	Section 9 - Technical Specifications	30	17	The proposed solution should support user/ip/mac binding functionality	As per the understanding with customer the Proxy should support the traffic flow from source IP/MAC/user binding done using external AAA/LDAP/AD. The Proxy does not support binding of IP to MAC address or IP to username on the Proxy platform itself. This is a AAA functionality. And the BlueCoat proxy does not host any AAA functionality for performance reason but can support any AAA solution like MSAD/LDAP/Novell/Lotus/Oracle Core-id etc.	This is not a feature supported in Bluecoat secure web gateway. Can NPCI exclude this point from RFP?	The proposed solution should be able to group the users based on IP or user credentials.

97	Section 9 - Technical Specifications	30	21	The proposed solution should support scanning of SMTP, SMTPS, POP3, IMAP, FTP over HTTP protocols.	This is already clarified with customer that this requires integration with out of box solution like the BlueCoat SAP(Security Analytics Platform and Threat Blades)	Can SMPT and SMTPS be excluded from this RFP point since it has to integrate with Blucoat Security Analytics Platform or the SI should propose with security analytics platform at additional cost over Secure web Gateway?	The proxy should support RPC over Hhttps and HTTP.
98	Section 9 - Technical Specifications	30	26	The solution should have multiple Anti- Virus engines for scanning AV and other malwares on the Web traffic. Enabling AV should not degrade the performance of and Proxy solutions.	The solution should have AV engines which are different as compared to the end-point AV solution of the customer. AV engines should be branded amongst atleast top 5 in the industry and not any freewares	Should AV engines can be freeware or non branded or NPCI expects the SI to quote top 5 AV engine in the industry. Also Please suggest should the AV engine be of a different brand from the endpoint AV engine?	The AV engine should not be a freeware and only from all top AV engine available in industry. A different AV engine is expected which should not be same as existing endpoint AV engine(McAfee)
99	Section 9 - Technical Specifications	31	35	The solution should ensure capabilities of caching to be quantified up to 25%	The solution should ensure capabilities of caching to be quantified up to 80% of the disk size and single object cache size should be at least 1GB	How NPCI will cache large Size objects / Videofile / Streaming content ?	We require caching for small objects files
100	Section 9 - Technical Specifications	32	44	The solution should provide decryption of unverified encrypted traffic for scanning and then re-encrypt it before sending (SSL decryption).	OK but need to mention the key size as minimum 2048 bits and up to 8172 bits with supported public key algorithms like RSA,DH	In this case what should be the minimum supported Key Size and the public key algorithm and cipher support?	No change in RFP
101	Section 9 Technical Specifications - Table 9.1	29	1	The Secure Web Gateway Offering should be appliance based solution designed for secure proxy and active content caching services. The Appliance should have Minimum 6 to 10 Interfaces upgradable to GE SFP Ports	Request to amend this to the Appliance should have Minimum 6 Interfaces		Appliance should have Minimum 4 GE Interfaces for data/user traffic excluding a dedicated mangament interface.
102	Section 9 Technical Specifications - Table 9.1	29	2	The solution should track and block sharing of Internet access from different IP source. Prevention of concurrent login / sharing of internet access by using same credentials (user id & password) from multiple workstations. E.g. User1 logged in with User1admin; User2 should not be able to log in with User1admin	Kindly note this point is a feature of identity management solutions and your Active directory . However you have clarified that this meant that user based policies should be applicable irrespective of whichever machine the user log in from		The solution should identify request from two different sources with same credential. That means at any given point ,the use should be able to login from single IP.
103	Section 9 Technical Specifications - Table 9.1	29	6	The Solution should have the capability to decrypt the SSL traffic and subsequently feed decrypted traffic to one passive device (IDS, Security Analytics etc) for further analysis	Request to amend this point that the solution should provide feeds to SIEM solutions. Since your earlier requirement of providing feeds to IDS does not qualify in a proxy requirement		All the logs including SSL logs should be passed though SIEM for further analysis.

104	Section 9 Technical Specifications - Table 9.1	29	10	The solution should be able to discover and classify, protect data within all infrastructure of NPCI, in file shares, databases and collaboration tools like SharePoint	This is a pure DLP requirement and can be achieved if DLP license will be activated. However since you do not require DLP request this clause be removed		It's an optional feature .
105	Section 9 Technical Specifications - Table 9.1	29	11	The Proxy solution should generate alerts to designated administrator and senior manager via email and SMS	The Proxy solution should generate alerts to designated administrator via email only .Request to delete the SMS requirement		Solution should have the capability to integrate with the third party SMS gateway solution if required in future.Email solution is a must.
106	Section 9 Technical Specifications - Table 9.1	29	12	Should have Capability to integrate with SIEM Tool, also should alert via SMS	Should have Capability to integrate with SIEM Tool.Request to delete the SMS requirement		Same as the response of clause no11.
107	Section 9 Technical Specifications - Table 9.1	30	15	It should also have feature of Reverse Proxy and also support terminal Services / Citrix client	Request to remove the requirement for reverse proxy since yours is a pure forward proxy requirement and the purpose of a reverse proxy is primarily for WAF for which you are already using Imperva in your environment		Reverse proxy is a mandatory requirement.
108	Section 9 Technical Specifications - Table 9.1	30	17	The proposed solution should support user/ip/mac binding functionality	This is a SSL VPN functionality and has no prevalence in a Proxy scenario for the endpoints. You are requested to remove this point		The proposed solution should be able to group the users based on IP or user credentials.
109	Section 9 Technical Specifications - Table 9.1	30	18	The proposed solution should support session time out and idle time out facility to forcefully logout the users.	We have time based facility available		OK
110	Section 9 Technical Specifications - Table 9.1	30	21	The proposed solution should support scanning of SMTP, SMTPS, POP3, IMAP, FTP over HTTP protocols.	If the Mail is accessed from outlook it will use RPC over Https which is supported by proxy. If the mail is accessed from browser (like https://webmail.npci.com/) as application which would be purely HTTPS and would be supported by proxy. Other than this no proxy would be able to support SMTP/POP3/IMAP Protocols as they are part of Email channel and not Web Channel.		The proxy should support RPC over Https and HTTP.
111	Section 9 Technical Specifications - Table 9.1	30	23	The proposed solution should provide option to define different bandwidth and policy.	This option is a packet shaping option available with your firewall and multiple packet shaping tools .We request you to remove this point		Understanding is correct.
112	Section 9 Technical Specifications - Table 9.1	31	31	The Solution should provide file filtering for upload / download	Request to change this option to "The Solution should provide file filtering for download".		The solution should have the capacity to control the content of download and upload .
113	Section 9 Technical Specifications - Table 9.1	31	32	The solution should be integrated with existing DLP and APT solution.	FireEye can be placed ahead of Websense Proxy (between proxy and internet) in the bridge mode. Having Said that with the help of websense proxy 95% of APTs can be taken care of.		Vendor should ensure after placing their solution there should not be any compatibility issue in the existing APT & DLP solution.
114	Section 9 Technical Specifications - Table 9.1	31	33	The Bidder should ensure that the appliance based solution is sized accordingly for 70% SSL Traffic	Kindly confirm if NPCI's existing usage of SSL sites are 70%. Websense being the most commonly used proxy we have seen the SSL site access of any organization has not been more than 40 to 50%		Considering the future requirements this percentage is expected anything more than 40 %

115	Section 9 Technical Specifications - Table 9.1	31	37	The solution should monitor and block instant messaging (IM) based file transfer	This is a pure DLP requirement and can be achieved if DLP license will be activated. However since you do not require DLP this Request for this clause to be removed		The solution should have atleast a feature to block and allow Peer to Peer or any IM /chat .
116	Section 9 Technical Specifications - Table 9.1	31	40	The solution should ensure reverse proxy functionality with web acceleration feature including security and anonymity	Request to remove the requirement for reverse proxy since yours is a pure forward proxy requirement and the purpose of a reverse proxy is primarily for WAF for which you are already using Imperva in your environment .The web acceleration feature is available in load balancers like Radware/F5 which provide reverse proxy/web acceleration solutions.		Same as clause no 15
117	Section 9 Technical Specifications - Table 9.1	32	43	The Available bandwidth is 45 Mbps that is expected to be scaled to 150Mbps at each location.	Is 45Mbps bandwidth used only for Web Traffic alone or is it used for all the traffic like SMTP, Application hosting, etc... Usually we have seen 50 to 60% of the total bandwidth is consumed by Web Traffic and rest for SMTP and application hosting. Websense appliances are sized based on the Web Traffic Bandwidth, and considering each page would at an average would be 10KB, for 100Mbps there could be around 1280 Web Transactions per second.		45 Mbps bandwidth is used by web and other applications .Out of which Web traffic 50 %.
118	Section 9 Technical Specifications - Table 9.1	32	45	The appliance should have Capability to restrict internet usage for end-users with ability to set limits in terms of daily/Weekly/Monthly download limits	This option is a packet shaping option available with your firewall and multiple packet shaping tools .We request you to remove this point		No Change in RFP
119	Section 9 Technical Specifications - Table 9.1	32	49	The solution would be able to generate, export reports in below mentioned formats i.e. PDF, Word, Excel, Html, Also it should be able to alert via SMS	Kindly amend the statement to The solution would be able to generate, export reports in below mentioned formats i.e. PDF, Excel, HTML .Request to delete the SMS statement		The solution should be able to generate, export reports in below mentioned formats i.e. PDF, Word, excel, html.
120	Section 9 Technical Specifications - Table 9.1	32	51	Policies based on Geo locations as destination.	This is a NGFW feature not available in proxies. Request you to remove this point		Irrespective of any locations user polices should be enforced .
121	Section 9 Technical Specifications - Table 9.1	32	54	Allocation of Volume Quota: Assign download/upload, internet browsing quota limit to user / users / group /groups /client/clients etc.	This option is a packet shaping option available with your firewall and multiple packet shaping tools . We request you to remove this point		No change in RFP
122	Section 9 Technical Specifications - Table 9.1	32	55	On reaching the quota limit the internet access should be blocked automatically with notification to users.	This option is a packet shaping option available with your firewall and multiple packet shaping tools .We request you to remove this point		No change in RFP
123	Section 9 Technical Specifications - Table 9.1	33	59	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.	Please mention in addition the mentioned statement Remote Filtering option has to be made with a on premise solution only. Cloud based filtering solutions should not be accepted		No of roaming users is around 200 at present but future scalability should be taken care.On premises solution is expected.
124	Section 9 Technical Specifications - Table 9.1	33	63	The solution should must detect and protect against anonymizing websites, anonymizing tools	Request to amend the statement to The solution should must detect and protect against anonymizing websites which are being accessed through the proxy		Understanding is correct it should detect and protect the website access through proxy