बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
1	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS **OR** Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -**1**- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector / **Any Enterprise** in India, at each Data Center / Disaster Recovery Center, during last -**10**- Years And b) with a contract value of minimum Rs. **1** Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	Pls refer addendum
2	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS **OR** Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -**1**- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector / **Any Enterprise** in India, at each Data Center / Disaster Recovery Center, during last -**10**- Years And b) with a contract value of minimum Rs. **1** Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	Pls refer addendum
3	2	12	Warranty including Annual Maintenance Contract (AMC)		Inspira requesting bank to clarify about existing helpdesk tool. Let us know the Work Flow	Details will be provided to successful bidder.
4	12	Payment Terms (Point 9)	General	Installation & Implementation Charges will be released after one month of successful installation and satisfactory functioning on submission of invoice & signoff report from Bank Authority.	Bidder request to release an interim payment of 50% within 4 weeks of installtion and the balance on completion of installation	No change
5	137	12. Warranty including Annual Maintenance Contract (AMC)	Annexure 12 – Project Details Scope of Work	In event of any equipment / part is replaced or any defect in respect of any equipment / part is corrected for more than one instance of any quarter during the base warranty period of 3 years, where the period of warranty remained is less than twelve month of the comprehensive warranty, the warranty in respect of the entire network hardware equipment for which the equipment / part is replaced / defect is corrected, will be extended for an additional period of twelve months from the date of such replacement/ correction of defects.	Request you ro kindly consider to remove this clause.	No change

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
6	54	9 / 4. NIPS Type C	Technical Specifications	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE . Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	The requirement is for 10 Gbps throughput and there are many ports asked in the RFP. So request to remove "additional I/O card slot to add 24X1/10 GE RJ45" or consider stacking of the appliances as an option.	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver
7	17	B.12, B.7	System Hardware and Interface Requirement	The proposed NIPS hardware/appliance/solution should support Link aggregation functionality (LACP((IEEE 802.3ad))/PAGP) to group multiple ports as single Channel to achieve higher bandwidth	Request to change the language as LACP is configured on upstream and downstream devices. **Kindly rephrase as - The proposed NIPS hardware/appliance/solution should support Link aggregation functionality (LACP((IEEE 802.3ad))/PAGP) or it should support port clustering to group multiple ports as single Channel.**	The proposed NIPS hardware/ appliance/solution should support Link aggregation functionality (LACP((IEEE 802.3ad))/PAGP) or it should support port clustering to group multiple ports as single Channel.
8	54	Type C: B.9	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE RJ45. Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	The number of ports asked for are beyond the performance capacity for the asked 10 G NIPS appliance. It is not recommended to have so many monitoring/prevention segments running on a 10 G appliance. Unlike firewalls, NIPS sensors need to perform a lot of signature as well as signature analysis on complete Network traffic along with heuristics, learning, etc. **Request to rephrase the clause as - Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4X10/25 GE Fiber, 8 x 10 GE RJ45. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities.**	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1 GE . The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities
9	17	B.12, B.7	System Hardware and Interface Requirement	The proposed NIPS hardware/appliance/solution should support Link aggregation functionality (LACP((IEEE 802.3ad))/PAGP) to group multiple ports as single Channel to achieve higher bandwidth	Request to change the language as LACP is configured on upstream and downstream devices. **Kindly rephrase as - The proposed NIPS hardware/appliance/solution should support Link aggregation functionality (LACP((IEEE 802.3ad))/PAGP) or it should support port clustering to group multiple ports as single Channel.**	The proposed NIPS hardware/appliance/solution should support Link aggregation functionality (LACP((IEEE 802.3ad))/PAGP) or it should support port clustering to group multiple ports as single Channel.
10	54	9 / 4. NIPS Type C	Technical Specifications	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE . Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	The requirement is for 10 Gbps throughput and there are many ports asked in the RFP. So request to remove "additional I/O card slot to add 24X1/10 GE RJ45" or consider stacking of the appliances as an option.	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
11	18	C.4	Performance Requirement	The proposed NIPS hardware/appliance/solution should support minimum 40 million concurrent connections	NIPS appliances are stateful protection devices that have hardware purpose built to provide optimum throughput. For a 60G appliance, as per best practice and optimum performance needs, it is not recommended to have more than 30 million concurrent connections. **Kindly rephrase as - The proposed NIPS hardware/appliance/solution should support minimum 30 million concurrent connections**	No change
12	54	9 / 4. NIPS Type C	Technical Specifications	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE . Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	The requirement is for 10 Gbps throughput and there are many ports asked in the RFP. So request to remove "additional I/O card slot to add 24X1/10 GE RJ45" or consider stacking of the appliances as an option.	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver
13	54	9 / 4. NIPS Type C	Technical Specifications	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE . Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	The requirement is for 10 Gbps throughput and there are many ports asked in the RFP. So request to remove "additional I/O card slot to add 24X1/10 GE RJ45" or consider stacking of the appliances as an option.	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver
14	54	9 / 4. NIPS Type C	Technical Specifications	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE . Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	The requirement is for 10 Gbps throughput and there are many ports asked in the RFP. So request to remove "additional I/O card slot to add 24X1/10 GE RJ45" or consider stacking of the appliances as an option.	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver
15	54	Type C: B.9	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE RJ45. Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	The number of ports asked for are beyond the performance capacity for the asked 10 G NIPS appliance. It is not recommended to have so many monitoring/prevention segments running on a 10 G appliance. Unlike firewalls, NIPS sensors need to perform a lot of signature as well as signature analysis on complete Network traffic along with heuristics, learning, etc. **Request to rephrase the clause as - Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4X10/25 GE Fiber, 8 x 10 GE RJ45. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities.**	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
16	18	C.4	Performance Requirement	The proposed NIPS hardware/appliance/solution should support minimum 40 million concurrent connections	NIPS appliances are stateful protection devices that have hardware purpose built to provide optimum throughput. For a 60G appliance, as per best practice and optimum performance needs, it is not recommended to have more than 30 million concurrent connections. **Kindly rephrase as - The proposed NIPS hardware/appliance/solution should support minimum 30 million concurrent connections**	No change
17	54	9 / 4. NIPS Type C	Technical Specifications	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE . Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	The requirement is for 10 Gbps throughput and there are many ports asked in the RFP. So request to remove "additional I/O card slot to add 24X1/10 GE RJ45" or consider stacking of the appliances as an option.	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver
18	54	9 / 4. NIPS Type C	Technical Specifications	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE . Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	The requirement is for 10 Gbps throughput and there are many ports asked in the RFP. So request to remove "additional I/O card slot to add 24X1/10 GE RJ45" or consider stacking of the appliances as an option.	9. Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver
19	19	7/ 2. NIPS Type A	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
20	19	9./ 2. NIPS Type A	Technical Specifications	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)	Network processing like "NAT & QOS are typically firewall functionality, hence requesting you to change the clause as "The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action	9. The proposed firewall solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed firewall irrespective of Firewall load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the firewall and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)
21	19	C.8	Performance Requirement	The proposed Firewall hardware/solution should supports minimum 50,000 -defined signatures with Regular Expressions	Please remove this as this looks like a firewall requirement. NIPS sensors do not support more than 20,000 signatures.	The proposed Firewall hardware/solution should support all existing signatures by default and all future signature released from time to time with Regular Expressions

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
22	19	D.2	Feature Requirement	The proposed NIPS hardware/appliance/solution should be providing flow information details (Netflow,Jflow, Sflow or similar) for a specific host for given time interval	Kindly remove this requirement as this is an NBAD/NDR requirement that requires different set of technologies.	~~The proposed NIPS hardware/appliance/solution should be providing flow information details (Netflow,Jflow, Sflow or similar) for a specific host for given time interval~~
23	19	7/ 2. NIPS Type A	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
24	19	9./ 2. NIPS Type A	Technical Specifications	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)	Network processing like "NAT & QOS are typically firewall functionality, hence requesting you to change the clause as "The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)"	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load /Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)
25	19	7/ 2. NIPS Type A	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
26	19	9./ 2. NIPS Type A	Technical Specifications	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)	Network processing like "NAT & QOS are typically firewall functionality, hence requesting you to change the clause as "The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action	9. The proposed firewall solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed firewall irrespective of Firewall load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the firewall and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
27	19	7/ 2. NIPS Type A	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
28	19	9./ 2. NIPS Type A	Technical Specifications	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)	Network processing like "NAT & QOS are typically firewall functionality, hence requesting you to change the clause as "The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)"	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load /Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)
29	19	7/ 2. NIPS Type A	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
30	19	9./ 2. NIPS Type A	Technical Specifications	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)	Network processing like "NAT & QOS are typically firewall functionality, hence requesting you to change the clause as "The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action	9.The proposed firewall solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed firewall irrespective of Firewall load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the firewall and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)
31	19	C.8	Performance Requirement	The proposed Firewall hardware/solution should supports minimum 50,000 -defined signatures with Regular Expressions	Please remove this as this looks like a firewall requirement. NIPS sensors do not support more than 20,000 signatures.	The proposed Firewall hardware/solution should support all existing signatures by default and all future signature released from time to time with Regular Expressions

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
32	19	D.2	Feature Requirement	The proposed NIPS hardware/appliance/solution should be providing flow information details (Netflow,Jflow, Sflow or similar) for a specific host for given time interval	Kindly remove this requirement as this is an NBAD/NDR requirement that requires different set of technologies.	~~The proposed NIPS hardware/appliance/solution should be providing flow information details (Netflow,Jflow, Sflow or similar) for a specific host for given time interval~~
33	19	7/ 2. NIPS Type A	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
34	19	9./ 2. NIPS Type A	Technical Specifications	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)	Network processing like "NAT & QOS are typically firewall functionality, hence requesting you to change the clause as "The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)"	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load /Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)
35	19	9./ 2. NIPS Type A	Technical Specifications	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)	Network processing like "NAT & QOS are typically firewall functionality, hence requesting you to change the clause as "The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action	9. The proposed firewall solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed firewall irrespective of Firewall load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the firewall and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
36	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	Kindly consider Firewall/NIPS reference . Also Request you to please remove the 30 Racks clause as getting Documentary Proof of order / contract copy / customer credentials is not possible of mentioning 30 Racks due to confidentailiaty of the Project. The bidder should have successfully delivered & installed minimum -02- numbers of firewall /NIPS of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, during last -6- Years (as on RFP date)	Pls refer addendum
37	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	Kindly consider Firewall/NIPS reference . Also Request you to please remove the 30 Racks clause as getting Documentary Proof of order / contract copy / customer credentials is not possible of mentioning 30 Racks due to confidentailiaty of the Project. The bidder should have successfully delivered & installed minimum -02- numbers of firewall /NIPS of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, during last -6- Years (as on RFP date)	Pls refer addendum
38	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	Kindly consider Firewall/NIPS reference . Also Request you to please remove the 30 Racks clause as getting Documentary Proof of order / contract copy / customer credentials is not possible of mentioning 30 Racks due to confidentailiaty of the Project. The bidder should have successfully delivered & installed minimum -02- numbers of firewall /NIPS of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, during last -6- Years (as on RFP date)	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
39	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	Kindly consider Firewall/NIPS reference . Also Request you to please remove the 30 Racks clause as getting Documentary Proof of order / contract copy / customer credentials is not possible of mentioning 30 Racks due to confidentailiaty of the Project. The bidder should have successfully delivered & installed minimum -02- numbers of firewall /NIPS of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, during last -6- Years (as on RFP date)	Pls refer addendum
40	11	Payment Terms (Point 9)	General	Payment Terms : For the 70% Payment a PBG of 5% needs to be submitted. Also There is a 10% PBG to besubmitted to get the Final 10% Payment.	We request to remove the 5% PBG Clause for the 70% Payment (As 10% PBG willanyways be submitted at the time of Final 10% Payment)	No change
41	12	Payment Terms (Point 9)	General	Annual Maintenance Contract (AMC) cost (Year -4 to Year -7)	We request to make the AMC Payment at the start of the Quarter (Instead of Arrears asmentioned in the RFP)	No change
42	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	Request to pl. Amend this Clause to Bidder /OEM	Pls refer addendum
43	30	C Others (Point 3)	Eligibility Criteria	Bidder must have the following Accreditations / Certifications: A) ISO 9001 The manufacturing facility of the products quoted under this RFP should have the following Accreditations / Certifications A) ISO 9001 B) ISO14001	We have ISO 9001 & 27001 Certification.Hope this is acceptable by the Bank	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
44	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	Kindly consider Firewall/NIPS reference . Also Request you to please remove the 30 Racks clause as getting Documentary Proof of order / contract copy / customer credentials is not possible of mentioning 30 Racks due to confidentailiaty of the Project. The bidder should have successfully delivered & installed minimum -02- numbers of firewall /NIPS of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, during last -6- Years (as on RFP date)	Pls refer addendum
45	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	Kindly consider Firewall/NIPS reference . Also Request you to please remove the 30 Racks clause as getting Documentary Proof of order / contract copy / customer credentials is not possible of mentioning 30 Racks due to confidentailiaty of the Project. The bidder should have successfully delivered & installed minimum -02- numbers of firewall /NIPS of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, during last -6- Years (as on RFP date)	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
46	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	The bidder should have successfully delivered & installed minimum -02- numbers of ~~each type of~~ firewall and -02- nos. of ~~each type of theequipment i.e~~ NIPS ~~and Router~~ of the ~~proposed~~ similar OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers /Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, ~~having at least 30 Racks at each Data Center / Disaster Recovery Center~~, duringlast -6- Years (as on RFP date).Request you to please remove the 30 Racks clause as getting Documentary Proof of order / contract copy / customer credentials is not possible of mentioning 30 Racks due to confidentailiaty of the Project. And b) with a contract value of minimum Rs. 5 Crore on eachorganization for firewall reference andcontract value of minimum Rs. 2 Crore on each organization for NIPS reference .The contract value shall comprise of similar work,as specified in thescope of work to be covered as part of this RFP.	Pls refer addendum
47	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	Request Bank to modify the clause basis the below suggestion as it would restrict the number of bidders that would be able to participate for this bid and remove router word **The bidder should have successfully delivered & installed minimum -02- numbers of proposed OEM any firewall/any other OEM firewall and -02- nos. of the equipment i.e any NIPS of proposed OEM /any other OEM NIPS a) at minimum -1- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be onsidered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions during last -6- Years (as on RFP date) b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.**	Pls refer addendum
48	32	D Experience & Support Infrastructure (Point 3)	Eligibility Criteria	The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	Request Bank to modify the clause basis the below suggestion as it would restrict the number of bidders that would be able to participate for this bid and remove router word **"The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS of the same OEM/any other OEM for this RFP) of Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in either 1 large bank with turnover of above Rs. 1 lakh crore or Financial Institutions or Government Organizations or Public Sector Undertakings (PSUs) having network of minimum 500**	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
49	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	Request Bank to modify the clause basis the below suggestion as it would restrict the number of bidders that would be able to participate for this bid and remove router word **"The bidder should have successfully delivered & installed minimum -02- numbers of proposed OEM any firewall/any other OEM firewall and -02- nos. of the equipment i.e any NIPS of proposed OEM /any other OEM NIPS a) at minimum -1- Data Centres / Disaster Recovery Centres (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions during last -6- Years (as on RFP date) b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.** **Explanation :-** This modification is required to ensure the Bank correctly qualifies the best along with maxumum participation from Bidders & checks his credentilas in terms	Pls refer addendum
50	32	D Experience & Support Infrastructure (Point 3)	Eligibility Criteria	The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	Request Bank to modify the clause basis the below suggestion as it would restrict the number of bidders that would be able to participate for this bid **"The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS of the same OEM/any other OEM for this RFP) of Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in either 1 large bank with turnover of above Rs. 2 lakh crore or Financial Institutions or Government Organizations or Public Sector Undertakings (PSUs) having network of minimum 500 domestic branches** **Explanation :-**This modification is required to ensure the Bank correctly qualifies the best along with maxumum participation from Bidders & checks his credentilas in terms of Deployment & installation capabilities	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
51	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	Kindly consider Firewall/NIPS reference . Also Request you to please remove the 30 Racks clause as getting Documentary Proof of order / contract copy / customer credentials is not possible of mentioning 30 Racks due to confidentiality of the Project. The bidder should have successfully delivered & installed minimum -02- numbers of firewall /NIPS of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, during last -6- Years (as on RFP date)	Pls refer addendum
52	32	J.1	Certification	Security effectiveness of the proposed Firewall hardware/solution should be recommended/certified by NSS / Forrester NGFW last published test report	Looks like Firewall certifications are wrongly mentioned under NIPS certifications. Request to change the requirement as per IPS	~~Security effectiveness of the proposed Firewall hardware/solution should be recommended/certified by NSS / Forrester NGFW last published test report~~
53	32	J.1	Certification	Security effectiveness of the proposed Firewall hardware/solution should be recommended/certified by NSS / Forrester NGFW last published test report	Looks like Firewall certifications are wrongly mentioned under NIPS certifications. Request to change the requirement as per IPS	~~Security effectiveness of the proposed Firewall hardware/solution should be recommended/certified by NSS / Forrester NGFW last published test report~~
54	33		Technical Specifications	Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack.	Request change it to "Note : If Bidder is proposing a cluster/stack based solution, the performance requirement applies to a single appliance of the cluster/stack".	As per RFP
55	33		Technical Specifications	Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack.	Request change it to "Note : If Bidder is proposing a cluster/stack based solution, the performance requirement applies to a single appliance of the cluster/stack".	As per RFP
56	33		Technical Specifications	Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack.	Request change it to "Note : If Bidder is proposing a cluster/stack based solution, the performance requirement applies to a single appliance of the cluster/stack".	As per RFP
57	33		Technical Specifications	Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack.	Request change it to "Note : If Bidder is proposing a cluster/stack based solution, the performance requirement applies to a single appliance of the cluster/stack".	As per RFP
58	33		Technical Specifications	Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack.	Request change it to "Note : If Bidder is proposing a cluster/stack based solution, the performance requirement applies to a single appliance of the cluster/stack".	As per RFP
59	137	12. Warranty including Annual Maintenance Contract (AMC)	Annexure 12 – Project Details Scope of Work	In event of any equipment / part is replaced or any defect in respect of any equipment / part is corrected for more than one instance of any quarter during the base warranty period of 3 years, where the period of warranty remained is less than twelve month of the comprehensive warranty, the warranty in respect of the entire network hardware equipment for which the equipment / part is replaced / defect is corrected, will be extended for an additional period of twelve months from the date of such replacement/ correction of defects.	Request you ro kindly consider to remove this clause.	No change
60	33		Technical Specifications	Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack.	Request change it to "Note : If Bidder is proposing a cluster/stack based solution, the performance requirement applies to a single appliance of the cluster/stack".	As per RFP

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
61	33		Technical Specifications	Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack.	Request change it to "Note : If Bidder is proposing a cluster/stack based solution, the performance requirement applies to a single appliance of the cluster/stack".	As per RFP
62	94	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10/25 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	The number of ports askd for are beyond the performance capacity for the asked 30 G NIPS appliance. It is not recommended to have so many monitoring/prevention segments running on a 30 G appliance. Unlike firewalls, NIPS sensors need to perform a lot of signature as well as signature analysis on complete Network traffic along with heuristics, learning, etc. **Request to rephrase the clause as - Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 2x40/100 GE Fiber, 8x10 GE Fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities.**	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,8 nos-10G. BIDI multimode transceiver.
63	35	Type B: B.9	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10/25 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	The number of ports askd for are beyond the performance capacity for the asked 30 G NIPS appliance. It is not recommended to have so many monitoring/prevention segments running on a 30 G appliance. Unlike firewalls, NIPS sensors need to perform a lot of signature as well as signature analysis on complete Network traffic along with heuristics, learning, etc. **Request to rephrase the clause as - Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 2x40/100 GE Fiber, 8x10 GE Fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities.**	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,8 nos-10G. BIDI multimode transceiver.
64	37	7 / 3. NIPS Type B	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
65	37	9 / 3. NIPS Type B	Technical Specifications	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)	Network processing like "NAT & QOS are typically firewall functionality, hence requesting you to change the clause as "The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action	9. The proposed firewall solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed firewall irrespective of Firewall load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the firewall and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)
66	37	7 / 3. NIPS Type B	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
67	37	9 / 3. NIPS Type B	Technical Specifications	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)	Network processing like "NAT & QOS are typically firewall functionality, hence requesting you to change the clause as "The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action	9. The proposed firewall solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed firewall irrespective of Firewall load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the firewall and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)
68	37	7 / 3. NIPS Type B	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
69	37	9 / 3. NIPS Type B	Technical Specifications	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)	Network processing like "NAT & QOS are typically firewall functionality, hence requesting you to change the clause as "The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action	9. The proposed firewall solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed firewall irrespective of Firewall load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the firewall and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)
70	37	7 / 3. NIPS Type B	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
71	37	9 / 3. NIPS Type B	Technical Specifications	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)	Network processing like "NAT & QOS are typically firewall functionality, hence requesting you to change the clause as "The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action	9. The proposed firewall solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed firewall irrespective of Firewall load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the firewall and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)
72	37	7 / 3. NIPS Type B	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
73	37	9 / 3. NIPS Type B	Technical Specifications	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)	Network processing like "NAT & QOS are typically firewall functionality, hence requesting you to change the clause as "The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action	9. The proposed firewall solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed firewall irrespective of Firewall load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the firewall and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)
74	37	7 / 3. NIPS Type B	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
75	37	9 / 3. NIPS Type B	Technical Specifications	9. The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)	Network processing like "NAT & QOS are typically firewall functionality, hence requesting you to change the clause as "The proposed NIPS solution architecture should have Control Plane separated from the Data Plane in the NIPS appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed NIPS irrespective of NIPS load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the NIPS and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action	9. The proposed firewall solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup etc). Control plane must have dedicated resources such as CPU, RAM etc. (This is to ensure administrator always has management access to proposed firewall irrespective of Firewall load / Traffic Spike / Cyber Attack and Performance tracking which drives higher CPU utilization. Bank should be able to login to the firewall and carry out reporting / management / packet capture etc., to identify the root cause and accordingly take necessary action to remediate it.)
76	38	10 / 3. NIPS Type B	Technical Specifications	The proposed NIPS hardware/solution should have capability to define time based rules/policy	This time based policy typically firewall functionality, hence requesting you to remove the clause	~~10. The proposed NIPS hardware/solution should have capability to define time based rules/policy.~~
77	38	10 / 3. NIPS Type B	Technical Specifications	The proposed NIPS hardware/solution should have capability to define time based rules/policy.	This time based policy typically firewall functionality, hence requesting you to remove the clause	~~10. The proposed NIPS hardware/solution should have capability to define time based rules/policy.~~
78	38	10 / 3. NIPS Type B	Technical Specifications	10. The proposed NIPS hardware/solution should have capability to define time based rules/policy.	This time based policy typically firewall functionality, hence requesting you to remove the clause	~~10. The proposed NIPS hardware/solution should have capability to define time based rules/policy.~~
79	38	10 / 3. NIPS Type B	Technical Specifications	10. The proposed NIPS hardware/solution should have capability to define time based rules/policy.	This time based policy typically firewall functionality, hence requesting you to remove the clause	~~10. The proposed NIPS hardware/solution should have capability to define time based rules/policy.~~
80	38	10 / 3. NIPS Type B	Technical Specifications	10. The proposed NIPS hardware/solution should have capability to define time based rules/policy.	This time based policy typically firewall functionality, hence requesting you to remove the clause	~~10. The proposed NIPS hardware/solution should have capability to define time based rules/policy.~~
81	38	10 / 3. NIPS Type B	Technical Specifications	10. The proposed NIPS hardware/solution should have capability to define time based rules/policy.	This time based policy typically firewall functionality, hence requesting you to remove the clause	~~10. The proposed NIPS hardware/solution should have capability to define time based rules/policy.~~

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
82	38	10 / 3. NIPS Type B	Technical Specifications	10. The proposed NIPS hardware/solution should have capability to define time based rules/policy.	This time based policy typically firewall functionality, hence requesting you to remove the clause	~~10. The proposed NIPS hardware/solution should have capability to define time based rules/policy.~~
83	51	Annexure 12 Section A Point 7	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
84	51	Annexure 12 Section A Point 8	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
85	51	Annexure 12 Section A Point 9	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
86	51	Annexure 12 Section A Point 7	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
87	51	Annexure 12 Section A Point 8	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
88	51	Annexure 12 Section A Point 9	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
89	51	Annexure 12 Section A Point 7	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
90	51	Annexure 12 Section A Point 8	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
91	51	Annexure 12 Section A Point 9	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
92	51	Annexure 12 Section A Point 7	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
93	51	Annexure 12 Section A Point 8	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
94	51	Annexure 12 Section A Point 9	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
95	51	Annexure 12 Section A Point 7	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
96	51	Annexure 12 Section A Point 8	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
97	51	Annexure 12 Section A Point 9	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
98	141	22. Right to Alter Quantities	Annexure 12 – Project Details Scope of Work	The Bank reserves the right to alter the requirements specified in the Tender. The Bank also reserves the right to delete one or more items from the list of items specified in the Tender. The Bank will inform all Bidders about changes, if any. The Bidder agrees that the Bank has no limit on the additions or deletions on the items for the period of the contract. Further the Bidder agrees that the prices quoted by the Bidder would be proportionately adjusted with such additions or deletions in quantities/items.	The prices are dependant on Taxes, Duties (including Custom Duty), Levies, USD-INR Exchnage Rate, OEM List Prices, OEM Discounting etc. These factors are not within bidder's control and hence the bidder requests the bank to allow for price revision for additional order after the first PO. The bidder can commit to price quoted in the commercial bid for the first purchase order within bid validity period. Any additional quantity if ordered in first PO then bidder will be able to honour the prices.	No change

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
99	51	Annexure 12 Section A Point 7	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
100	51	Annexure 12 Section A Point 8	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
101	51	Annexure 12 Section A Point 9	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
102	149	section i	Annexure 15 – Commercial Bid	I. In the case of additional requirements desired by the Bank, the Bank can place the order for additional 25-30% of the over and above the quantity for which Order is placed with a selected bidder.	The prices are dependant on Taxes, Duties (including Custom Duty), Levies, USD-INR Exchnage Rate, OEM List Prices, OEM Discounting etc. These factors are not within bidder's control and hence the bidder requests to consider first year to place any order for additonal quantity over and above the quantity for which order is placed with a selected bidder The bidder can commit to price quoted in the commercial bid for the first purchase order within bid validity period. Any additional quantity if ordered in first PO then bidder will be able to honour the prices	No change
103	11	Payment Terms (Point 9)	General	The Vendor must accept the payment terms proposed by the Bank. The commercial bid submitted by the Vendor must be in conformity with the payment terms proposed by the Bank. Any deviation from the proposed payment terms would not be accepted. The Bank shall have the right to withhold or deduct (in event of SLA breach) any payment due to the selected Vendor, in case of delays or defaults on the part of the selected Vendor. Such withholding of payment shall not amount to a default on the part of the Bank. If any of the items / activities as mentioned in the price bid is not taken up by the Bank during the course of the assignment, the Bank will not pay the professional fees quoted by the vendor in the price bid against such activity / item	The Vendor must accept the payment terms proposed by the Bank. The commercial bid submitted by the Vendor must be in conformity with the payment terms proposed by the Bank. Any deviation from the proposed payment terms would not be accepted. The Bank be provided with appropriate SLA credit notes, which would be adjusted from the further billing cycles. If any of the items / activities as mentioned in the price bid is not taken up by the Bank during the course of the assignment, the Bank will not pay the professional fees quoted by the vendor in the price bid against such activity / item We submit that, since a bill once generated on the system cannot be rolled back. In case of a SLA breach a credit note corresponding to the SLA credits applicable to that particular breach will be provider. This would be duly adjusted from the next billing cycle	No change

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
104	169	Indemnity (Point 18)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	The Service Provider shall indemnify the Bank, and shall always keep indemnified and hold the Bank, its employees, personnel, officers, directors, (hereinafter collectively referred to as "Personnel") harmless from and against any and all losses, liabilities, claims, actions, costs and expenses (including attorneys' fees) relating to, resulting directly or indirectly from or in any way arising out of any claim, suit or proceeding brought against the Bank as a result of: • Bank's authorized / bona fide use of the Deliverables and /or the Services provided by selected Service Provider under this Agreement; and/or • an act or omission of the Service Provider and/or its employees, agents, sub-contractors in performance of the obligations under this Agreement; and/or • claims made by employees or subcontractors or subcontractors' employees, who are deployed by the Service Provider, against the Bank; and/or • claims arising out of employment, non-payment of remuneration and non-provision of statutory benefits by the Service Provider to its employees, its agents, contractors and sub-contractors • breach of any of the term of this Agreement or breach of any representation or false representation or inaccurate statement or assurance or covenant or warranty of the Service Provider under this Agreement; and/or • any or all Deliverables or Services infringing any patent, trademarks, copyrights or such other Intellectual Property Rights;	Indemnity should be for direct claims only. Indirect indemnity is far fetched. Although Bank may use the the services in an authorized/ Bonafide way, claims may arise which are not due to any fault of the Vendor. Hence an generic indemnity for claims arising out of bonafide use of Services is not acceptable. We cannot provide Indemnity for Claims an act or omission of the Service Provider and/or its employees, agents, sub-contractors in performance of the obligations under this Agreement; and/or. The act or omission can be in compliance with the Agreement but the outcome may still result in a loss for the Bank. For breach of any representation or false representation or inaccurate statement or assurance or covenant or warranty of the Service Provider under this Agreement, the settled principle in India in that a Termination right accrues in case of this and not an Indemnity , hence request bank to consider below • ~~Bank's authorized / bona fide use of the Deliverables and /or the Services provided by selected Service Provider under this Agreement; and/or~~ • an act or omission of the Service Provider and/or its employees, agents, sub-contractors in performance of the obligations under this Agreement which results in a breach of the Agreement; and/or	No change
105	174	Limitation of Liability (Point 25)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	Under no circumstances BOB shall be liable to the Service Provider for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of this Agreement, even if BOB has been advised of the possibility of such damages, such as, but not limited to, loss of revenue or anticipated profits or lost business.	We propose some modifications to this clause	No change
106	172	Termination (Point 21)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	Termination Rights (Bank):- Notwithstanding above, in case of change of policy or any unavoidable circumstances or without any reason Bank reserve the right to terminate this assignment or any subsequent agreement and / or any particular order, in whole or in part by giving Service Provider at least 60 days prior notice in writing	This is very open ended, propose deletion of this sub clause.	No change

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
107	174	Audit (Point 24)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	All Service Provider records with respect to any matters covered by this Agreement shall be made available to auditors and or inspecting officials of the Bank and/or Reserve Bank of India and/or any regulatory authority, at any time during normal business hours, as often as the Bank deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data. Said records are subject to examination. Bank's auditors would execute confidentiality agreement with the Service Provider provided that the auditors would be permitted to submit their findings to the Bank, which would be used by the Bank. The cost of the audit will be borne by the Bank. The scope of such audit would be limited to Service Levels being covered under the contract, and financial information would be excluded from such inspection, which will be subject to the requirements of statutory and regulatory authorities. The Bank and its authorized representatives, including Reserve Bank of India (RBI) or any other regulator shall have the right to visit any of the Service Provider's premises without prior notice to ensure that data provided by the Bank is not misused. The Service Provider shall cooperate with the authorized representative/s of the Bank and shall provide all information/ documents required by the Bank	Please confirm that the Service Provider shall furnish the required details strictly in relation to the services under the concerned engagement with the Bank, and that the Service Provider shall not disclose any commercial confidential information such as profit margins, cost breakups, Internal Management/ Board Meeting papers, etc.	No change
108	166	Set-off (Point 15)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	Without prejudice to other rights and remedies available to Bank, Bank shall be entitled to set-off or adjust any amounts due to Bank under this clause from the Service Provider against payments due and payable by Bank to the Service Provider for the services rendered. The provisions of this Clause shall survive the termination of this Agreement.	Bank can set-off/adjust invoices only against applicable LD/penalty clause	No change
109	169	Confidentiality (Point 17)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	The confidentiality obligations shall survive the expiry or termination of the Agreement between the Service Provider and the Bank	There should be a definite period until which the confidentiality obligations survive after termination of the Contract. We propose 5 years.	No change
110	51	Annexure 12 Section A Point 7	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
111	51	Annexure 12 Section A Point 8	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
112	51	Annexure 12 Section A Point 9	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
113	51	Annexure 12, A, pt 5	Migrated to the proposed Firewall appliance/solutions post optimization	Please share the existing appliance details from which we need to migrate from.		Details will be shared later with L1 bidder

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
114	51	Annexure 12, A, pt 6	In the proposed Firewall appliance/solutions if any changes done in existing Policy, Rules, Object and Object Group etc. all audit logs should be available with user id, date/time and Remarks/comments or any other field which should show audit trail change.	The audit log should be maintained by customer's PIM solution. Bidder will integrate the new appliance with customer's PIM solution.		No change
115	51	Annexure 12 Section A Point 7	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
116	51	Annexure 12 Section A Point 8	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
117	51	Annexure 12 Section A Point 9	Firewall: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
118	53	Annexure 12 Section B Point 7	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
119	53	Annexure 12 Section B Point 8	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
120	53	Annexure 12 Section B Point 9	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
121	53	Annexure 12 Section B Point 7	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
122	53	Annexure 12 Section B Point 8	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
123	53	Annexure 12 Section B Point 9	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
124	53	Annexure 12 Section B Point 7	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
125	53	Annexure 12 Section B Point 8	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
126	53	Annexure 12 Section B Point 9	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
127	53	Annexure 12 Section B Point 7	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
128	53	Annexure 12 Section B Point 8	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
129	30	C Others (Point 3)	Eligibility Criteria	Bidder must have the following Accreditations / Certifications: A) ISO 9001 The manufacturing facility of the products quoted under this RFP should have the following Accreditations / Certifications A) ISO 9001 B) ISO14001	Request you revise this clause as - Bidder must have the following Accreditations / Certifications: A) ISO 9001 B) ISO27001 , as certification 9001 is pertaining to Enviormental Management and 27001 is for compliance with information security requirements OR remove certification requirement of ISO 9001	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
130	137	12. Warranty including Annual Maintenance Contract (AMC)	Annexure 12 – Project Details Scope of Work	In event of any equipment / part is replaced or any defect in respect of any equipment / part is corrected for more than one instance of any quarter during the base warranty period of 3 years, where the period of warranty remained is less than twelve month of the comprehensive warranty, the warranty in respect of the entire network hardware equipment for which the equipment / part is replaced / defect is corrected, will be extended for an additional period of twelve months from the date of such replacement/ correction of defects.	Request you ro kindly consider to remove this clause.	No change
131	53	Annexure 12 Section B Point 9	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
132	53	Annexure 12 Section B Point 7	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
133	53	Annexure 12 Section B Point 8	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
134	53	Annexure 12 Section B Point 9	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
135	53	Annexure 12 Section B Point 7	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
136	53	Annexure 12 Section B Point 8	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
137	53	Annexure 12 Section B Point 9	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	No change

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
138	53	Annexure 12 Section B Point 7	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
139	53	Annexure 12 Section B Point 8	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
140	53	Annexure 12 Section B Point 9	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
141	53	Annexure 12, B, pt 6	In the proposed NIPS appliance/solutions if any changes done in existing Policy, Rules, Object and Object Group etc. all audit logs should be available with user id, date/time and Remarks/comments or any other field which should show audit trail change.	The audit log should be maintained by customer's PIM solution. Bidder will integrate the new appliance with customer's PIM solution.		No change
142	53	Annexure 12 Section B Point 7	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
143	53	Annexure 12 Section B Point 8	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
144	53	Annexure 12 Section B Point 9	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
145	54	Annexure 12 Section B Point 19	NIPS: Scope of Work	The proposed NIPS appliance/solutions should provide integration support with Sandboxing solution for in-depth static code analysis, dynamic analysis (malware sandboxing) and machine learning to detect zero-day threats, including threats that use evasion techniques and ransomware.	Fortigate can be integrated with FortiSandbox solution. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR. If yes, should we consider an HA for the same?	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
146	54	Annexure 12 Section B Point 28	NIPS: Scope of Work	The proposed NIPS appliance/solutions should have dedicated emulation engine.	A dedicated emulation engine requires a dedicated appliance for Sandboxing. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR.	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
147	54	Annexure 12 Section B Point 31	NIPS: Scope of Work	The proposed appliance/solutions should have integrated Emulation - GAM (Browser) on appliance itself.	Please provide more details on Integrated emulation - GAM (browser) on appliance, the exact requirement and use-case.	The proposed appliance/solutions should have integrated Emulation - on appliance itself.
148	94	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10/25 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 4x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 8x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,8 nos-10G. BIDI multimode transceiver.
149	54	Annexure 12 Section B Point 19	NIPS: Scope of Work	The proposed NIPS appliance/solutions should provide integration support with Sandboxing solution for in-depth static code analysis, dynamic analysis (malware sandboxing) and machine learning to detect zero-day threats, including threats that use evasion techniques and ransomware.	Fortigate can be integrated with FortiSandbox solution. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR. If yes, should we consider an HA for the same?	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
150	54	Annexure 12 Section B Point 28	NIPS: Scope of Work	The proposed NIPS appliance/solutions should have dedicated emulation engine.	A dedicated emulation engine requires a dedicated appliance for Sandboxing. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR.	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
151	54	Annexure 12 Section B Point 31	NIPS: Scope of Work	The proposed appliance/solutions should have integrated Emulation - GAM (Browser) on appliance itself.	Please provide more details on Integrated emulation - GAM (browser) on appliance, the exact requirement and use-case.	The proposed appliance/solutions should have integrated Emulation - on appliance itself.
152	54	Annexure 12 Section B Point 19	NIPS: Scope of Work	The proposed NIPS appliance/solutions should provide integration support with Sandboxing solution for in-depth static code analysis, dynamic analysis (malware sandboxing) and machine learning to detect zero-day threats, including threats that use evasion techniques and ransomware.	Fortigate can be integrated with FortiSandbox solution. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR. If yes, should we consider an HA for the same?	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
153	54	Annexure 12 Section B Point 28	NIPS: Scope of Work	The proposed NIPS appliance/solutions should have dedicated emulation engine.	A dedicated emulation engine requires a dedicated appliance for Sandboxing. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR.	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
154	54	Annexure 12 Section B Point 31	NIPS: Scope of Work	The proposed appliance/solutions should have integrated Emulation - GAM (Browser) on appliance itself.	Please provide more details on Integrated emulation - GAM (browser) on appliance, the exact requirement and use-case.	The proposed appliance/solutions should have integrated Emulation - on appliance itself.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
155	94/178	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10/25 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 4x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 8x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,8 nos-10G. BIDI multimode transceiver.
156	54	Annexure 12 Section B Point 19	NIPS: Scope of Work	The proposed NIPS appliance/solutions should provide integration support with Sandboxing solution for in-depth static code analysis, dynamic analysis (malware sandboxing) and machine learning to detect zero-day threats, including threats that use evasion techniques and ransomware.	Fortigate can be integrated with FortiSandbox solution. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR. If yes, should we consider an HA for the same?	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
157	54	Annexure 12 Section B Point 28	NIPS: Scope of Work	The proposed NIPS appliance/solutions should have dedicated emulation engine.	A dedicated emulation engine requires a dedicated appliance for Sandboxing. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR.	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
158	54	Annexure 12 Section B Point 31	NIPS: Scope of Work	The proposed appliance/solutions should have integrated Emulation GAM (Browser) on appliance itself.	Please provide more details on Integrated emulation - GAM (browser) on appliance, the exact requirement and use-case.	The proposed appliance/solutions should have integrated Emulation - on appliance itself.
159	17	B.9	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x40/100 GE Fiber, 16x10/25 GE Fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have	The number of ports askd for are beyond the performance capacity for the asked 60G NIPS appliance. It is not recommended to have so many monitoring/prevention segments running on a 60G appliance. Unlike firewalls, NIPS sensors need to perform a lot of signature as well as signature analysis on complete Network traffic along with heuristics, learning, etc. **Request to rephrase the clause as - Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 16x10 GE Fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers.**	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/ 100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20 nos-10G. BIDI multimode transceiver. **To achieve number of ports, stacking is permitted however all other parameters are applicable on single devices.**
160	17	B.9	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x40/100 GE Fiber, 16x10/25 GE Fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have	The number of ports askd for are beyond the performance capacity for the asked 60G NIPS appliance. It is not recommended to have so many monitoring/prevention segments running on a 60G appliance. Unlike firewalls, NIPS sensors need to perform a lot of signature as well as signature analysis on complete Network traffic along with heuristics, learning, etc. **Request to rephrase the clause as - Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 16x10 GE Fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers.**	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/ 100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20 nos-10G. BIDI multimode transceiver. **To achieve number of ports, stacking is permitted however all other parameters are applicable on single devices.**

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
161	54	Annexure 12 Section B Point 19	NIPS: Scope of Work	The proposed NIPS appliance/solutions should provide integration support with Sandboxing solution for in-depth static code analysis, dynamic analysis (malware sandboxing) and machine learning to detect zero-day threats, including threats that use evasion techniques and ransomware.	Fortigate can be integrated with FortiSandbox solution. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR. If yes, should we consider an HA for the same?	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
162	54	Annexure 12 Section B Point 28	NIPS: Scope of Work	The proposed NIPS appliance/solutions should have dedicated emulation engine.	A dedicated emulation engine requires a dedicated appliance for Sandboxing. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR.	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
163	54	Annexure 12 Section B Point 31	NIPS: Scope of Work	The proposed appliance/solutions should have integrated Emulation - GAM (Browser) on appliance itself.	Please provide more details on Integrated emulation - GAM (browser) on appliance, the exact requirement and use-case.	The proposed appliance/solutions should have integrated Emulation - on appliance itself.
164	54	Annexure 12 Section B Point 19	NIPS: Scope of Work	The proposed NIPS appliance/solutions should provide integration support with Sandboxing solution for in-depth static code analysis, dynamic analysis (malware sandboxing) and machine learning to detect zero-day threats, including threats that use evasion techniques and ransomware.	Fortigate can be integrated with FortiSandbox solution. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR. If yes, should we consider an HA for the same?	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
165	54	Annexure 12 Section B Point 28	NIPS: Scope of Work	The proposed NIPS appliance/solutions should have dedicated emulation engine.	A dedicated emulation engine requires a dedicated appliance for Sandboxing. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR.	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
166	54	Annexure 12 Section B Point 31	NIPS: Scope of Work	The proposed appliance/solutions should have integrated Emulation - GAM (Browser) on appliance itself.	Please provide more details on Integrated emulation - GAM (browser) on appliance, the exact requirement and use-case.	The proposed appliance/solutions should have integrated Emulation - on appliance itself.
167	54	Annexure 12 Section B Point 19	NIPS: Scope of Work	The proposed NIPS appliance/solutions should provide integration support with Sandboxing solution for in-depth static code analysis, dynamic analysis (malware sandboxing) and machine learning to detect zero-day threats, including threats that use evasion techniques and ransomware.	Fortigate can be integrated with FortiSandbox solution. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR. If yes, should we consider an HA for the same?	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
168	54	Annexure 12 Section B Point 28	NIPS: Scope of Work	The proposed NIPS appliance/solutions should have dedicated emulation engine.	A dedicated emulation engine requires a dedicated appliance for Sandboxing. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR.	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
169	54	Annexure 12 Section B Point 31	NIPS: Scope of Work	The proposed appliance/solutions should have integrated Emulation - GAM (Browser) on appliance itself.	Please provide more details on Integrated emulation - GAM (browser) on appliance, the exact requirement and use-case.	The proposed appliance/solutions should have integrated Emulation - on appliance itself.
170	18	9 / 2. NIPS Type A	Technical Specifications	9. Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x40/100 GE Fiber, 16x10/25 GE Fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have	Requesting you to change the ports requirement from 16x10/25 GE Fiber to 12x10/25 GE Fiber or consider stacking of the appliances as an option.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/ 100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20 nos-10G. BIDI multimode transceiver. **To achieve number of ports, stacking is permitted however all other parameters are applicable on single devices.**

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
171	18	9 / 2. NIPS Type A	Technical Specifications	9. Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x40/100 GE Fiber, 16x10/25 GE Fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have	Requesting you to change the ports requirement from 16x10/25 GE Fiber to 12x10/25 GE Fiber or consider stacking of the appliances as an option.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/ 100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20 nos-10G. BIDI multimode transceiver. **To achieve number of ports, stacking is permitted however all other parameters are applicable on single devices.**
172	54	Annexure 12 Section B Point 19	NIPS: Scope of Work	The proposed NIPS appliance/solutions should provide integration support with Sandboxing solution for in-depth static code analysis, dynamic analysis (malware sandboxing) and machine learning to detect zero-day threats, including threats that use evasion techniques and ransomware.	FortiGate can be integrated with Forti Sandbox solution. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR. If yes, should we consider an HA for the same?	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
173	54	Annexure 12 Section B Point 28	NIPS: Scope of Work	The proposed NIPS appliance/solutions should have dedicated emulation engine.	A dedicated emulation engine requires a dedicated appliance for Sandboxing. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR.	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
174	54	Annexure 12 Section B Point 31	NIPS: Scope of Work	The proposed appliance/solutions should have integrated Emulation - GAM (Browser) on appliance itself.	Please provide more details on Integrated emulation - GAM (browser) on appliance, the exact requirement and use-case.	The proposed appliance/solutions should have integrated Emulation - on appliance itself.
175	18	9 / 2. NIPS Type A	Technical Specifications	9. Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x40/100 GE Fiber, 16x10/25 GE Fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have	Requesting you to change the ports requirement from 16x10/25 GE Fiber to 12x10/25 GE Fiber or consider stacking of the appliances as an option.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/ 100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20 nos-10G. BIDI multimode transceiver. **To achieve number of ports, stacking is permitted however all other parameters are applicable on single devices.**
176	30	C Others (Point 2)	Eligibility Criteria	The Bidder should be the Original Equipment Manufacturer (OEM) or their authorized partner for supply, installation & support under the proposed product category in India at least for the last 3 years (as on RFP date).	The Bidder should be the Original Equipment Manufacturer (OEM) or **their highest level of partner** for supply, installation & support under the proposed product category in India at least for the last 3 years (as on RFP date).	Pls refer addendum
177	12	Payment Terms (Point 9)	General	AMC payments will be divided into four equal instalments for the each year and paid quarterly at the end of each quarter, on actuals.	Bidder requests Bank to at least pay in 2 equal installments paid in advance at the start of each half year; sicne payout to OEM is annual in advance	No change

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
178	18	9 / 2. NIPS Type A	Technical Specifications	9. Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x40/100 GE Fiber, 16x10/25 GE Fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have	Requesting you to change the ports requirement from 16x10/25 GE Fiber to 12x10/25 GE Fiber or consider stacking of the appliances as an option.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/ 100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20 nos-10G. BIDI multimode transceiver. **To achieve number of ports, stacking is permitted however all other parameters are applicable on single devices.**
179	18	9 / 2. NIPS Type A	Technical Specifications	9. Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x40/100 GE Fiber, 16x10/25 GE Fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have	Requesting you to change the ports requirement from 16x10/25 GE Fiber to 12x10/25 GE Fiber or consider stacking of the appliances as an option.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/ 100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20 nos-10G. BIDI multimode transceiver. **To achieve number of ports, stacking is permitted however all other parameters are applicable on single devices.**
180	137	12. Warranty including Annual Maintenance Contract (AMC)	Annexure 12 – Project Details Scope of Work	In event of any equipment / part is replaced or any defect in respect of any equipment / part is corrected for more than one instance of any quarter during the base warranty period of 3 years, where the period of warranty remained is less than twelve month of the comprehensive warranty, the warranty in respect of the entire network hardware equipment for which the equipment / part is replaced / defect is corrected, will be extended for an additional period of twelve months from the date of such replacement/ correction of defects.	Request you ro kindly consider to remove this clause.	No change
181	55	7 / 4. NIPS Type C	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
182	55	7 / 4. NIPS Type C	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
183	55	7 / 4. NIPS Type C	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
184	55	7 / 4. NIPS Type C	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
185	55	7 / 4. NIPS Type C	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
186	55	7 / 4. NIPS Type C	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
187	55	7 / 4. NIPS Type C	Technical Specifications	7. In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	This is vendor specific, as there is only one OEM provides 50,000 + IPS signatures. So request to change it to at least 20,000+ IPS signatures	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
188	56	Point 8 section A	General Requirement	The proposed Firewall hardware/solution should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats	~~Every vendor has proprietary Hardware / Software~~ architecture to deliver the high scale of performance required in today's demanding environment. ASIC based architecture is not specific to just firewall but also adopted in routers, switches etc. Fortinet has deicated ASIC based architecture which helps deliver higher throughput by offloading specific tasks to the ASIC. Also with regards to the Bank last RFP BID NO: GEM/2023/B/3471981 Dated 22nd May, 2023 Addendum dated 1st July 2023, the same clause has been deleted in the addendum. **Hence Request yuo to please delete this caluse or ammend the clause as** " The device should support multi-~~core architecture~~"	The proposed Firewall hardware/solution should ~~not be proprietary ASIC based in nature & should be open architecture~~ based on multi-core CPU's to protect & scale against dynamic latest security threats
189	56	Point 8 section A	General Requirement	The proposed Firewall hardware/solution should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats	~~Every vendor has proprietary Hardware / Software~~ architecture to deliver the high scale of performance required in today's demanding environment. ASIC based architecture is not specific to just firewall but also adopted in routers, switches etc. Fortinet has deicated ASIC based architecture which helps deliver higher throughput by offloading specific tasks to the ASIC. Also with regards to the Bank last RFP BID NO: GEM/2023/B/3471981 Dated 22nd May, 2023 Addendum dated 1st July 2023, the same clause has been deleted in the addendum. **Hence Request yuo to please delete this caluse or ammend the clause as** " The device should support multi-~~core architecture~~"	The proposed Firewall hardware/solution should ~~not be proprietary ASIC based in nature & should be open architecture~~ based on multi-core CPU's to protect & scale against dynamic latest security threats

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
190	56	Point 8 section A	General Requirement	The proposed Firewall hardware/solution should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats	~~Every vendor has proprietary Hardware / Software~~ architecture to deliver the high scale of performance required in today's demanding environment. ASIC based architecture is not specific to just firewall but also adopted in routers, switches etc. Fortinet has deicated ASIC based architecture which helps deliver higher throughput by offloading specific tasks to the ASIC. Also with regards to the Bank last RFP BID NO: GEM/2023/B/3471981 Dated 22nd May, 2023 Addendum dated 1st July 2023, the same clause has been deleted in the addendum. **Hence Request yuo to please delete this caluse or ammend the clause as** " The device should support multi-~~core architecture~~"	The proposed Firewall hardware/solution should ~~not be proprietary ASIC based in nature & should be open architecture~~ based on multi-core CPU's to protect & scale against dynamic latest security threats
191	56	Point 8 section A	General Requirement	The proposed Firewall hardware/solution should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats	~~Every vendor has proprietary Hardware / Software~~ architecture to deliver the high scale of performance required in today's demanding environment. ASIC based architecture is not specific to just firewall but also adopted in routers, switches etc. Fortinet has deicated ASIC based architecture which helps deliver higher throughput by offloading specific tasks to the ASIC. Also with regards to the Bank last RFP BID NO: GEM/2023/B/3471981 Dated 22nd May, 2023 Addendum dated 1st July 2023, the same clause has been deleted in the addendum. **Hence Request yuo to please delete this caluse or ammend the clause as** " The device should support multi-~~core architecture~~"	The proposed Firewall hardware/solution should ~~not be proprietary ASIC based in nature & should be open architecture~~ based on multi-core CPU's to protect & scale against dynamic latest security threats
192	56	Point 8 section A	General Requirement	The proposed Firewall hardware/solution should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats	~~Every vendor has proprietary Hardware / Software~~ architecture to deliver the high scale of performance required in today's demanding environment. ASIC based architecture is not specific to just firewall but also adopted in routers, switches etc. Fortinet has deicated ASIC based architecture which helps deliver higher throughput by offloading specific tasks to the ASIC. Also with regards to the Bank last RFP BID NO: GEM/2023/B/3471981 Dated 22nd May, 2023 Addendum dated 1st July 2023, the same clause has been deleted in the addendum. **Hence Request yuo to please delete this caluse or ammend the clause as** " The device should support multi-~~core architecture~~"	The proposed Firewall hardware/solution should ~~not be proprietary ASIC based in nature & should be open architecture~~ based on multi-core CPU's to protect & scale against dynamic latest security threats

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
193	56	Point 8 section A	General Requirement	The proposed Firewall hardware/solution should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats	Every vendor has proprietary Hardware / Software architecture to deliver the high scale of performance required in today's demanding environment. ASIC based architecture is not specific to just firewall but also adopted in routers, switches etc. Fortinet has deicated ASIC based architecture which helps deliver higher throughput by offloading specific tasks to the ASIC. Also with regards to the Bank last RFP BID NO: GEM/2023/B/3471981 Dated 22nd May, 2023 Addendum dated 1st July 2023, the same clause has been deleted in the addendum. **Hence Request yuo to please delete this caluse or ammend the clause as** " The device should support multi-core architecture"	The proposed Firewall hardware/solution should ~~not be proprietary ASIC based in nature & should be open architecture~~ based on multi-core CPU's to protect & scale against dynamic latest security threats
194	56	Point 8 section A	General Requirement	The proposed Firewall hardware/solution should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats	Every vendor has proprietary Hardware / Software architecture to deliver the high scale of performance required in today's demanding environment. ASIC based architecture is not specific to just firewall but also adopted in routers, switches etc. Fortinet has deicated ASIC based architecture which helps deliver higher throughput by offloading specific tasks to the ASIC. Also with regards to the Bank last RFP BID NO: GEM/2023/B/3471981 Dated 22nd May, 2023 Addendum dated 1st July 2023, the same clause has been deleted in the addendum. **Hence Request yuo to please delete this caluse or ammend the clause as** " The device should support multi-core architecture"	The proposed Firewall hardware/solution should ~~not be proprietary ASIC based in nature & should be open architecture~~ based on multi-core CPU's to protect & scale against dynamic latest security threats
195	56	Point 8 section A	General Requirement	The proposed Firewall hardware/solution should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats	Every vendor has proprietary Hardware / Software architecture to deliver the high scale of performance required in today's demanding environment. ASIC based architecture is not specific to just firewall but also adopted in routers, switches etc. Fortinet has dedicated ASIC based architecture which helps deliver higher throughput by offloading specific tasks to the ASIC. Also with regards to the Bank last RFP BID NO: GEM/2023/B/3471981 Dated 22nd May, 2023 Addendum dated 1st July 2023, the same clause has been deleted in the addendum. **Hence Request you to please delete this clause or amend the clause as** " The device should support multi-core architecture"	The proposed Firewall hardware/solution should ~~not be proprietary ASIC based in nature & should be open architecture~~ based on multi-core CPU's to protect & scale against dynamic latest security threats

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
196	57	7	B:-Networking , System and Performance Requirements:	The proposed Firewall hardware/solution should support minimum 60 Gbps of production performance (http based) / multiprotocol combined, Firewall & IPS throughput.	Request Bank to change the specification as suggested to ensure performance gurantee of device & current specs seems to be particular OEM proprietory specs."The proposed firewall must provide minimum 60 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and notVideo/JPEG based traffic) (enterprise testing condition). The throughput must remain 60 Gbps even after enabling NGFW + Threat Prevention + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)-"	As per RFP
197	57	8	B:-Networking , System and Performance Requirements:	The proposed Firewall hardware/solution should support minimum 40 Million concurrent sessions with application visibility.	Request Bank to change the specification as suggested to ensure performance gurantee of device & current specs seems to be particular OEM proprietory specs."The proposed firewall must provide minimum 40 Million concurrent sessions with application visibility with Real world Appmix traffic. OEM to provide publicly available Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)-"	As per RFP
198	57	7	B:-Networking , System and Performance Requirements:	The proposed Firewall hardware/solution should support minimum 60 Gbps of production performance (http based) / multiprotocol combined, Firewall & IPS throughput.	Request Bank to change the specification as suggested to ensure performance guarantee of device & current specs seems to be particular OEM proprietary specs. **"The proposed firewall must provide minimum 60 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 60 Gbps even after enabling NGFW + Threat Prevention + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)-"** **Explanation :-** This modification is required to ensure the Bank doesn't run into PERFORMANCE issues with the NGFW in future after enabling various SECURITY functions/features & it will also provode written confimation/certification proof from OEM thus reducing the future Risks to the Bank	As per RFP

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
199	57	8	B:-Networking , System and Performance Requirements:	The proposed Firewall hardware/solution should support minimum 40 Million concurrent sessions with application visibility.	Request Bank to change the specification as suggested to ensure performance guarantee of device & current specs seems to be particular OEM proprietary specs. **"The proposed firewall must provide minimum 40 Million concurrent sessions with application visibility with Real world Appmix traffic. OEM to provide publicly available Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)-"** Explanation :- This modification is required to ensure the Bank doesn't run into PERFORMANCE issues with the NGFW in future after enabling various SECURITY functions/features & it will also provode written confimation/certification proof from OEM thus reducing the	As per RFP
200	18	9 / 2. NIPS Type A	Technical Specifications	9. Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x40/100 GE Fiber, 16x10/25 GE Fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have	Requesting you to change the ports requirement from 16x10/25 GE Fiber to 12x10/25 GE Fiber or consider stacking of the appliances as an option.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/ 100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20 nos-10G. BIDI multimode transceiver. **To achieve number of ports, stacking is permitted however all other parameters are applicable on single devices.**
201	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	~~The bidder should have successfully delivered & installed~~ minimum -02- numbers of each type of firewall and ~~-02- nos. of each type of the equipment i.e~~ NIPS ~~and Router~~ of the proposed/**Similar OEM**, ~~whose products are quoted under this RFP:~~ a)at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having ~~at least 30 Racks~~ at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b)with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part ~~of this RFP~~	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
202	32	D Experience & Support Infrastructure (Point 3)	Eligibility Criteria	The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same / **Similar OEM** ~~whose products are quoted under this RFP~~) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks ~~with turnover of above Rs. 2 lakh crore~~ / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches or with turnover of above Rs. 2 lakh crore	Pls refer addendum
203	30	C Others (Point 3)	Eligibility Criteria	Bidder must have the following Accreditations / Certifications: A) ISO 9001 The manufacturing facility of the products quoted under this RFP should have the following Accreditations / Certifications A) ISO 9001 B) ISO14001	Bidder must have the following Accreditations / Certifications: A) ISO 9001 and ISO 27001:2013. The manufacturing facility of the products quoted under this RFP should have the following Accreditations / Certifications A) ISO 9001 B) ISO14001	Pls refer addendum
204	17	Section 22.11,	General Terms and conditions	The Bank expects the Bidder to adhere to the terms of this tender document and would not accept any deviations to the same.	We request to relax this clause so as to give us an opportunity to suggest amendments.	No change
205	169	Indemnity (Point 18)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	Indemnity-The Service Provider shall indemnify the Bank, and shall always keep indemnified and hold the Bank, its employees, personnel, officers, directors, (hereinafter collectively referred to as "Personnel") harmless from and against any and all losses, liabilities, claims, actions, costs and expenses (including attorneys' fees) relating to, resulting directly or indirectly from or in any way arising out of any claim, suit or proceeding brought against the Bank as a result of: •Bank's authorized / bona fide use of the Deliverables and /or the Services provided by Service Provider under this Agreement; and/or •an act or omission of the Service Provider and/or its employees, agents, subcontractors in performance of the obligations under this Agreement; and/or •claims made by employees or subcontractors or subcontractors' employees, who are deployed by the Service Provider, against the Bank; and/or •claims arising out of employment, non-payment of remuneration and non-provision of statutory benefits by the Service Provider to its employees, its agents, contractors and sub-contractors •breach of any of the term of this Agreement or breach of any representation or false representation or inaccurate statement or assurance or covenant or warranty of the Service Provider under this Agreement; and/or •any or all Deliverables or Services infringing any patent, trademarks, copyrights or such other Intellectual Property Rights; and/or •breach of confidentiality obligations of the Service Provider contained in this Agreement; and/or •Negligence or gross misconduct attributable to the Service Provider or its employees or sub-contractors. Indemnity shall exclude indirect, consequential and incidental damages. However	We submit replacing the current language with the following: "The Indemnifying Party ("Bidder") shall defend (settle and/or pay damages awarded by the court) the Indemnified Party 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 Indemnified Party by reasons of any act or omission of the Indemnifying Party , his agents or employees in the performance of the contractual obligation." We request removal of indemnity clause from NDA.	No change
206	171	Property Rights (Point 19)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	Property Rights -Whereas title to all inventions and discoveries made jointly by the parties resulting from the Work performed as per this agreement shall reside jointly between the parties. Both the parties shall mutually decide the future course of action to protect/ commercial use of such joint IPR. The Intellectual Property Rights shall be determined in accordance with Indian Laws.	We submit that no transfer of ownership of any intellectual property will occur. Customer grants to 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 Customer and identified as such, we grant to the Customer a worldwide, non-exclusive, fully paid, royalty-free license to reproduce and use copies of the deliverables internally.	No change

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
207	174	Limitation of Liability (Point 25)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	Under no circumstances BOB shall be liable to the Service Provider for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of this Agreement, even if BOB has been advised of the possibility of such damages, such as, but not limited to, loss of revenue or anticipated profits or lost business.	We request to make this clause mutual. We will be liable only for direct damages as set out under this clause.	No change
208	174	Limitation of Liability (Point 25)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	However, Service Provider's liability in case of claims against the Bank resulting from Willful Misconduct or Gross Negligence of Service Provider, its employees and Subcontractors or from infringement of patents, trademarks, copyrights or such other Intellectual Property Rights or breach of confidentiality obligations shall be unlimited.	Request to remove IP infringement and breach of confidentiality obligations from unlimited liability.	No change
209	12	Complaince with Laws (Point 12)	General	Compliance with Laws	Please clarify and call out all applicable and relevant laws that the Bidder should be complying with, other than labour laws	No change
210	13	Termination (Point 13)	General	Termination + Risk purchase -Bank reserves the right to terminate this RFP at any stage without any notice or assigning any reason.After the award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one month notice for the same, In such an event, the bidder is bound to make good the additional expenditure which the Bank may have to incur for the execution of the balance of the contract.	Request payments for termination assistance. Request to insert termination for convenience for both parties of 90 days. We also request termination right for Bidder for non-payments by customer. Further, request to include notice period to cure the breach prior to order cancellation / termination. Also request to keep risk purchase to 10% of undelivered deliverables.	No change
211	138	Monitoring and Audit (Point 14)	Annexure 12 – Project Details Scope of Work	Compliance with best security practices may be monitored periodically by computer security audits / Information Security Audits performed by or on behalf of the Bank. The periodicity of these audits will be decided at the discretion of the Bank. These audits may include, but are not limited to, a review of access and authorization procedures, backup and recovery procedures, network security controls and program change controls. The Vendor must provide the Bank access to various monitoring and performance measurement systems. The Vendor has to remedy all discrepancies observed by the auditors at no additional cost to the Bank.	We submit that: Auditors shall NOT be given access to: 1.Any information not related to the Services; 2.Bidder locations/premises (or portions thereof) that are not related to the Services; or 3.Bidder records or documents relating to the make up of Bidder's internal overhead calculations or direct costs, their relationship to the service charges, any financial cost model, calculation of service charges or Bidder's profitability; or 4. Internal Bidder audit reports, or any summaries thereof. We require Independent Monitors to: 1. provide Bidder with at least thirty (10) days notice of its requirement for an Audit allowed once in a year, with such notice describing the issue(s) that will be the subject of the audit; 2. be subject to Bidder site/premises security obligations and have their access controlled/monitored by Bidder; 3. pay all Bidder costs associated with the audit at current time and material rates and submit any requests for Bidder assistance with an audit as a change request. A third party auditor/inspector shall: 1. not be a competitor of Bidder or a third party in dispute / conflict with Bidder; 2. execute a confidentiality agreement acceptable to Bidder; 3. be independent.	No change
212	17	Section 22.9	General Terms and conditions	Acceptance of Terms: the bidders will, by responding to the Bank's RFP document, be deemed to have accepted the terms as stated in this RFP document	We request to relax this clause so as to give us an opportunity to suggest amendments.	No change

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
213	171	Termination (Point 21)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	Termination and Effect of Termination : In following events Bank shall terminate this assignment or cancel any particular order if service provider: breaches any of its obligations set forth in this agreement and Such breach is not cured within 15) Working Days after Bank gives written notice; or • Failure by Service Provider to provide Bank, within 15) Working Days, with a reasonable plan to cure such breach, which is acceptable to the Bank. Or • The progress regarding execution of the contract/ services rendered by the Service Provider is not as per the prescribed time line, and found to be unsatisfactory. • Supply of substandard materials/ services • Delay in delivery / installation / commissioning of services. • Discrepancy in the quality of service / security expected during the implementation, rollout and subsequent maintenance process.	Request payments for termination assistance. Request to insert termination for convenience for both parties of 90 days. We also request termination right for Bidder for non-payments by customer. Further, request to include longer notice period to cure the breach prior to order cancellation / termination (30 days atleast). Also request to keep risk purchase to 10% of undelivered deliverables. In case bank terminates, bank have to compensate for all advance payment done by HPE to OEM and other expences.	No change
214	176	Force Majeure (Point 32)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	Force Majeure- The Service Provider shall not be liable for forfeiture of its performance security, liquidated damages, penalties or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure. For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Service Provider and not involving the Service Provider's fault or negligence and not foreseeable. Such events are Acts of God or of public enemy, acts of Government of India in their sovereign capacity, strikes, political disruptions, bandhs, riots, civil commotions and acts of war. If a Force Majeure situation arises, the Service Provider shall promptly notify the Bank in writing of such conditions and the cause thereof within fifteen calendar days. Unless otherwise directed by the Bank in writing, the Service Provider shall continue to perform Service Provider's obligations under this Agreement as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. In such a case the time for performance shall be extended by a period(s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, the Bank and Service Provider shall hold consultations in an endeavor to find a solution to the problem.	We request all payments be made by BoB to Service Provdier up to the date of suspension of services due to Force Majeure event	No change
215	175	Non-Solicitation (Point 30)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	The Service Provider, during the term of the contract shall not without the express written consent of the Bank, directly or indirectly: a) recruit, hire, appoint or engage or attempt to recruit, hire, appoint or engage or discuss employment with or otherwise utilize the services of any person who has been an employee or associate or engaged in any capacity, by the Bank in rendering services in relation to the contract; or b) induce any person who shall have been an employee or associate of the Bank at any time to terminate his/ her relationship with the Bank.	Request to make clause mutual and keep it to 2 years post termination / expiry of engagement	No change

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
216	18	9 / 2. NIPS Type A	Technical Specifications	9. Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x40/100 GE Fiber, 16x10/25 GE Fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have	Requesting you to change the ports requirement from 16x10/25 GE Fiber to 12x10/25 GE Fiber or consider stacking of the appliances as an option.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/ 100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20 nos-10G. BIDI multimode transceiver. **To achieve number of ports, stacking is permitted however all other parameters are applicable on single devices.**
217	58	Point 12 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.
218	58	Point 12 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.
219	58	Point 12 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
220	58	Point 12 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.
221	58	Point 12 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.
222	58	Point 12 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.
223	58	Point 12 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
224	58	12	B:-Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers.	Request Bank to change the specification as suggested to ensure general specs since current specs seems to be particular OEM proprietory specs,. "Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 12x10G SFP/SFP+ & 4x25G SFP28 fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers."	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.
225	61	7	D :- Network Intrusion Detection & Prevention System Requirements:	The proposed Firewall hardware/solution should supports minimum 50,000 user-defined signatures with Regular Expressions	Request Bank to change point as "The proposed Firewall hardware/solution should supports minimum 15,000 user-defined signatures with Regular Expressions"	The proposed Firewall hardware/solution should support all existing signatures by default and all future signature released from time to time with Regular Expressions
226	61	7	D :- Network Intrusion Detection & Prevention System Requirements:	The proposed Firewall hardware/solution should supports minimum 50,000 user-defined signatures with Regular Expressions	Request Bank to change point as "The proposed Firewall hardware/solution should supports minimum 15,000 user-defined signatures with Regular Expressions" Explanation :- This modification is required to ensure the Bank doesn't run into PERFORMANCE issues with the NGFW in future after enabling various SECURITY functions/features thus reducing the future Risks to the Bank	The proposed Firewall hardware/solution should support all existing signatures by default and all future signature released from time to time with Regular Expressions
227	32	D Experience & Support Infrastructure (Point 4)	Eligibility Criteria	The bidder should have direct support offices in Mumbai and Hyderabad and technically qualified engineers who have expertise in support and installations of the proposed product	We request to you kindly allow us for declataion for opening office at hydrabad location.	Pls refer addendum
228	32	D Experience & Support Infrastructure (Point 3)	Eligibility Criteria	The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	we are request you to kindly change the clause as " The bidder/oem must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches"	Pls refer addendum
229	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	we are request you to kinldy change the clause as "The bidder /oem should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP."	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
230	29	B Financial - Below clause Applicable for the Bidder if submitting bid as a partner of the OEM (Point 1)	Eligibility Criteria	The bidder must have registered average annual turnover of Rs. 120 Crore (MSEs /Start-ups - 50 Crore) or above during the last three completed financial years – 2020-21, 2021-22 and 2022-23 (Not inclusive of the turnover of associate companies) from Indian Operations only.	we are request you to change the clause as " The bidder must have registered average annual turnover of Rs. 100 Crore or above during the last three completed financial years – 2020-21, 2021-22 and 2022-23 (Not inclusive of the turnover of associate companies) from Indian Operations only."	Pls refer addendum
231	11	Payment Terms (Point 9)	General	• 70% of the Hardware cost plus 100% of taxes including GST at actuals after successful delivery. The invoices for claiming the payment should be submitted along with the following documents: a. Original delivery Challans dully stamped and signed by the Bank Official. b. Bill of Materials (BOM) verification report signed by Bank Official. c. Performance Bank Guarantee of 5% of Contact value (As per RFP format) d. Confirmation letter from the OEM mentioning the serial number of Firewall and NIPS and additional components along with underlying software, licenses, allied components (i.e. Operating System etc. if any) and warranty details. • 20% of the cost after one month of successful installation and satisfactory functioning or after two month post-delivery in the case of Site Not Ready (SNR).	we are request you to kinldy change the calsue as "• 80% of the Hardware cost plus 100% of taxes including GST at actuals after successful delivery. The invoices for claiming the payment should be submitted along with the following documents: a. Original delivery Challans dully stamped and signed by the Bank Official. b. Bill of Materials (BOM) verification report signed by Bank Official. c. Performance Bank Guarantee of 5% of Contact value (As per RFP format) d. Confirmation letter from the OEM mentioning the serial number of Firewall and NIPS and additional components along with underlying software, licenses, allied components (i.e. Operating System etc. if any) and warranty details. • 20% of the cost after one month of successful installation and satisfactory functioning or after two month post-delivery in the case of Site Not Ready (SNR)."	No change
232	70	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below-** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
233	70	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below-** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
234	137	12. Warranty including Annual Maintenance Contract (AMC)	Annexure 12 – Project Details Scope of Work	In event of any equipment / part is replaced or any defect in respect of any equipment / part is corrected for more than one instance of any quarter during the base warranty period of 3 years, where the period of warranty remained is less than twelve month of the comprehensive warranty, the warranty in respect of the entire network hardware equipment for which the equipment / part is replaced / defect is corrected, will be extended for an additional period of twelve months from the date of such replacement/ correction of defects.	Request you ro kindly consider to remove this clause.	No change
235	70	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below-** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
236	70	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below-** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
237	70	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below-** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
238	70	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below-** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
239	70	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below-** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
240	70	35	H:- Administration, Management , Centralized Logging & Reporting	The proposed Firewall hardware/solution must be sql based to design custom queries on it	Request Bank to change point as"The proposed Firewall hardware/solution must support custom granular reporting, event management & dashboard for events on it."	The proposed Firewall hardware/solution must support custom granular reporting, event management & dashboard for events on it.
241	70	2	K:- Services ,Support& Training	The proposed Firewall hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC) operated from India	Request Bank to change point as"The proposed Firewal hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC) operated globally"	The proposed Firewall hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC)
242	70	35	H:- Administration, Management , Centralized Logging & Reporting	The proposed Firewall hardware/solution must be SQL based to design custom queries on it	Request Bank to change point as "The proposed Firewall hardware/solution must support custom granular reporting, event management & dashboard for events on it." Explanation :- This is to ensure Bank doesn't run into SQL issues & vulnerabilities of SQL injection thus increasing Riska to the Bank…….also pls. note each OEM uses different techniques to achieve the desired resuls as asked by Bank.	The proposed Firewall hardware/solution must support custom granular reporting, event management & dashboard for events on it.
243	70	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below-** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
244	71	4	K:- Services ,Support& Training	For the proposed Firewall hardware/appliance/solution, the Bidder should arrange/provide highest level of support from OEM Vendor and should assign a designated Technical Account Manager (TAM) on OEM payroll for addressing all critical issues whenever a support ticket is raised. Bank should have 24*7 access to OEM TAM. The OEM TAM should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the proposed firewall hardware/appliance/solution. The OEM TAM should conduct onsite meetings with the concerned Bank officials as well as bidder official to present the findings of the health check and suggest required corrective actions for the proposed firewall hardware/appliance/solution. The OEM TAM should provide monthly status reports for the support cased raised for that month with concerned Bank officials for the proposed firewall hardware/appliance/solution. The OEM TAM should proactively provide security advisories, product version release etc. with the concerned Bank officials and should also extend all required support to the partner in implementing new product releases for the proposed Firewall hardware/appliance/solution.	Request Bank to change point as bidders will provide resources which would be much more cost efficient as compared to OEM resource"For the proposed Firewall hardware/appliance/solution, the Bidder should arrange/provide highest level of support from OEM Vendor and should assign a designated Technical Account Manager (TAM) on Bidder payroll for addressing all critical issues whenever a support ticket is raised. Bank should have 24*7 access to TAM. The OEM Professional Services should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the proposed firewall hardware/appliance/solution. The OEM Professional Services should conduct onsite meetings with the concerned Bank officials as well as bidder official to present the findings of the health check and suggest required corrective actions for the proposed firewall hardware/appliance/solution. The bidder TAM should provide monthly status reports for the support cased raised for that month with concerned Bank officials for the proposed firewall hardware/appliance/solution. The Bidder TAM should proactively provide security advisories, product version release etc. with the concerned Bank officials and should also extend all required support to the partner in implementing new product releases for the proposed Firewall hardware /appliance/solution	Bidders will provide resources which would be much more cost efficient as compared to OEM resource For the proposed Firewall hardware/ appliance /solution, the Bidder should arrange/provide highest level of support from OEM Vendor and should assign a designated Technical Account Manager (TAM) on Bidder payroll for addressing all critical issues whenever a support ticket is raised. Bank should have 24*7 access to TAM. The OEM Professional Services should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the proposed firewall hardware/appliance/solution. The OEM Professional Services should conduct onsite meetings with the concerned Bank officials as well as bidder official to present the findings of the health check and suggest required corrective actions for the proposed firewall hardware/appliance/solution. The bidder TAM should provide monthly status reports for the support cased raised for that month with concerned Bank officials for the proposed firewall hardware/ appliance/solution. The Bidder TAM should proactively provide security advisories, product version release etc. with the concerned Bank officials and should also extend all required support to the partner in implementing new product releases for the proposed Firewall hardware /appliance/solution

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
245	58	12	B:-Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers.	Request Bank to change the specification as suggested to ensure general specs since current specs seems to be particular OEM proprietary specs,. **"Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 12x10G SFP/SFP+ & 4x25G SFP28 fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers."** Explanation :- This modification is required to ensure the Bank gets the correct Connectivity & doesn't OVERSUBSCRIBE/OVERSIZE on the ports,Pls. note since Bank is requiring a 60Gbps NGFW the required ports asked in modification will suffice the 60Gbps Throughput needs of Bank & ensure Bank is not overpaying on per port cost.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/ 100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20 nos-10G. BIDI multimode transceiver. **To achieve number of ports, stacking is permitted however all other parameters are applicable on single devices.**
246	58	Point 12 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.
247	74	Point 9 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.
248	74	Point 9 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
249	74	Point 9 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.
250	74	Point 9 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.
251	74	Point 9 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.
252	74	Point 9 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
253	74	Point 9 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.
254	74	9	B:- System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x40/100 GE Fiber, 16x10/25 GE Fiber. All ports should be populated with required transceivers.	Request Bank to change the specification as suggested to ensure general specs since current specs seems to be particular OEM proprietory specs,. **"Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 12x10G SFP/SFP+ & 4x25G SFP28 fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers."**	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/ 100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20 nos-10G. BIDI multimode transceiver. **To achieve number of ports, stacking is permitted however all other parameters are applicable on single devices.**
255	75	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove this clause.**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
256	75	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed NIPS should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
257	75	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove this clause.**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
258	75	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed NIPS should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
259	75	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove this clause.**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
260	75	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed NIPS should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
261	75	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove this clause.**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
262	75	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed NIPS should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
263	75	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove this clause.**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
264	75	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed NIPS should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
265	75	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove this clause.**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
266	75	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed NIPS should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
267	75	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove this clause.**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
268	75	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed NIPS should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
269	75	7	C:- Performance Requirement	In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	In the proposed NIPS hardware/appliance/solution should support more than 15,000+ IPS attack signatures by default excluding custom signatures.	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
270	133	Compliance and Audit (Point 5)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	Bidder required to participate and comply with in various audits, regulatory requirements and certifications conducted by Bank, RBI, other agencies and various legal entities.	Inspira requesting bank to clarify how frequently will do the audit	No change

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
271	75	8	C:- Performance Requirement	The proposed Firewall hardware/solution should supports minimum 50,000 user-defined signatures with Regular Expressions	Request Bank to change point as "The proposed Firewall hardware/solution should supports minimum 15,000 user-defined signatures with Regular Expressions"	The proposed Firewall hardware/solution should support all existing signatures by default and all future signature released from time to time with Regular Expressions
272	75	7	C:- Performance Requirement	In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	In the proposed NIPS hardware/appliance/solution should support more than 15,000+ IPS attack signatures by default excluding custom signatures. Explanation :-This modification is required to ensure the Bank doesn't run into PERFORMANCE issues with the NGFW in future after enabling various SECURITY functions/features thus reducing the future Risks to the Bank	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
273	75	8	C:- Performance Requirement	The proposed Firewall hardware/solution should supports minimum 50,000 user-defined signatures with Regular Expressions	Request Bank to change point as "The proposed Firewall hardware/solution should supports minimum 15,000 user-defined signatures with Regular Expressions" Explanation :- This modification is required to ensure the Bank doesn't run into PERFORMANCE issues with the NGFW in future after enabling various SECURITY functions/features thus reducing the future Risks to the Bank	The proposed Firewall hardware/solution should support all existing signatures by default and all future signature released from time to time with Regular Expressions
274	75	4	C Performance Requirement	The proposed Firewall hardware/solution should support minimum 40 Million concurrent sessions with application visibility.	Request Bank to change the specification as suggested to ensure performance guarantee of device & current specs seems to be particular OEM proprietary specs. **"The proposed firewall must provide minimum 40 Million concurrent sessions with application visibility with Real world Appmix traffic. OEM to provide publicly available Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)."**	As per RFP
275	171	Termination (Point 21)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	Termination	We propose to add below mentioned language in Termination clause "The bidder shall have right to terminate in the event of winding up of the Bank or in case Bank breaches its obligations under the tender document or the subsequent agreement and if the Bank fails to cure such breach within thirty (30) days from the receipt of notice from the bidder.	No change

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
276	174	Limitation of Liability (Point 25)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	Limitation of liability	Since the liability of parties is not mentioned in the RFP we propose to add the below mentioned language " NOTWITHSTANDING ANY OTHER PROVISION HEREOF, NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES OR ANY DAMAGES FOR LOST PROFITS, LOST REVENUES, LOSS OF GOODWILL, LOSS OF ANTICIPATED SAVINGS, LOSS OF CUSTOMERS, OR LOSS OF DATA, OR INTERFERENCE WITH BUSINESS, ARISING OUT OF THE PERFORMANCE OR FAILURE TO PERFORM UNDER THE AGREEMENT, WHETHER OR NOT CAUSED BY THE ACTS OR OMISSIONS OR NEGLIGENCE (INCLUDING GROSS NEGLIGENCE OR WILLFUL MISCONDUCT) OF ITS EMPLOYEES OR AGENTS, AND REGARDLESS OF WHETHER SUCH PARTY HAS BEEN INFORMED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES. In no event, regardless of the form of the claim or cause of action (whether based in contract, negligence, strict liability, tort or otherwise) shall either Party's aggregate liability to the other Party under the Agreement exceed the fees actually paid under a relevant Purchase Order or Statement of Work which is subject matter of claim.	No change
277	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	We would request you to kindly amend the clause as per below. "The bidder / OEM should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part	Pls refer addendum
278	32	D Experience & Support Infrastructure (Point 3)	Eligibility Criteria	The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	We would request you to amend the clause as per below The bidder/OEM must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
279	75	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove this clause.**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
280	75	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed NIPS should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
281	81	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	NO change
282	81	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	NO change
283	81	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	NO change
284	81	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	NO change
285	81	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	NO change
286	81	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	NO change
287	81	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	NO change
288	81	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	NO change

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
289	87	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
290	87	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
291	87	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
292	87	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
293	87	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
294	87	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
295	87	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
296	87	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
297	87	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
298	87	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
299	87	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec:
300	87	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
301	87	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec:
302	87	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
303	87	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
304	87	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
305	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	Request you to kindly change the clause to Any OEM reference instead of proposed OEM	Pls refer addendum
306	90	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
307	90	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
308	137	12. Warranty including Annual Maintenance Contract (AMC)	Annexure 12 – Project Details Scope of Work	In event of any equipment / part is replaced or any defect in respect of any equipment / part is corrected for more than one instance of any quarter during the base warranty period of 3 years, where the period of warranty remained is less than twelve month of the comprehensive warranty, the warranty in respect of the entire network hardware equipment for which the equipment / part is replaced / defect is corrected, will be extended for an additional period of twelve months from the date of such replacement/ correction of defects.	Request you ro kindly consider to remove this clause.	No change
309	90	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
310	90	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below** · The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
311	90	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
312	90	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
313	90	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
314	90	2	K:- Services ,Support& Training	The proposed Firewall hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC) operated from India	Request Bank to change point as"The proposed Firewal hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC) operated globally"	The proposed Firewall hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC)
315	90	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
316	91	4	K:- Services ,Support& Training	For the proposed Firewall hardware/appliance/solution, the Bidder should arrange/provide highest level of support from OEM Vendor and should assign a designated Technical Account Manager (TAM) on OEM payroll for addressing all critical issues whenever a support ticket is raised. Bank should have 24*7 access to OEM TAM. The OEM TAM should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the proposed firewall hardware/appliance/solution. The OEM TAM should conduct onsite meetings with the concerned Bank officials as well as bidder official to present the findings of the health check and suggest required corrective actions for the proposed firewall hardware/appliance/solution. The OEM TAM should provide monthly status reports for the support cased raised for that month with concerned Bank officials for the proposed firewall hardware/appliance/solution. The OEM TAM should proactively provide security advisories, product version release etc. with the concerned Bank officials and should also extend all required support to the partner in implementing new product releases for the proposed Firewall hardware/appliance/solution.	Request Bank to change point as bidders will provide resources which would be much more cost efficient as compared to OEM resource"For the proposed Firewall hardware/appliance/solution, the Bidder should arrange/provide highest level of support from OEM Vendor and should assign a designated Technical Account Manager (TAM) on Bidder payroll for addressing all critical issues whenever a support ticket is raised. Bank should have 24*7 access to TAM. The OEM Professional Services should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the proposed firewall hardware/appliance/solution. The OEM Professional Services should conduct onsite meetings with the concerned Bank officials as well as bidder official to present the findings of the health check and suggest required corrective actions for the proposed firewall hardware/appliance/solution. The bidder TAM should provide monthly status reports for the support cased raised for that month with concerned Bank officials for the proposed firewall hardware/appliance/solution. The Bidder TAM should proactively provide security advisories, product version release etc. with the concerned Bank officials and should also extend all required support to the	Bidders will provide resources which would be much more cost efficient as compared to OEM resource For the proposed Firewall hardware/ appliance /solution, the Bidder should arrange/provide highest level of support from OEM Vendor and should assign a designated Technical Account Manager (TAM) on Bidder payroll for addressing all critical issues whenever a support ticket is raised. Bank should have 24*7 access to TAM. The OEM Professional Services should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the proposed firewall hardware/appliance/solution. The OEM Professional Services should conduct onsite meetings with the concerned Bank officials as well as bidder official to present the findings of the health check and suggest required corrective actions for the proposed firewall hardware/appliance/solution. The bidder TAM should provide monthly status reports for the support cased raised for that month with concerned Bank officials for the proposed firewall hardware/ appliance/solution. The Bidder TAM should proactively provide security advisories, product version release etc. with the concerned Bank officials and should also extend all required support to the partner in implementing new product releases for the proposed Firewall hardware /appliance/solution
317	74	9	B:- System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x40/100 GE Fiber, 16x10/25 GE Fiber. All ports should be populated with required transceivers.	Request Bank to change the specification as suggested to ensure general specs since current specs seems to be particular OEM proprietary specs,. **"Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 12x10G SFP/SFP+ & 4x25G SFP28 fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers."** Explanation :- This modification is required to ensure the Bank gets the correct Connectivity & doesn't OVERSUBSCRIBE/OVERSIZE on the ports,Pls. note since Bank is requiring a 60Gbps NGFW the required ports asked in modification will suffice the 60Gbps Throughput needs of Bank & ensure Bank is not overpaying on per port cost.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/ 100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20 nos-10G. BIDI multimode transceiver. **To achieve number of ports, stacking is permitted however all other parameters are applicable on single devices.**

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
318	74	Point 9 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.
319	94	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10/25 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 4x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 8x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,8 nos-10G. BIDI multimode transceiver.
320	94	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10/25 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 4x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 8x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,8 nos-10G. BIDI multimode transceiver.
321	94	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10/25 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 4x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 8x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,8 nos-10G. BIDI multimode transceiver.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
322	94	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10/25 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 4x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 8x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,8 nos-10G. BIDI multimode transceiver.
323	94	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10/25 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 4x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 8x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,8 nos-10G. BIDI multimode transceiver.
324	94	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10/25 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	Request Bank to change the specification as suggested to ensure general specs since current specs seems to be particular OEM proprietory specs,. **"Each Appliance of the proposed NIPS hardware/solution should have at least 4x40G/100G QSFP fiber, 12x10G SFP/SFP+ & 4x25G SFP28 fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers."**	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,8 nos-10G. BIDI multimode transceiver.
325	94	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10/25 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	Request Bank to change the specification as suggested to ensure general specs since current specs seems to be particular OEM proprietary specs,. **"Each Appliance of the proposed NIPS hardware/solution should have at least 4x40G/100G QSFP fiber, 12x10G SFP/SFP+ & 4x25G SFP28 fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers."** Explanation :- This modification is required to ensure the Bank gets the correct Connectivity & doesn't OVERSUBSCRIBE/OVERSIZE on the ports,Pls. note since Bank is requiring a 60Gbps NGFW the required ports asked in modification will suffice the 60Gbps Throughput needs of Bank & ensure Bank is not overpaying on per port cost.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,8 nos-10G. BIDI multimode transceiver.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
326	94	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10/25 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 4x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 8x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,8 nos-10G. BIDI multimode transceiver.
327	95	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
328	95	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
329	95	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
330	95	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
331	95	Point 3 Section C	Point 3 Section C	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
332	95	Point 6 Section C	Point 6 Section C	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
333	95	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
334	95	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
335	95	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
336	95	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
337	95	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
338	95	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
339	95	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
340	95	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
341	95	1	C:- Performance Requirement	The proposed NIPS hardware/appliance/solutions IPS Inspection throughput (HTTP Based) should have minimum 30 Gbps	Request Bank to change the specification as suggested to ensure performance gurantee of device & current specs seems to be particular OEM proprietory specs.**"The proposed NIPS hardware/appliance/solutions IPS 30 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and notVideo/JPEG based traffic) (enterprise testing condition). The throughput must remain 30 Gbps even after enabling Threat Prevention + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)-**	As per RFP
342	95	7	C:- Performance Requirement	In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	In the proposed NIPS hardware/appliance/solution should support more than 15,000+ IPS attack signatures by default excluding custom signatures.	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
343	95	8	C:- Performance Requirement	The proposed Firewall hardware/solution should supports minimum 50,000 user-defined signatures with Regular Expressions	Request Bank to change point as "The proposed Firewall hardware/solution should supports minimum 15,000 user-defined signatures with Regular Expressions"	The proposed Firewall hardware/solution should support all existing signatures by default and all future signature released from time to time with Regular Expressions

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
344	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	Request you to consider a contract value of Rs 1.0 Cr instead of 5 Cr	Pls refer addendum
345	31	D Experience & Support Infrastructure (Point 2)	Eligibility Criteria	The bidder should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers / Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the scope of work to be covered as part of this RFP.	We would request you please keep terms as " The bidder/OEM should have successfully delivered & installed minimum -02- numbers of each type of firewall and -02- nos. of each type of the equipment i.e NIPS and Router of the proposed OEM, whose products are quoted under this RFP: a) at minimum -2- Data Centers /Disaster Recovery Centers (Data Centre/ Disaster Recovery Centre of single Organization will be considered as one Order) of Public Sector Banks / Commercial Banks / Financial Institutions / Government Organizations / Public Sector Undertakings (PSUs) / Telecom sector in India, having at least 30 Racks at each Data Center / Disaster Recovery Center, during last -6- Years (as on RFP date) And b) with a contract value of minimum Rs. 5 Crore on each organization. The contract value shall comprise of similar work, as specified in the	Pls refer addendum
346	32	D Experience & Support Infrastructure (Point 3)	Eligibility Criteria	The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	We would request you please keep terms as "The bidder/OEM must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
347	95	1	C:- Performance Requirement	The proposed NIPS hardware/appliance/solutions IPS Inspection throughput (HTTP Based) should have minimum 30 Gbps	Request Bank to change the specification as suggested to ensure performance guarantee of device & current specs seems to be particular OEM proprietary specs. **"The proposed NIPS hardware/appliance/solutions IPS 30 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 30 Gbps even after enabling Threat Prevention + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)-** Explanation :- This modification is required to ensure the Bank doesn't run into PERFORMANCE issues with the NIPS in future after enabling various SECURITY functions/features & it will also provode written confimation/certification proof from OEM thus reducing the future Risks to the Bank.	As per RFP
348	95	7	C:- Performance Requirement	In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	In the proposed NIPS hardware/appliance/solution should support more than 15,000+ IPS attack signatures by default excluding custom signatures. Explanation: - This modification is required to ensure the Bank doesn't run into PERFORMANCE issues with the NGFW in future after enabling various SECURITY functions/features thus reducing the future Risks to the Bank.	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
349	137	12. Warranty including Annual Maintenance Contract (AMC)	Annexure 12 – Project Details Scope of Work	In event of any equipment / part is replaced or any defect in respect of any equipment / part is corrected for more than one instance of any quarter during the base warranty period of 3 years, where the period of warranty remained is less than twelve month of the comprehensive warranty, the warranty in respect of the entire network hardware equipment for which the equipment / part is replaced / defect is corrected, will be extended for an additional period of twelve months from the date of such replacement/ correction of defects	Request you ro kindly consider to remove this clause.	No change
350	95	8	C:- Performance Requirement	The proposed Firewall hardware/solution should supports minimum 50,000 user-defined signatures with Regular Expressions	Request Bank to change point as "The proposed Firewall hardware/solution should supports minimum 15,000 user-defined signatures with Regular Expressions" Explanation :- This modification is required to ensure the Bank doesn't run into PERFORMANCE issues with the NGFW in future after enabling various SECURITY functions/features thus reducing the future Risks to the Bank.	The proposed Firewall hardware/solution should support all existing signatures by default and all future signature released from time to time with Regular Expressions
351	95	4	C:- Performance Requirement	The proposed Firewall hardware/solution should support minimum 20 Million concurrent sessions with application visibility.	Request Bank to change the specification as suggested to ensure performance guarantee of device & current specs seems to be particular OEM proprietary specs. **"The proposed firewall must provide minimum 20 Million concurrent sessions with application visibility with Real world Appmix traffic. OEM to provide publicly available Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)."**	As per RFP

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
352	95	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
353	95	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
354	101	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.
355	101	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.
356	101	Section E Point 32	Section E Point 32	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.
357	101	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.
358	101	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.
359	101	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.
360	101	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
361	101	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.
362	107	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
363	107	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
364	107	Point 31 Section G	Point 31 Section G	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
365	107	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
366	107	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
367	107	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
368	107	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
369	107	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
370	108	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
371	108	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
372	108	Point 34 Section G	Point 34 Section G	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
373	108	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
374	108	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
375	108	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
376	108	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
377	108	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
378	111	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
379	111	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
380	111	Point 2 Section K	Point 2 Section K	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
381	111	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below** · The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
382	111	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
383	111	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
384	111	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
385	111	2	K:- Services ,Support& Training	The proposed Firewall hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC) operated from India	Request Bank to change point as"The proposed Firewal hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC) operated globally"	The proposed Firewall hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC)

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
386	111	4	K:- Services ,Support& Training	For the proposed Firewall hardware/appliance/solution, the Bidder should arrange/provide highest level of support from OEM Vendor and should assign a designated Technical Account Manager (TAM) on OEM payroll for addressing all critical issues whenever a support ticket is raised. Bank should have 24*7 access to OEM TAM. The OEM TAM should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the proposed firewall hardware/appliance/solution. The OEM TAM should conduct onsite meetings with the concerned Bank officials as well as bidder official to present the findings of the health check and suggest required corrective actions for the proposed firewall hardware/appliance/solution. The OEM TAM should provide monthly status reports for the support cased raised for that month with concerned Bank officials for the proposed firewall hardware/appliance/solution. The OEM TAM should proactively provide security advisories, product version release etc. with the concerned Bank officials and should also extend all required support to the partner in implementing new product releases for the proposed Firewall hardware/appliance/solution.	Request Bank to change point as bidders will provide resources which would be much more cost efficient as compared to OEM resource"For the proposed Firewall hardware/appliance/solution, the Bidder should arrange/provide highest level of support from OEM Vendor and should assign a designated Technical Account Manager (TAM) on Bidder payroll for addressing all critical issues whenever a support ticket is raised. Bank should have 24*7 access to TAM. The OEM Professional Services should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the proposed firewall hardware/appliance/solution. The OEM Professional Services should conduct onsite meetings with the concerned Bank officials as well as bidder official to present the findings of the health check and suggest required corrective actions for the proposed firewall hardware/appliance/solution. The bidder TAM should provide monthly status reports for the support cased raised for that month with concerned Bank officials for the proposed firewall hardware/appliance/solution. The Bidder TAM should proactively provide security advisories, product version release etc. with the concerned Bank officials and should also extend all required support to the	Bidders will provide resources which would be much more cost efficient as compared to OEM resource For the proposed Firewall hardware/ appliance /solution, the Bidder should arrange/provide highest level of support from OEM Vendor and should assign a designated Technical Account Manager (TAM) on Bidder payroll for addressing all critical issues whenever a support ticket is raised. Bank should have 24*7 access to TAM. The OEM Professional Services should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the proposed firewall hardware/appliance/solution. The OEM Professional Services should conduct onsite meetings with the concerned Bank officials as well as bidder official to present the findings of the health check and suggest required corrective actions for the proposed firewall hardware/appliance/solution. The bidder TAM should provide monthly status reports for the support cased raised for that month with concerned Bank officials for the proposed firewall hardware/ appliance/solution. The Bidder TAM should proactively provide security advisories, product version release etc. with the concerned Bank officials and should also extend all required support to the partner in implementing new product releases for the proposed Firewall hardware /appliance/solution
387	137	12. Warranty including Annual Maintenance Contract (AMC)	Annexure 12 – Project Details Scope of Work	In event of any equipment / part is replaced or any defect in respect of any equipment / part is corrected for more than one instance of any quarter during the base warranty period of 3 years, where the period of warranty remained is less than twelve month of the comprehensive warranty, the warranty in respect of the entire network hardware equipment for which the equipment / part is replaced / defect is corrected, will be extended for an additional period of twelve months from the date of such replacement/ correction of defects.	Request you ro kindly consider to remove this clause.	No change
388	111	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
389	111	Point 2 Section k	Services ,Support& Training	The proposed Firewall hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC) operated from India	Request Bank to change point as"The proposed Firewal hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC) operated globally" Explanation :- This is to ensure the Bank gets round the clock/across the sun time zones support during the entire day with 24x7x365 support.	The proposed Firewall hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC)

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
390	111	Point 4 Section K	Services ,Support& Training	For the proposed Firewall hardware/appliance/solution, the Bidder should arrange/provide highest level of support from OEM Vendor and should assign a designated Technical Account Manager (TAM) on OEM payroll for addressing all critical issues whenever a support ticket is raised. Bank should have 24*7 access to OEM TAM. The OEM TAM should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the proposed firewall hardware/appliance/solution. The OEM TAM should conduct onsite meetings with the concerned Bank officials as well as bidder official to present the findings of the health check and suggest required corrective actions for the proposed firewall hardware/appliance/solution. The OEM TAM should provide monthly status reports for the support cased raised for that month with concerned Bank officials for the proposed firewall hardware/appliance/solution. The OEM TAM should proactively provide security advisories, product version release etc. with the concerned Bank officials and should also extend all required support to the partner in implementing new product releases for the proposed Firewall hardware/appliance/solution.	Request Bank to change point as bidders will provide resources which would be much more cost efficient as compared to OEM resource"For the proposed Firewall hardware/appliance/solution, the Bidder should arrange/provide highest level of support from OEM Vendor and should assign a designated Technical Account Manager (TAM) on Bidder payroll for addressing all critical issues whenever a support ticket is raised. Bank should have 24*7 access to TAM. The OEM Professional Services should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the proposed firewall hardware/appliance/solution. The OEM Professional Services should conduct onsite meetings with the concerned Bank officials as well as bidder official to present the findings of the health check and suggest required corrective actions for the proposed firewall hardware/appliance/solution. The bidder TAM should provide monthly status reports for the support cased raised for that month with concerned Bank officials for the proposed firewall hardware/appliance/solution. The Bidder TAM should proactively provide security advisories, product version release etc. with the concerned Bank officials and should also extend all required support to the	Bidders will provide resources which would be much more cost efficient as compared to OEM resource For the proposed Firewall hardware/ appliance /solution, the Bidder should arrange/provide highest level of support from OEM Vendor and should assign a designated Technical Account Manager (TAM) on Bidder payroll for addressing all critical issues whenever a support ticket is raised. Bank should have 24*7 access to TAM. The OEM Professional Services should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the proposed firewall hardware/appliance/solution. The OEM Professional Services should conduct onsite meetings with the concerned Bank officials as well as bidder official to present the findings of the health check and suggest required corrective actions for the proposed firewall hardware/appliance/solution. The bidder TAM should provide monthly status reports for the support cased raised for that month with concerned Bank officials for the proposed firewall hardware/ appliance/solution. The Bidder TAM should proactively provide security advisories, product version release etc. with the concerned Bank officials and should also extend all required support to the partner in implementing new product releases for the proposed Firewall hardware /appliance/solution
391	114	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE RJ45. Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	IPS devices are typically deployed at perimeter or Core layer as a L3/L2 device. Hence requirements like additional 24 ports slots cannot be meet by IPS Device, instead you can use a L2 switch as an extender. Also you can ask for additional 4 x 40G/100G slot support if required in future, which will help bank to cater to high bandwidth connectivity requirement when switching infra upgrades in future. **Also let us know beow requirement for SFP transceiver:** 4x10/25 GE Fiber - Please let us know which transceiver should be cosnidered 10G or 25G **Request to modify this clause as below -** Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x10/25 GE Fiber and 16X GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
392	114	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE RJ45. Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	IPS devices are typically deployed at perimeter or Core layer as a L3/L2 device. Hence requirements like additional 24 ports slots cannot be meet by IPS Device, instead you can use a L2 switch as an extender. Also you can ask for additional 4 x 40G/100G slot support if required in future, which will help bank to cater to high bandwidth connectivity requirement when switching infra upgrades in future. **Also let us know beow requirement for SFP transceiver:** 4x10/25 GE Fiber - Please let us know which transceiver should be cosnidered 10G or 25G **Request to modify this clause as below -** Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x10/25 GE Fiber and 16X GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver.
393	114	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE RJ45. Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	IPS devices are typically deployed at perimeter or Core layer as a L3/L2 device. Hence requirements like additional 24 ports slots cannot be meet by IPS Device, instead you can use a L2 switch as an extender. Also you can ask for additional 4 x 40G/100G slot support if required in future, which will help bank to cater to high bandwidth connectivity requirement when switching infra upgrades in future. **Also let us know beow requirement for SFP transceiver:** 4x10/25 GE Fiber - Please let us know which transceiver should be cosnidered 10G or 25G **Request to modify this clause as below -** Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x10/25 GE Fiber and 16X GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
394	114	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE RJ45. Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	IPS devices are typically deployed at perimeter or Core layer as a L3/L2 device. Hence requirements like additional 24 ports slots cannot be meet by IPS Device, instead you can use a L2 switch as an extender. Also you can ask for additional 4 x 40G/100G slot support if required in future, which will help bank to cater to high bandwidth connectivity requirement when switching infra upgrades in future. **Also let us know beow requirement for SFP transceiver:** 4x10/25 GE Fiber - Please let us know which transceiver should be cosnidered 10G or 25G **Request to modify this clause as below -** Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x10/25 GE Fiber and 16X GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver.
395	114	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE RJ45. Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	IPS devices are typically deployed at perimeter or Core layer as a L3/L2 device. Hence requirements like additional 24 ports slots cannot be meet by IPS Device, instead you can use a L2 switch as an extender. Also you can ask for additional 4 x 40G/100G slot support if required in future, which will help bank to cater to high bandwidth connectivity requirement when switching infra upgrades in future. **Also let us know beow requirement for SFP transceiver:** 4x10/25 GE Fiber - Please let us know which transceiver should be cosnidered 10G or 25G **Request to modify this clause as below -** Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x10/25 GE Fiber and 16X GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
396	114	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE RJ45. Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	IPS devices are typically deployed at perimeter or Core layer as a L3/L2 device. Hence requirements like additional 24 ports slots cannot be meet by IPS Device, instead you can use a L2 switch as an extender. Also you can ask for additional 4 x 40G/100G slot support if required in future, which will help bank to cater to high bandwidth connectivity requirement when switching infra upgrades in future. **Also let us know beow requirement for SFP transceiver:** 4x10/25 GE Fiber - Please let us know which transceiver should be cosnidered 10G or 25G **Request to modify this clause as below -** Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x10/25 GE Fiber and 16X GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver.
397	114	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE RJ45. Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	IPS devices are typically deployed at perimeter or Core layer as a L3/L2 device. Hence requirements like additional 24 ports slots cannot be meet by IPS Device, instead you can use a L2 switch as an extender. Also you can ask for additional 4 x 40G/100G slot support if required in future, which will help bank to cater to high bandwidth connectivity requirement when switching infra upgrades in future. **Also let us know beow requirement for SFP transceiver:** 4x10/25 GE Fiber - Please let us know which transceiver should be cosnidered 10G or 25G **Request to modify this clause as below -** Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x10/25 GE Fiber and 16X GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver.
398	114	9	B:- System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x10/25 G E Fiber and 24X1/10 GE RJ45 . Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	Request Bank to change the specification as suggested to ensure general specs since current specs seems to be particular OEM proprietory specs,. **"Each Appliance of the proposed NIPS hardware/solution should have at least 4x40G/100G QSFP fiber, 12x10G SFP/SFP+ & 4x25G SFP28 fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers."**	Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
399	114	9	B:- System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x10/25 G E Fiber and 24X1/10 GE RJ45 . Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	Request Bank to change the specification as suggested to ensure general specs since current specs seems to be particular OEM proprietary specs,. **"Each Appliance of the proposed NIPS hardware/solution should have at least 4x40G/100G QSFP fiber, 12x10G SFP/SFP+ & 4x25G SFP28 fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers."**	Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver
400	114	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE RJ45. Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	IPS devices are typically deployed at perimeter or Core layer as a L3/L2 device. Hence requirements like additional 24 ports slots cannot be meet by IPS Device, instead you can use a L2 switch as an extender. Also you can ask for additional 4 x 40G/100G slot support if required in future, which will help bank to cater to high bandwidth connectivity requirement when switching infra upgrades in future. **Also let us know below requirement for SFP transceiver -** 4x10/25 GE Fiber - Please let us know which transceiver should be considered 10G or 25G **Request to modify this clause as below -** Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x10/25 GE Fiber and 16X GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver.
401	115	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
402	115	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
403	115	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
404	115	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
405	115	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
406	115	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
407	115	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
408	115	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
409	115	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
410	115	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
411	115	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
412	115	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
413	115	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
414	115	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
415	115	1	C:- Performance Requirement	The proposed NIPS hardware/appliance/solutions IPS Inspection throughput (HTTP Based) should have minimum 10 Gbps .	Request Bank to change the specification as suggested to ensure performance gurantee of device & current specs seems to be particular OEM proprietory specs.**"The proposed NIPS hardware/appliance/solutions IPS 30 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and notVideo/JPEG based traffic) (enterprise testing condition). The throughput must remain 30 Gbps even after enabling Threat Prevention + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)-**	As per RFP
416	115	7	C:- Performance Requirement	In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	In the proposed NIPS hardware/appliance/solution should support more than 15,000+ IPS attack signatures by default excluding custom signatures.	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.
417	115	4	C:- Performance Requirement	The proposed Firewall hardware/solution should support minimum 12 Million concurrent sessions with application visibility.	Request Bank to change the specification as suggested to ensure performance gurantee of device & current specs seems to be particular OEM proprietory specs."The proposed firewall must provide minimum 12 Million concurrent sessions with application visibility with Real world Appmix traffic. OEM to provide publicly available Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)-"	As per RFP
418	115	1	C:- Performance Requirement	The proposed NIPS hardware/appliance/solutions IPS Inspection throughput (HTTP Based) should have minimum 10 Gbps .	Request Bank to change the specification as suggested to ensure performance guarantee of device & current specs seems to be particular OEM proprietary specs. **"The proposed NIPS hardware/appliance/solutions IPS 30 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 30 Gbps even after enabling Threat Prevention + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)-**	As per RFP
419	115	7	C:- Performance Requirement	In the proposed NIPS hardware/appliance/solution should support more than 50,000+ IPS attack signatures by default excluding custom signatures.	In the proposed NIPS hardware/appliance/solution should support more than 15,000+ IPS attack signatures by default excluding custom signatures.	In the proposed NIPS hardware/appliance/solution should support all existing IPS attack signatures by default excluding custom signatures and all future signature released from time to time.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
420	115	4	C:- Performance Requirement	The proposed Firewall hardware/solution should support minimum 12 Million concurrent sessions with application visibility.	Request Bank to change the specification as suggested to ensure performance guarantee of device & current specs seems to be particular OEM proprietary specs. **"The proposed firewall must provide minimum 12 Million concurrent sessions with application visibility with Real world Appmix traffic. OEM to provide publicly available Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)."**	As per RFP
421	115	Point 3 Section C	Performance Requirement	The proposed NIPS hardware/appliance/solution can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.	This clause contradicts to the below Note given in RFP: - Note : The performance requirement is for a single hardware appliance and should not be for a cluster/stack. **Hence request you to remove the same**	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.
422	115	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
423	115	Point 4 Section C	C:- Performance Requirement	The proposed Firewall hardware/solution should support minimum 12 Million concurrent sessions with application visibility.	Request Bank to change the specification as suggested to ensure performance gurantee of device & current specs seems to be particular OEM proprietory specs."The proposed firewall must provide minimum 12 Million concurrent sessions with application visibility with Real world Appmix traffic. OEM to provide publicly available Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)-" Explanation :- This modification is required to ensure the Bank doesn't run into PERFORMANCE issues with the NIPS in future after enabling various SECURITY functions/features & it will also provode written confimation/certification proof from OEM thus reducing the future Risks to the Bank.	As per RFP
424	116	10	C:- Performance Requirement	The proposed Firewall hardware/solution should supports minimum 50,000 user-defined signatures with Regular Expressions	Request Bank to change point as "The proposed Firewall hardware/solution should supports minimum 15,000 user-defined signatures with Regular Expressions"	The proposed Firewall hardware/solution should support all existing signatures by default and all future signature released from time to time with Regular Expressions
425	116	10	C:- Performance Requirement	The proposed Firewall hardware/solution should supports minimum 50,000 user-defined signatures with Regular Expressions	Request Bank to change point as "The proposed Firewall hardware/solution should supports minimum 15,000 user-defined signatures with Regular Expressions"	The proposed Firewall hardware/solution should support all existing signatures by default and all future signature released from time to time with Regular Expressions
426	121	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
427	121	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.
428	121	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.
429	121	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.
430	121	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.
431	121	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.
432	121	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.
433	121	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.
434	127	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
435	127	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
436	127	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
437	127	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
438	127	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
439	127	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
440	127	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
441	127	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated on firewall per day. Which depends on the number of firewall policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
442	128	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
443	128	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
444	128	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
445	128	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
446	128	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
447	128	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
448	128	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
449	128	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
450	131	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
451	131	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
452	131	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
453	131	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below** · The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
454	131	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
455	131	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
456	131	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
457	131	2	K:- Services ,Support& Training	The proposed Firewall hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC) operated from India	Request Bank to change point as"The proposed Firewal hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC) operated globally"	The proposed Firewall hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC)
458	131	Point 2 Section K	Service ,Support & Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	**Request to modify this clause as below -** The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.
459	133	Point 2 Section 8	Project Management and Implementation	Bidder should engage OEM's Professional Service for Designing/Deploying/Configuring/Implementing/Integration of the Solution at DC & DR.	Please let us know whether it will be a as is configuration migration from existing Firewall and IPS. And whether bank can provide configuration files from existing firewall and IPS?	It will be as is migration. Details will be shared with L1 bidder.
460	133	Point 2 Section 8	Project Management and Implementation	Bidder should ensure that engaged OEM's Professional Service resources should be deployed onsite at Bank's identified locations DC Mumbai and DC Hyderabad.	Please let us know whether oniset OEM resource is required during implementation only or needed for operational support also.	Onsite support required for implementation only.
461	133	Point 2 Section 8	Project Management and Implementation	Bidder should engage OEM's Professional Service for Designing/Deploying/Configuring/Implementing/Integration of the Solution at DC & DR.	Please let us know whether it will be a as is configuration migration from existing Firewall and IPS. And whether bank can provide configuration files from existing firewall and IPS?	It will be as is migration. Details will be shared with L1 bidder.
462	133	Point 2 Section 8	Project Management and Implementation	Bidder should ensure that engaged OEM's Professional Service resources should be deployed onsite at Bank's identified locations DC Mumbai and DC Hyderabad.	Please let us know whether oniset OEM resource is required during implementation only or needed for operational support also.	Onsite support required for implementation only.
463	133	8. Project Management and Implementation	scope		Is bank considering solution from different OEM for different firewall and NIPS stack?	All firewall should be of the same OEM. Similarly all NIPS should be of same OEM. But firewall and NIPS can be of different OEMs.
464	157	Annexure 20 – Declaration regarding Local Content (LC) for Telecom Product, Services or Works	General		Since the RFP is for procuring security products-NGFW and NIPS and not Telecom Product ,request the bank to remove this annexure.	Pls refer addendum
465	158	Annexure 21 – Certificate of Local Content	general		Request you to exempt the submission of the letter or allow the Bidder/OEM to submit the same in their own format	No Change
466	11	Payment Terms (Point 9)	General	(i) Cost of Firewall and NIPS (Hardware with 3 Years warranty): 20% of the cost after one month of successful installation and satisfactory functioning or after two month post-delivery in the case of Site Not Ready (SNR).	Request Bank to kindly modify the clause as *"20% of the cost after one month of successful installation and satisfactory functioning or after two month post-delivery in the case of Site Not Ready (SNR) whichever is earlier"*	No Change
467	12	Payment Terms (Point 9)	General	(iii) Annual Maintenance Contract (AMC) Cost (Year-4 to Year-7): AMC payments will be divided into four equal instalments for the each year and paid quarterly at the end of each quarter, on actuals. • The payment will be on production of original invoice against receipt of satisfactory support report of previous quarter from Operations Managers of the Bank.	Request bank to kindly release the payment Annual in advance at the start of the year against submission of equal amount of bank guarantee valid for one (1) year	No Change

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
468	140	Delivery (Point 18)	Annexure 12 – Project Details Scope of Work	Vendor will have to pay late delivery charges to Bank @ 1% of the purchase order value inclusive of all taxes, duties, levies etc., per week or part thereof, for late delivery beyond due date of delivery, to a maximum of 5% of the total purchase order value inclusive of all taxes, duties, levies etc. If delay exceeds the maximum percentage of 5%, Bank reserves the right to cancel the entire order.	Request Bank to kindly modify the clause as *"Vendor will have to pay late delivery charges to Bank @ 0.5% of the purchase order value inclusive of all taxes, duties, levies etc., per week or part thereof, for late delivery beyond due date of delivery, to a maximum of 5% of the total purchase order value inclusive of all taxes, duties, levies etc. If delay exceeds the maximum percentage of 5%, Bank reserves the right to cancel the entire order"*	Pls refer addendum
469	144	Annexure 14 – Masked Commercial Bid	General	In the case of additional requirements desired by the Bank, the Bank can place the order for additional 25-30% of the over and above the quantity for which Order is placed with a selected bidder.	Bank will place any additional order in the first 2 years of the contract period. Kindly confirm	Pls refer addendum
470	12	Sub - Contracting (Point 10)	General		We propose to include the following: The Services may be provided in conjunction with other foreign-end administrations, underlying or interconnecting third party carriers, local loop providers or any other authorized providers (collectively or individually **"Third Party Service Providers"**). Bidder's obligations under this RFP do not apply, unless otherwise expressly specified as part of a order form or PO, to the lines, facilities, or services provided by any Third Party Service Provider	No Change
471	12	Compliance with Laws (Point 12)	General		We propose to include the following: "i)The maximum aggregate liability of Bidder, with respect to all indemnity claims under the RFP including intellectual property claims, shall in no event exceeds, the most recent twelve (12) months of charges collected by Bidder pursuant to the applicable PO giving rise to the liability. ii. Under no circumstances shall either Party be liable for any indirect, consequential or incidental losses, damages or claims including loss of profit, loss of business or revenue."	No Change
472	171	Termination (Point 21)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal		We propose that any termination should be subject to Early Termination Charges. Further, kindly include the following: "c) Either Party (the "Non-Defaulting Party") may terminate a Service upon written notice of termination to the other Party ("Defaulting Party") if the Defaulting Party breaches a material provision of this Agreement or the applicable purchase order and the Defaulting Party fails to cure such breach within thirty (30) days after receipt of written notice of breach from the Non-Defaulting Party. d) Bank fails to make a payment when due and Bank fails to cure such breach within fifteen (15) days after receipt of written notice from Bidder. "	No Change
473	16	Right to Reject Bids (Point 21)	General		We propose that bank to be liable for any damages. Loss caused due to such rejection. Further, Bidder should have the right to appeal for any unconditional rejection	No Change
474	133	Point 2 Section 8	Project Management and Implementation	Bidder should engage OEM's Professional Service for Designing/Deploying/Configuring/Implementing/Integration of the Solution at DC & DR.	Please let us know whether it will be a as is configuration migration from existing Firewall and IPS. And whether bank can provide configuration files from existing firewall and IPS?	It will be as is migration. Details will be shared with L1 bidder.

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
475	166	Set-off (Point 15)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	15. SET-OFF Without prejudice to other rights and remedies available to Bank, Bank shall be entitled to set-off or adjust any amounts due to Bank under this clause from the Service Provider against payments due and payable by Bank to the Service Provider for the services rendered.	We propose to delete this clause	No Change
476	166	Covenants of the Service Provider (Point 16)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	16. COVENANTS OF THE SERVICE PROVIDER	We propose that the covenants are too broad therefore it should be reduced to the following for both the Parties: Representations and Warranties of Bank. Bank represents and warrants that (i) it has the legal right and authority, and will maintain the legal right and authority during each Term, to install and use the Services as contemplated hereunder; (ii) the performance of Bank's obligations under this Agreement and use of Services will not violate any applicable law, rule or regulation or any applicable manufacturers' specifications or unreasonably interfere with Successful Bidder's or its other Banks' use of the Services or network; (iii) Bank is authorized and has completed all required corporate actions necessary to execute this Agreement and all order form/purchase order(s); and (iv) Bank shall not carry out any act or omission that results in Successful Bidder breaching any law, rule or regulation. Representations and Warranties of Successful Bidder. Successful Bidder represents and warrants that (i) it has the legal right and authority, and will maintain the legal right and authority during each Service Term, to provide the Services ordered by Bank hereunder; (ii) the performance of Successful Bidder's obligations under this Agreement will not violate any applicable law, rule or regulation; and (iii) Successful Bidder is authorized and has completed all required corporate actions necessary to execute the applicable order form/purchase order (s).	No Change
477	168	Confidentiality (Point 17)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal		We request the Bank to make this provision mutual	No Change
478	169	Indemnity (Point 18)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal		The Indemnity is too broad hence, We request this clause to be replaced with the following: "i. Each Party shall indemnify the other from and against any claims by third parties (including any governmental authority) and expenses (including legal fees and court costs) arising from damage to tangible property, personal injury or death caused by such Party's negligence or wilful misconduct. ii.The maximum aggregate liability of Bidder, with respect to all indemnity claims under the RFP including intellectual property claims, shall in no event exceeds, the most recent twelve (12) months of charges collected by Bidder pursuant to the applicable PO giving rise to the liability."	No Change

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
479	171	Property Rights (Point 19)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	There is no IPR development hence joint ownership is not applicable	There is no IPR development hence joint ownership is not applicable. We propose to replace this clause with the following: (i)Intellectual Property. Bank is and shall remain exclusively entitled to all right and interest in and to all Bank technology, and Successful Bidder is and shall remain exclusively entitled to all right and interest in and to all Successful Bidder technology. Bank shall not, directly or indirectly, reverse engineer, de-compile, disassemble or otherwise attempt to derive source code or other trade secrets from Successful Bidder technology. (ii)License. Ownership of any and all intellectual property rights in any Successful Bidder-provided CPE, software, operating manuals and associated documentation, made available as part of any Service or otherwise generated by or for Successful Bidder in connection with this Agreement, shall remain the property of Successful Bidder or its licensors. Successful Bidder will grant the Bank a personal, non-transferable and non-exclusive license to use and to permit its End-Users to use, in object code form, all software and associated written and electronic documentation and data furnished by Successful Bidder pursuant to this Agreement ("Software"), solely as necessary for receipt of the Service and solely in accordance with this Agreement and the applicable written and electronic documentation. The term of any license granted by Successful Bidder pursuant to this Section is co-terminus with the term for the Service with which the Software is associated. If the Bank purchases the Successful Bidder-provided CPE, once title and risk-of-loss pass to Bank, Bank will be granted a perpetual, royalty free	No Change
480	171	Termination (Point 21)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal		We propose this clause to be made mutual and any termination shall be subject to early termination charges	No Change
481	171	Termination (Point 21)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal	Effect of termination If bank terminates or cancels the assignment on the default mentioned in the termination clause, in such case bob reserves the right to get the balance contract executed by another party of its choice. In this event, the Service Provider shall be bound to make good the additional expenditure, which the Bank may have to incur to carry out bidding process for the selection of a new service provider and for execution of the balance of the contract	We propose that Bank should be liable for early termination charges and all the liability under this RFP to be capped to the TCV	No Change
482	174	Limitation of Liability (Point 25)	Annexure 23 – SERVICE LEVEL AND NON DISCLOSURE AGREEMENT FORMAT - Legal		We request the Bank to restrict the liability to below: "The maximum aggregate liability of Bidder, with respect to all indemnity claims under the RFP including intellectual property claims, shall in no event exceeds, the most recent twelve (12) months of charges collected by Bidder pursuant to the applicable PO giving rise to the liability.""	No Change
483	120	MII	general		Local Make 50% Required is Vendor qualifying for this	No Change
484	142	Annexure 13 – Service Levels	General		99.999 Uptime SLA	No Change
485	133	Point 2 Section 8	Project Management and Implementation	Bidder should ensure that engaged OEM's Professional Service resources should be deployed onsite at Bank's identified locations DC Mumbai and DC Hyderabad.	Please let us know whether oniset OEM resource is required during implementation only or needed for operational support also.	Onsite support required for implementation only.
486	133	Point 2 Section 8	Project Management and Implementation	Bidder should engage OEM's Professional Service for Designing/Deploying/Configuring/Implementing/Integration of the Solution at DC & DR.	Please let us know whether it will be a as is configuration migration from existing Firewall and IPS. And whether bank can provide configuration files from existing firewall and IPS?	It will be as is migration. Details will be shared with L1 bidder.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
487	133	Point 2 Section 8	Project Management and Implementation	Bidder should ensure that engaged OEM's Professional Service resources should be deployed onsite at Bank's identified locations DC Mumbai and DC Hyderabad.	Please let us know whether oniset OEM resource is required during implementation only or needed for operational support also.	Onsite support required for implementation only.
488	53	Annexure 12, B, pt 5	Bidder should ensure that all existing Policy, Rules, Object and Object Group should be migrated to the proposed NIPS appliance/solutions post optimization as application based Policy, Rules, Object and Object Group.	Please share the existing appliance details from which we need to migrate from.		Details will be shared later with L1 bidder
489	133	Point 2 Section 8	Project Management and Implementation	Bidder should engage OEM's Professional Service for Designing/Deploying/Configuring/Implementing/Integration of the Solution at DC & DR.	Please let us know whether it will be a as is configuration migration from existing Firewall and IPS. And whether bank can provide configuration files from existing firewall and IPS?	It will be as is migration. Details will be shared with L1 bidder.
490	134	8.6	Bidder should ensure Onsite Resources for Management and co-ordination.	Bidder will provide on-site implementation team. Kindly accept the project management to be remote.		As per RFP
491	133	Point 2 Section 8	Project Management and Implementation	Bidder should ensure that engaged OEM's Professional Service resources should be deployed onsite at Bank's identified locations DC Mumbai and DC Hyderabad.	Please let us know whether oniset OEM resource is required during implementation only or needed for operational support also.	Onsite support required for implementation only.
492	133	Point 2 Section 8	Project Management and Implementation	Bidder should engage OEM's Professional Service for Designing/Deploying/Configuring/Implementing/Integration of the Solution at DC & DR.	Please let us know whether it will be a as is configuration migration from existing Firewall and IPS. And whether bank can provide configuration files from existing firewall and IPS?	It will be as is migration. Details will be shared with L1 bidder.
493	133	Point 2 Section 8	Project Management and Implementation	Bidder should ensure that engaged OEM's Professional Service resources should be deployed onsite at Bank's identified locations DC Mumbai and DC Hyderabad.	Please let us know whether oniset OEM resource is required during implementation only or needed for operational support also.	Onsite support required for implementation only.
494	133	Point 2 Section 8	Project Management and Implementation	Bidder should engage OEM's Professional Service for Designing/Deploying/Configuring/Implementing/Integration of the Solution at DC & DR.	Please let us know whether it will be a as is configuration migration from existing Firewall and IPS. And whether bank can provide configuration files from existing firewall and IPS?	It will be as is migration. Details will be shared with L1 bidder.
495	133	Point 2 Section 8	Project Management and Implementation	Bidder should ensure that engaged OEM's Professional Service resources should be deployed onsite at Bank's identified locations DC Mumbai and DC Hyderabad.	Please let us know whether oniset OEM resource is required during implementation only or needed for operational support also.	Onsite support required for implementation only.
496	136	10.11	During the contract period, if there is an upgrade done by Bidder and require a knowledge transfer on the process in to addition to existing process in place , The Bidder should provide such training on best practices to Bank's MSP/Vendor and be followed to support the hardware/software function smoothly	This should be the scope of the security team managing the device. If customer need yearly training, then this requirement should be part of the requirement.		As per RFP
497	133	Point 2 Section 8	Project Management and Implementation	Bidder should engage OEM's Professional Service for Designing/Deploying/Configuring/Implementing/Integration of the Solution at DC & DR.	Please let us know whether it will be a as is configuration migration from existing Firewall and IPS. And whether bank can provide configuration files from existing firewall and IPS?	It will be as is migration. Details will be shared with L1 bidder.
498	133	Point 2 Section 8	Project Management and Implementation	Bidder should ensure that engaged OEM's Professional Service resources should be deployed onsite at Bank's identified locations DC Mumbai and DC Hyderabad.	Please let us know whether onset OEM resource is required during implementation only or needed for operational support also.	Onsite support required for implementation only.
499	134	9. Scope of Work for Onsite support during implementation	Scope	Bidder should engage OEM's Professional Service for Designing/Deploying/Configuring/Implementing/Integration of the Solution at DC & DR.	Our understanding is Design/Deploying/Configuring/Implementing/Integrating of the proposed solution will be performed by bidder. OEM will be responsible for review and guiding bidder for implementation. Kindly confirm	It will be as is migration. Details will be shared with L1 bidder.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
500	134	9. Scope of Work for Onsite support during implementation	Scope	The OEM's technical/implementation team should be an active part of the implementation team and should support throughout the solution implementation/project sign off, which should be provided without any additional cost	Our understanding is OEM will support bidder throughout mplementation/project sign off of the proposed solution will be performed by bidder. Bidder will be responsible for above activities. Kindly confirm	As per RFP
501	134	9. Scope of Work for Onsite support during implementation	scope	Overall management of the complete solution such as refinement of policies,creation of policies, configuration optimization or any changes/modifications to be done for enforcing Bank's policies, etc.	Our understanding is rule optimization of any existing solution will be out of bidders scope and bidder is responsible to implementation solution in As-Is basis in case migration from existing to new solution is required. Kindly confirm	As per RFP
502	134	9. Scope of Work for Onsite support during implementation	scope	Overall management of the complete solution such as refinement of policies,creation of policies, configuration optimization or any changes/modifications to be done for enforcing Bank's policies, etc.	Requesting bank to provide clarity on refinement of policies. Our udnerstanding is policy optimization will be out of bidders scope and bidder is responsible to implement solution As-Is in case migration from existing to new solution is required. Kindly confirm	As per RFP
503	134	9. Scope of Work for Onsite support during implementation	scope	Proactive monitoring of health of the solution, including the H/W, S/W, application, solution on various parameters such as CPU, memory, interface utilizations, etc. Reporting abnormalities to the Bank as and when observed/occurred.	Requesting bank to comnfirm if bank will provide monitoring tool to integrate proposed solution and monitoring via the same.	EMS tools will be used for monitoring.
504	134	9. Scope of Work for Onsite support during implementation	scope	Preparing and submitting regular reports as and when required by the Bank	Our understanding is bidder is required to submit standard reports generated from proposed firewall and IPS solution.	As per RFP
505	134	9. Scope of Work for Onsite support during implementation	scope	Troubleshooting day to day issues, faced by end users, pertaining to solution in coordination with Bank's Network integrator, security integrator, or other relevant teams/Bidders.	Requesting bank to confirm how bidders engineer will access to deployed solution components in case troubleshooting activity is required to be performed post implementation sign-off, as bank will take handover of the proposed solution post deployment done by the bidder	As per RFP
506	134	9. Scope of Work for Onsite support during implementation	scope	Keep back up of log, configuration, data etc.	Our understanding is bank will provide required tools and infra to store configuration and log level backup. Bidder is not required to propose the same. Kindly confirm	Bank will provide required tools.
507	134	9. Scope of Work for Onsite support during implementation	scope	Bidder shall suitably and adequately train the Bank's and its MSP team for fully and effectively manning, operating and maintaining the deliverables under this contract.	Requesting bank to confirm if OEM training is required to be provided to banks officials. If yes, requesting to confirm -No. of training sessions -No. of days for each training sessions -No. of officials for which training sessions are required	Details will be shared later with L1 bidder
508	134	9. Scope of Work for Onsite support during implementation	scope	Bidder shall provide inventory details for Firewall, NIPS assets including licenses.	Our understanding is bidder is required to provide inventory details only for proposed Firewall NIPS solution. Kindly confirm	As per RFP
509	134	9. Scope of Work for Onsite support during implementation	scope	Bidder shall provide inventory details for Firewall, NIPS assets including licenses.	For OEM training requesting you to confirm -No. of training sessions -No. of days for each training sessions -No. of officials for which training sessions are required	Details will be shared later with L1 bidder
510	134	9.2	Overall management of the complete solution such as refinement of policies, creation of policies, configuration optimization or any changes/modifications to be done for enforcing Bank's policies, etc.	Does BoB need dedicated team on-site for management of all the required appliance for the duration of the contract		Onsite team required for post implementation support phase.
511	134	9.2	Overall management of the complete solution such as refinement of policies, creation of policies, configuration optimization or any changes/modifications to be done for enforcing Bank's policies, etc.	If it is one time installation only - Then post migration and acceptance. The device will be handed over to the BoB's security team for management.		As per RFP

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
512	134	9.4	Proactive monitoring of health of the solution, including the H/W, S/W, application, solution on various parameters such as CPU, memory, interface utilizations, etc. Reporting abnormalities to the Bank as and when observed/occurred.	Does BoB have an central NMS tool to monitor hardware?		EMS tools will be used for monitoring.
513	134	9.6	Troubleshooting day to day issues, faced by end users, pertaining to solution in coordination with Bank's Network integrator, security integrator, or other relevant teams/Bidders.	Post device handover. This should be managed by BoB security team.		As per RFP
514	136	10.10	Post-handover of services, the Bidder shall continue to provide necessary support and services during warranty and AMC period for all the components supplied and installed as per this contract including SLA.	Define in detail the post handover support required.		Details will be shared later with L1 bidder
515	138	12	General	Warranty should not become void if the Bank buys any other supplemental hardware from third party and installs it with/in these machines. However, the warranty will not apply to such hardware items installed.	Warranty will not be applicable if the root cause of system failure is installation of such 3rd party HWs	No Change
516	138	13	General		HPE will be submitting the best price based on the duration and quantity of the RFP, the same will be used in negotiating best cost from OEMs as well, hence any reduction in scope and duration may lead to change in price	No Change
517	138	13	Annual Maintenance Contract and Annual Technical Support		Inspira requesting bank to clarify about existing helpdesk tool. Let us know the call logging flow (Work Flow)	Details will be shared later with L1 bidder
518	139	16. Technical Proposal Attention Items	scope	Compliance with best security practices may be monitored periodically by computer security audits / Information Security Audits performed by or on behalf of the Bank. The periodicity of these audits will be decided at the discretion of the Bank. These audits may include, but are not limited to, a review of access and authorization procedures, backup and recovery procedures, network security controls and program change controls. The Vendor must provide the Bank access to various monitoring and performance measurement systems. The Vendor has to remedy all discrepancies observed by the auditors at no additional cost to the Bank.	Our understanding is bank will provide existing monitoring tool owned by bank to integrate proposed solution for monitoring purposes. Kindly confirm	Bank will provide required tools.
519	140	Delivery (Point 18)	Annexure 12 – Project Details Scope of Work	Vendor will have to pay late delivery charges to Bank @ 1% of the purchase order value inclusive of all taxes, duties, levies etc., per week or part thereof, for late delivery beyond due date of delivery, to a maximum of 5% of the total purchase order value inclusive of all taxes, duties, levies etc.	Kindly request the bank to levy penalty on the undelivered value of product or services for the delay in project deliverables, also LD keep LD as 0.5% with Maximum cap 2.5%	Pls refer addendum
520	140	Installation & Implementation (Point 19)	Annexure 12 – Project Details Scope of Work	Vendor will have to pay late installation / implementation charges to the Bank @ 1% of the total Purchase Order Value per day or part thereof subject to maximum of 5% of the total purchase order value, for delay in installation, if the delay is caused owing to reasons attributable to the Vendor.	Kindly request the bank to levy penalty on the undelivered value of product or services for the delay in project deliverables, also LD keep LD as 0.5% with Maximum cap 2.5%	Pls refer addendum
521	140	Delivery (Point 18)	Annexure 12 – Project Details Scope of Work	The successful vendor shall deliver and complete installation as per project scope within a period of 8 weeks in totality from the date of placing of purchase order by the Bank. The delivery and installation as per the required scope needs to be completed as per the timelines mentioned.	We request you to revise the Project delivery timeline as - 12-14 weeks	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
522	140	18	General	The successful vendor shall deliver and complete installation as per project scope within a period of 8 weeks in totality from the date of placing of purchase order by the Bank. The delivery and installation as per the required scope needs to be completed as per the timelines mentioned. Vendor will have to pay late delivery charges to Bank @ 1% of the purchase order value inclusive of all taxes, duties, levies etc., per week or part thereof, for late delivery beyond due date of delivery, to a maximum of 5% of the total purchase order value inclusive of all taxes, duties, levies etc. If delay exceeds the maximum percentage of 5%, Bank reserves the right to cancel the entire order	Bidder request to clarify that the LD shall be 0.5% of the TCV (excluding GST) of the delayed component subject to a cap of 5% of Delayed delivered Item	Pls refer addendum
523	140	19	General	Vendor will have to pay late installation / implementation charges to the Bank @ 1% of the total Purchase Order Value per day or part thereof subject to maximum of 5% of the total purchase order value, for delay in installation, if the delay is caused owing to reasons attributable to the Vendor	Bidder request to clarify that the LD shall be 0.5% of the TCV (excluding GST) of the delayed component subject to a cap of 5% of TCV	Pls refer addendum
524	140	21	General	Acceptance Test (AT)	Bidder request to clarify that the Acceptance test shall be completed and communication of acceptance/rejection shall be done within 2 weeks from the date of completion of installation. If no response is received from the customer within this period, the deliverable shall be deemed as accepted.	No Change
525	140	Installation & Implementation (Point 19)	Annexure 12 – Project Details Scope of Work	Vendor will have to install the network hardware and hand it over to Bank for acceptance testing within 2 weeks from the date of receipt of the network hardware at our office and Bank's notification for installation of the same	Inspira requesting bank to extend four week more here.Migration parts also available. So totally delivery and Implementation we need 14 weeks.	Pls refer addendum
526	141	22	General	The Bank reserves the right to alter the requirements specified in the Tender. The Bank also reserves the right to delete one or more items from the list of items specified in the Tender. The Bank will inform all Bidders about changes, if any. The Bidder agrees that the Bank has no limit on the additions or deletions on the items for the period of the contract. Further the Bidder agrees that the prices quoted by the Bidder would be proportionately adjusted with such additions or deletions in quantities/items	Bidder request to clarify that the price shall be redetermined using the proposed rates only if the change is within +/-25% of the original quanity. Any change beyond this will lead to change in rates used to calculate overall price. Additional order to be placed within the initial implementation period, price shall be mutually agrred between teh parties for order placed beyond this period	Pls refer addendum
527	142	Annexure 13 – Service Levels	General	Penalty to be levied on product cost during warranty period.	Kindly reuest the bank to levy service level penalties on the AMC value throughout the contract duration (warranty and AMC period) at the levels mentioned for AMC.	No Change
528	142	Annexure 13 – Service Levels	General	The SLA charges will be subject to an overall cap of 10% of the product cost during warranty period and 50% of the total quarterly AMC cost during AMC period	Kindly request the bank to cap the service level penalties to overall 10% of AMC value in each year of contract (warranty and AMC)	No Change
529	142	Annexure 13 – Service Levels	General	Bidder should have to guarantee a minimum uptime of 99.999%, calculated on a monthly basis. Application availability along with the requisite hardware /appliance will be 99.999% on 24x7x365.	Inspira requesting bank to change this with Proposed solution be 99.999% on 24X7X365 Instead of Application availability along with the requisite hardware /appliance will be 99.999% on 24x7x365.Please clarify applicatio availability. And let us know the which application	No Change
530	146	Annexure 14, L	General	In the case of additional requirements desired by the Bank, the Bank can place the order for additional 25-30% of the over and above the quantity for which Order is placed with a selected bidder.	Bidder request to clarify that the additional quanity shall be priced at teh proposed rates only if the additional order is placed during the initial implementation period. Price of order placed beyind this period shall be mutually agreed between the parties	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
531	148	Section f	Annexure 15 – Commercial Bid	f. The minimum AMC / ATS amount to be quoted by the vendor in the commercial proposal is 4% per annum on the base price of Hardware.	4% per annum is very high amount for AMC of hardware products. Kindly request the bank to revise this percentage to 2% per annum on base price of hardware.	No Change
532	166	15.Set off	Annexure 12 – Project Details Scope of Work	Without prejudice to other rights and remedies available to Bank, Bank shall be entitled to set-off or adjust any amounts due to Bank under this clause from the Service Provider against payments due and payable by Bank to the Service Provider for the services rendered.	Bidder request to clarify that the set off shall be done only with the amounts due under this contract. Inter contract set off shall not be allowed	No Change
533	167	16.x	General	shall be liable to BANK for any and all losses of any nature whatsoever arisen directly or indirectly by negligence, dishonest, criminal or fraudulent act of any of the representatives and employees of the Service Provider while providing the services to the BANK.	under no circumstances, the bidder shall be liable for indirect damages	No Change
534	137	12. Warranty including Annual Maintenance Contract (AMC)	Annexure 12 – Project Details Scope of Work	In event of any equipment / part is replaced or any defect in respect of any equipment / part is corrected for more than one instance of any quarter during the base warranty period of 3 years, where the period of warranty remained is less than twelve month of the comprehensive warranty, the warranty in respect of the entire network hardware equipment for which the equipment / part is replaced / defect is corrected, will be extended for an additional period of twelve months from the date of such replacement/ correction of defects.	Request you to kindly consider to remove this clause.	No Change
535	172	21	General	Effect of termination If bank terminates or cancels the assignment on the default mentioned in the termination clause, in such case bob reserves the right to get the balance contract executed by another party of its choice. In this event, the Service Provider shall be bound to make good the additional expenditure, which the Bank may have to incur to carry out bidding process for the selection of a new service provider and for execution of the balance of the contract. Immediately upon the date of expiration or termination of the Agreement, Bank shall have no further obligation to pay any fees for any periods commencing on or after such date. Without prejudice to the rights of the Parties, upon termination or expiry of this Agreement, Bank shall pay to Service Provider, within thirty (30) days of such termination or expiry, All the undisputed fees outstanding till the date	Bidder request the below modification. 1. Service Provider shall be bound to make good the additional **reasonable** expenditure incurred by the bank to get the balance contract excuted. Risk purchase under this clause shall be capped to 10% of the TCV. 2. Irrespective of the resaon for termination, BOB shall pay the fee for the services rendered till teh effective date of termination along with the **upfront payment made by the service provider to the OEM for warranty/AMCs.** This is required as service provider pays the AMC charge upfront to teh OEMs whereas the billing to BOB is done quarterly in arrears	No Change
536	32	D Experience & Support Infrastructure (Point 3)	Eligibility Criteria	The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	Request you to please remove having network of minimum 1000 domestice branches clause as mostly Banks have 1000 domestices branches. Financials institutions / Government orginization / Telecom sectors dosent have this scale of Branches.	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
537	114/178	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x10/25 GE Fiber and 24X1/10 GE RJ45. Also should have provision to add additional I/O card slot to add 24X1/10 GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	IPS devices are typically deployed at perimeter or Core layer as a L3/L2 device. Hence requirements like additional 24 ports slots cannot be meet by IPS Device, instead you can use a L2 switch as an extender. Also you can ask for additional 4 x 40G/100G slot support if required in future, which will help bank to cater to high bandwidth connectivity requirement when switching infra upgrades in future. **Also let us know beow requirement for SFP transceiver:** 4x10/25 GE Fiber - Please let us know which transceiver should be cosnidered 10G or 25G **Request to modify this clause as below -** Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 8x10/25 GE Fiber and 16X GE RJ45.The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	Each Appliance in the proposed NIPS ardware/appliance/solution should have at least 4x10 GE Fiber and 24X1 GE or higher The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities". BIDI multimode transceiver.
538	131-132	4	K:- Services ,Support& Training	For the proposed Firewall hardware/appliance/solution, the Bidder should arrange/provide highest level of support from OEM Vendor and should assign a designated Technical Account Manager (TAM) on OEM payroll for addressing all critical issues whenever a support ticket is raised. Bank should have 24*7 access to OEM TAM. The OEM TAM should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the proposed firewall hardware/appliance/solution. The OEM TAM should conduct onsite meetings with the concerned Bank officials as well as bidder official to present the findings of the health check and suggest required corrective actions for the proposed firewall hardware/appliance/solution. The OEM TAM should provide monthly status reports for the support cased raised for that month with concerned Bank officials for the proposed firewall hardware/appliance/solution. The OEM TAM should proactively provide security advisories, product version release etc. with the concerned Bank officials and should also extend all required support to the partner in implementing new product releases for the proposed Firewall hardware/appliance/solution.	Request Bank to change point as bidders will provide resources which would be much more cost efficient as compared to OEM resource"For the proposed Firewall hardware/appliance/solution, the Bidder should arrange/provide highest level of support from OEM Vendor and should assign a designated Technical Account Manager (TAM) on Bidder payroll for addressing all critical issues whenever a support ticket is raised. Bank should have 24*7 access to TAM. The OEM Professional Services should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the proposed firewall hardware/appliance/solution. The OEM Professional Services should conduct onsite meetings with the concerned Bank officials as well as bidder official to present the findings of the health check and suggest required corrective actions for the proposed firewall hardware/appliance/solution. The bidder TAM should provide monthly status reports for the support cased raised for that month with concerned Bank officials for the proposed firewall hardware/appliance/solution. The Bidder TAM should proactively provide security advisories, product version release etc. with the concerned Bank officials and should also extend all required support to the	Bidders will provide resources which would be much more cost efficient as compared to OEM resource For the proposed Firewall hardware/ appliance /solution, the Bidder should arrange/provide highest level of support from OEM Vendor and should assign a designated Technical Account Manager (TAM) on Bidder payroll for addressing all critical issues whenever a support ticket is raised. Bank should have 24*7 access to TAM. The OEM Professional Services should conduct half yearly health check for the deployed solution. The health check should cover detailed configuration audit, findings and recommendations of the proposed firewall hardware/appliance/solution. The OEM Professional Services should conduct onsite meetings with the concerned Bank officials as well as bidder official to present the findings of the health check and suggest required corrective actions for the proposed firewall hardware/appliance/solution. The bidder TAM should provide monthly status reports for the support cased raised for that month with concerned Bank officials for the proposed firewall hardware/ appliance/solution. The Bidder TAM should proactively provide security advisories, product version release etc. with the concerned Bank officials and should also extend all required support to the partner in implementing new product releases for the proposed Firewall hardware /appliance/solution
539	133/178	Point 2 Section 8	Project Management and Implementation		Please let us know whether it will be as is configuration migration from existing Firewall and IPS. And whether bank can provide configuration files from existing firewall and IPS?	Configuation file for existing firewall and IPS will be provided

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
540	133/178	Point 2 Section 8	Project Management and Implementation	Bidder should ensure that engaged OEM's Professional Service resources should be deployed onsite at Bank's identified locations DC Mumbai and DC Hyderabad.	Please let us know whether oniset OEM resource is required during implementation only or needed for operational support also.	Onsite support required for implementation only.
541	140	Delivery (Point 18)	Annexure 12 – Project Details Scope of Work	The successful vendor shall deliver and complete installation as per project scope within a period of 8 weeks in totality from the date of placing of purchase order by the Bank.	Bidder request bank to change this to : The successful vendor shall deliver and complete installation as per project scope within a period of **12** weeks in totality from the date of placing of purchase order by the Bank since this is not going to be greenfield deployment but there will be some amount of migration from existing devices to proposed solution	Pls refer addendum
542	142	Annexure 13 – Service Levels	General	99/998% =<A<99.999%	This indicates penalty for more than 5 min of Product downtime . Kindly relook viz.a.viz CTR SLA sought by the bank. Request to change this to Solution downtime instead of Product downtime . Bidder request to reduce the SLA% under each category and cap the SLA% as per below. 1. During Warranty period : Quarterly capping of 10% of the indicative quarterly warranty chages for the specific product calculated based on the AMC rates provided during AMC period for that particular product 2. During AMC period : 10% of the quarterly AMC charges per quarter	No Change
543	51/178	Annexure 12 Section A Point 7	Firewall: Scope of Work	The proposed Firewall appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for Firewall. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed Firewall appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
544	51/178	Annexure 12 Section A Point 8	Firewall: Scope of Work	The proposed Firewall appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for Firewall. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed Firewall appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
545	51/178	Annexure 12 Section A Point 9	Firewall: Scope of Work	The proposed Firewall appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for Firewall. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed Firewall appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
546	53/178	Annexure 12 Section B Point 7	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if the same is already present i.e. should not allow duplicate policy addition or deployment	Detection of duplicate objects is achieved by management solution for NIPS. It performs policy checks during policy installation to check duplicate objects. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify duplicate objects so that corrective actions can be taken.
547	53/178	Annexure 12 Section B Point 8	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping or shadowed with existing Policy Rule and Objects.	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
548	53/178	Annexure 12 Section B Point 9	NIPS: Scope of Work	The proposed NIPS appliance/solutions should not allow addition of any new policy rule or objects if it is overlapping with existing Policy Rule and Objects	Detection of overlapping/shadowed objects is achieved by management solution for NIPS. It performs policy checks during policy installation to find shadow object. **Hence request to modify this clause as below -** The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.	The proposed NIPS appliance/solutions should have a capability to identify shadow objects so that corrective actions can be taken.
549	54/178	Annexure 12 Section B Point 19	NIPS: Scope of Work	The proposed NIPS appliance/solutions should provide integration support with Sandboxing solution for in-depth static code analysis, dynamic analysis (malware sandboxing) and machine learning to detect zero-day threats, including threats that use evasion techniques and ransomware.	Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR. If yes, should we consider an HA for the same?	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
550	54/178	Annexure 12 Section B Point 28	NIPS: Scope of Work	The proposed NIPS appliance/solutions should have dedicated emulation engine.	A dedicated emulation engine requires a dedicated appliance for Sandboxing. Please let us know if dedicated on-prem Sandbox appliance needs to be proposed in DC and DR.	On-prem sandboxing appliance one each at DC and DR with required hardware, software and licenses included to be considered from Day-1. Sandbox appliance should support minimum 8 simultaneous file scan.
551	54/178	Annexure 12 Section B Point 31	NIPS: Scope of Work	The proposed appliance/solutions should have integrated Emulation - GAM (Browser) on appliance itself.	Please provide more details on Integrated emulation - GAM (browser) on appliance, the exact requirement and use-case.	The proposed appliance/solutions should have integrated Emulation - on appliance itself.
552	56/178	Point 8 section A	General Requirement	The proposed Firewall hardware/solution should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats	~~Every vendor has proprietary Hardware / Software~~ architecture to deliver the high scale of performance required in today's demanding environment. ASIC based architecture is not specific to just firewall but also adopted in routers, switches etc. Fortinet has deicated ASIC based architecture which helps deliver higher throughput by offloading specific tasks to the ASIC. Also with regards to the Bank last RFP BID NO: GEM/2023/B/3471981 Dated 22nd May, 2023 Addendum dated 1st July 2023, the same clause has been deleted in the addendum. **Hence Request you to please delete this clause or amend the clause as** " The device should support multi-~~core architecture~~"	The proposed Firewall hardware/solution should ~~not be proprietary ASIC based in nature & should be open architecture~~ based on multi-core CPU's to protect & scale against dynamic latest security threats
553	94	Point 9 Section B	System Hardware and Interface Requirement	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10/25 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 4x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 8x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance in the proposed NIPS hardware/appliance/solution should have at least 4x40/100 GE Fiber, 8x10 GE Fiber.. All ports should be populated with required transceivers. The networks switches supports 10Gb/25Gb/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,8 nos-10G. BIDI multimode transceiver.
554	70/178 & 90/178 & 111/178 &131/178	Technical Specifications of Active Components	Service/Support and Training	The proposed Firewall hardware/appliance/solution should be under 4 Hrs CTR support.	Bidder requests to change from 4 hr CTR to 6 hr CTR .OEM RMA timelines are at the lowest 4 hours/5 hours and hence CTR requires min 6 hours	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
555	74,75	1	C:- Performance Requirement	The proposed NIPS hardware/appliance/solutions IPS Inspection throughput (HTTP Based) should have minimum 60 Gbps	Request Bank to change the specification as suggested to ensure performance gurantee of device & current specs seems to be particular OEM proprietory specs.**"The proposed NIPS hardware/appliance/solutions IPS 60 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and notVideo/JPEG based traffic) (enterprise testing condition). The throughput must remain 60 Gbps even after enabling Threat Prevention + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)-**	As per RFP
556	74,75	1	C:- Performance Requirement	The proposed NIPS hardware/appliance/solutions IPS Inspection throughput (HTTP Based) should have minimum 60 Gbps	Request Bank to change the specification as suggested to ensure performance guarantee of device & current specs seems to be particular OEM proprietary specs. **"The proposed NIPS hardware/appliance/solutions IPS 60 Gbps of Threat prevention throughput with Real world traffic. (Throughput must be derived from Appmix traffic and not Video/JPEG based traffic) (enterprise testing condition). The throughput must remain 60 Gbps even after enabling Threat Prevention + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available The Test methodology and result should be compliant to the benchmark testing methodology for the above parameters provided in the Internet Engineering Task Force (IETF)-** **Explanation :- T**his modification is required to ensure the Bank doesn't run into PERFORMANCE issues with the NIPS in future after enabling various SECURITY functions/features & it will also provode written confimation/certification proof from OEM thus reducing the future Risks to the Bank.	As per RFP
557	58/178	Point 12 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
558	75/178;95/178;115/178	Point 6 Section C	Performance Requirement	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	All services (IPS, AV/AMP etc) latency numbers are not published in datasheet by any OEM because it is hard to replicate real-world traffic numbers in different customer environments with variable parameters like, packet size, security policies, traffic type, services enabled - IPS, AV, SSL etc. Making it difficult to calculate latency number in the appliance. Generally latency numbers are published for firewall only. **Hence request you to amend this clause as below -** Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection	Proposed appliance should be able to cater to the throughput requirement provided in RFP without any performance impact or delay in traffic processing and security inspection
559	81/178;101/178;121/178	Section E Point 32	Detection and Prevention Requirement	In the proposed NIPS hardware/appliance/solution Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.	Please provide more clarity on customization of vendor provided rules. IPS can provide capability for creating custom signatures.	In the proposed NIPS hardware/appliance/solution Detection signatures should be based on an extensible, open language that enables users to create their own signatures, as well as to customize any vendor-provided signatures.
560	87/178;107/178;127/178	Point 31 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The proposed NIPS hardware/solution should have dedicated Centralized Logging & Report server with below logging capabilities a. Comprehensive event logging b. Historical Reporting c. Report generation with emailing capability d. Syslog e. SNMP v2 & v3 f. Real Time Monitor g. E-mail Notification h. GUI based interface i. Command Line Interface (SSH) j. Unused Rules k. Obsolete IP addresses etc. All the logs shall be stored for 90 days with all features and policies enabled. The sizing of the disk space has to be done accordingly.	To determine the log storage requirement, we need to know the logs getting generated per day. Which depends on the number of policies, concurrent users and features enabled (IPS,URL filter, etc.) Hence we need to know the following details to size the storage: - - Log rate per second - Log generation in mb/sec	Log rate/sec: 2500 events/sec Log size mb/sec: 100 mb/sec
561	87/178;108/178;128/178	Point 34 Section G	Administration, Management, Centralised Logging and Reporting Feature Requirement	The management software for the proposed NIPS hardware/solution should integrate with EMS (Micro focus) product suite or any third party Tool	Please provide more details on Micro focus integration use-case requirement.	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.
562	74/178	Point 9 Section B	Networking , System and Performance Requirements:	Each Appliance of the proposed Firewall hardware/solution should have at least 8x40G/100G QSFP fiber, 16x10G/25G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities	**Please confirm transceivers requirement as below: -** 1) 8x40G/100G QSFP fiber: - Which transceiver should be considered 40G or 100G? 2) 16x10G/25G SFP/SFP+ fiber: - Which transceiver should be considered 10G or 25G? Also, please confirm if the transceivers type at switch end is BIDI or normal and if it is requirement for single mode or multimode transceiver.	Each Appliance of the proposed Firewall hardware/solution should have at least 4x40G/100G QSFP fiber, 20x10G SFP/SFP+ fiber. The networks switches supports 10G/25G/40Gb/100Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored. All ports should be populated with required transceivers. Apart from above each appliance should have additional ports for sync, HA and other functionalities. Bidder has to supply SFPs as under: 4 nos-100G, 2 Nos-40G,20nos-10G. BIDI multimode transceiver.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
563	32	D Experience & Support Infrastructure (Point 3)	Eligibility Criteria	The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	Request you to please remove having network of minimum 1000 domestice branches clause as mostly Banks have 1000 domestices branches. Financials institutions / Government orginization / Telecom sectors dosent have this scale of Branches.	Pls refer addendum
564			General	We request to add technical specifications for a dedicated NIPS solutions	The proposed IPS solution should be able automatically/manually be able to consume Vulnerability reports like Qualys , Nessus,Rapid7,nexpose etc. for building & fine tuning the Profile	As per RFP
565			General	We request to add technical specifications for a dedicated NIPS solutions	The IPS vendor must provide 'the acknowledgement' data from the Microsoft security bulletin over the last 3 years to ensure that IPS vendor be the leader in the discovery of the zero-day vulnerability in Microsoft product	As per RFP
566			General	We request to add technical specifications for a dedicated NIPS solutions	Should be based on purpose-built platform that has Field Programmable Gate Arrays (FPGAs), On-board L2 Switch and dual plane architecture for Data and control plane and NIPS should be independent standalone solution	As per RFP
567			General	We request to add technical specifications for a dedicated NIPS solutions	The proposed NIPS solution should have latency <70 microseconds and information should be publically available	As per RFP
568	32	D Experience & Support Infrastructure (Point 3)	Eligibility Criteria	The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	Request you to please remove having network of minimum 1000 domestice branches clause as mostly Banks have 1000 domestices branches. Financials institutions / Government orginization / Telecom sectors dosent have this scale of Branches.	Pls refer addendum
569		EMD	General	EMD amount requested of Rs. 1.2 Cr	Rs. 1.2 Cr is significantly high amount. Kindly request the bank the limit the EMD amount upto 1% of bank's estimated value of RFP as per industry standard, **Also Since we have turnover more than 500 cr , hence EMD fee will be not apllicable**	No Change
570		Technical Proposal Attention Items (Point 16J)	General	As the contract is on Turnkey solution basis, any other miscellaneous requirements related to the scope described in the RFP or extra work required to be perform due to existing structure limitation shall be provided by the successful bidder even if those items are not mentioned explicitly in this RFP.	Requesting bank to relax this clause as any existing structure limitation from banks side will not be covered as part if this RFP by the bidder.	No Change
571			General		Requesting bank to provide details of existing OEM solution used by bank with which proposed solution is required to be integrated -SIEM -PIM -NAC/IDAM, SAML and TACACS+/AAA -SNMP,Syslog -Any other security solution with which integration	Details will be provided to successful bidder.
572			General		Kindly confirm if Management server for proposed OEM are required in HA setup at DC & HA setup in DR for Firewall & NIPS.	As per RFP
573	157	Annexure 20 – Declaration regarding Local Content (LC) for Telecom Product, Services or Works	General		Since the RFP is for procuring security products-NGFW and NIPS and not Telecom Product ,request the bank to remove this annexure.	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
574	158	Annexure 21 – Certificate of Local Content	general		Request you to exempt the submission of the letter or allow the Bidder/OEM to submit the same in their own format	No Change
575	32	D Experience & Support Infrastructure (Point 3)	Eligibility Criteria	The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	Request you to please remove having network of minimum 1000 domestice branches clause as mostly Banks have 1000 domestices branches. Financials institutions / Government orginization / Telecom sectors dosent have this scale of Branches.	Pls refer addendum
576			New Query		Bidder requests bank to share the OEM make of the current Firewall and NIPS for Internet and Partner network in both DC and DR so as to enable us to quote the right solution	Details will be shared later with L1 bidder
577			General	We request to add technical specifications for a dedicated NIPS solutions	The proposed IPS solution should be able automatically/manually be able to consume Vulnerability reports like Qualys , Nessus,Rapid7,nexpose etc. for building & fine tuning the Profile	As per RFP
578			General	We request to add technical specifications for a dedicated NIPS solutions	The IPS vendor must provide 'the acknowledgement' data from the Microsoft security bulletin over the last 3 years to ensure that IPS vendor be the leader in the discovery of the zero-day vulnerability in Microsoft product	As per RFP
579			General	We request to add technical specifications for a dedicated NIPS solutions	Should be based on purpose-built platform that has Field Programmable Gate Arrays (FPGAs), On-board L2 Switch and dual plane architecture for Data and control plane and NIPS should be independent standalone solution	As per RFP
580			General	We request to add technical specifications for a dedicated NIPS solutions	The proposed NIPS solution should have latency <70 microseconds and information should be publically available	As per RFP
581			General	We request to add technical specifications for a dedicated NIPS solutions	The proposed IPS solution should be able automatically/manually be able to consume Vulnerability reports like Qualys , Nessus,Rapid7,nexpose etc. for building & fine tuning the Profile	As per RFP
582			General	We request to add technical specifications for a dedicated NIPS solutions	The IPS vendor must provide 'the acknowledgement' data from the Microsoft security bulletin over the last 3 years to ensure that IPS vendor be the leader in the discovery of the zero-day vulnerability in Microsoft product	As per RFP
583			General	We request to add technical specifications for a dedicated NIPS solutions	Should be based on purpose-built platform that has Field Programmable Gate Arrays (FPGAs), On-board L2 Switch and dual plane architecture for Data and control plane and NIPS should be independent standalone solution	As per RFP
584			General	We request to add technical specifications for a dedicated NIPS solutions	The proposed NIPS solution should have latency <70 microseconds and information should be publically available	As per RFP
585	32	D Experience & Support Infrastructure (Point 3)	Eligibility Criteria	The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	Request you to please remove having network of minimum 1000 domestice branches clause as mostly Banks have 1000 domestices branches. Financials institutions / Government orginization / Telecom sectors dosent have this scale of Branches.	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
586	32	D Experience & Support Infrastructure (Point 3)	Eligibility Criteria	The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	Request you to please remove having network of minimum 1000 domestice branches clause as mostly Banks have 1000 domestices branches. Financials institutions / Government orginization / Telecom sectors dosent have this scale of Branches.	Pls refer addendum
587	32	D Experience & Support Infrastructure (Point 3)	Eligibility Criteria	The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	Since the bank has allowed Banks/Financial Institutions/Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India however its only certain Banks which have 1000+ branches and others i,e,Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector do not have such scale. We hereby request you to please remove having network of minimum 1000 domestice branches	Pls refer addendum
588			General	We request to add technical specifications for a dedicated NIPS solutions	The proposed IPS solution should be able automatically/manually be able to consume Vulnerability reports like Qualys , Nessus,Rapid7,nexpose etc. for building & fine tuning the Profile	As per RFP
589			General	We request to add technical specifications for a dedicated NIPS solutions	The IPS vendor must provide 'the acknowledgement' data from the Microsoft security bulletin over the last 3 years to ensure that IPS vendor be the leader in the discovery of the zero-day vulnerability in Microsoft product	As per RFP
590			General	We request to add technical specifications for a dedicated NIPS solutions	Should be based on purpose-built platform that has Field Programmable Gate Arrays (FPGAs), On-board L2 Switch and dual plane architecture for Data and control plane and NIPS should be independent standalone solution	As per RFP
591			General	We request to add technical specifications for a dedicated NIPS solutions	The proposed NIPS solution should have latency <70 microseconds and information should be publically available	As per RFP
592	140	Delivery (Point 18)	Annexure 12 – Project Details Scope of Work		Delivery & Installation 8 Weeks needs to be extended	Pls refer addendum
593			General	We request to add technical specifications for a dedicated NIPS solutions	The proposed IPS solution should be able automatically/manually be able to consume Vulnerability reports like Qualys , Nessus,Rapid7,nexpose etc. for building & fine tuning the Profile	As per RFP
594			General	We request to add technical specifications for a dedicated NIPS solutions	The IPS vendor must provide 'the acknowledgement' data from the Microsoft security bulletin over the last 3 years to ensure that IPS vendor be the leader in the discovery of the zero-day vulnerability in Microsoft product	As per RFP
595			General	We request to add technical specifications for a dedicated NIPS solutions	Should be based on purpose-built platform that has Field Programmable Gate Arrays (FPGAs), On-board L2 Switch and dual plane architecture for Data and control plane and NIPS should be independent standalone solution	As per RFP
596			General	We request to add technical specifications for a dedicated NIPS solutions	The proposed NIPS solution should have latency <70 microseconds and information should be publically available	As per RFP
597	32	D Experience & Support Infrastructure (Point 3)	Eligibility Criteria	The bidder must have experience in delivery, installation & Support for Network Infrastructure (Firewall / NIPS / Router of the same OEM whose products are quoted under this RFP) of TIER –III Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least Two large banks with turnover of above Rs. 2 lakh crore / Financial Institutions / Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India having network of minimum 1000 domestic branches	Request you to please remove having network of minimum 1000 domestic branches clause as mostly Banks have 1000 domestics branches. Financials institutions / Government organization / Telecom sectors doesn't have this scale of Branches.	Pls refer addendum

बैंक ऑफ़ बड़ौदा
Bank of Baroda

S No	Page #	Point / Section #	Category (Eligibility/Scope/Commercial/Legal/General)	Clauses mentioned in RFP Document	Comment/Suggestions (From Vendors)	Bank's Clarifications to the bidder query
598			General	We request to add technical specifications for a dedicated NIPS solutions	The proposed IPS solution should be able automatically/manually be able to consume Vulnerability reports like Qualys , Nessus,Rapid7,nexpose etc. for building & fine tuning the Profile	As per RFP
599			General	We request to add technical specifications for a dedicated NIPS solutions	The IPS vendor must provide 'the acknowledgement' data from the Microsoft security bulletin over the last 3 years to ensure that IPS vendor be the leader in the discovery of the zero-day vulnerability in Microsoft product	As per RFP
600			General	We request to add technical specifications for a dedicated NIPS solutions	Should be based on purpose-built platform that has Field Programmable Gate Arrays (FPGAs), On-board L2 Switch and dual plane architecture for Data and control plane and NIPS should be independent standalone solution	As per RFP
601			General	We request to add technical specifications for a dedicated NIPS solutions	The proposed NIPS solution should have latency <70 microseconds and information should be publically available	As per RFP
602			General	We request to add technical specifications for a dedicated NIPS solutions	The proposed IPS solution should be able automatically/manually be able to consume Vulnerability reports like Qualys , Nessus,Rapid7,nexpose etc. for building & fine tuning the Profile	As per RFP
603			General	We request to add technical specifications for a dedicated NIPS solutions	The IPS vendor must provide 'the acknowledgement' data from the Microsoft security bulletin over the last 3 years to ensure that IPS vendor be the leader in the discovery of the zero-day vulnerability in Microsoft product	As per RFP
604			General	We request to add technical specifications for a dedicated NIPS solutions	Should be based on purpose-built platform that has Field Programmable Gate Arrays (FPGAs), On-board L2 Switch and dual plane architecture for Data and control plane and NIPS should be independent standalone solution	As per RFP
605			General	We request to add technical specifications for a dedicated NIPS solutions	The proposed NIPS solution should have latency <70 microseconds and information should be publically available	As per RFP