[A] Important Dates:

Sr. No.	RFP / Bid	Timeline
1	Last Date of Submission of RFP Response (Closing Date)	**17th May 2024 at 04:00 PM**
2	Eligibility Cum Technical Bid Opening Date	**17th May 2024 at 04:30 PM**

Addendum to following Annexure:

1. Annexure 02 – Bid Evaluation Terms (Eligibility Criteria)
2. Delivery – section 6
3. Annexure 20 – Local Content (LC) for Telecom Product, Services or Works
4. Masked & Commercial Bid – Point i
5. Technical Specifications – Annexure 12 (Scope)

Clarification of Pre-bid queries is enclosed as "Annexure A"

All other Terms & Conditions are the same as per our RFP for Supply, Installation and Maintenance of Firewall and NIPS (Bid Number: GEM/2023/B/4772658 dated 13th March 2024).

S No	Existing Clause	Modifications / Relaxation
1	**B-2 Below clause Applicable for the Bidder if submitting bid as a partner of the OEM:** …….. …….. 1. 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. …….. ……..	**B-2 Below clause Applicable for the Bidder if submitting bid as a partner of the OEM** …….. …….. 1. The bidder must have registered average annual turnover of **Rs. 100 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. …….. ……..
2	**C Others:** …….. …….. 2. 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). …….. ……..	No Change
3	**C Others:** …….. …….. 3. 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 …….. ……..	No Change

4	**D. Experience & Support Infrastructure:** …….. …….. 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. …….. ……..	**D. Experience & Support Infrastructure:** …….. …….. The bidder should have successfully delivered & installed minimum -02- numbers of firewall and -02- nos. of NIPS 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 in India during last -6- Years (as on RFP date). …….. ……..
5	**D. Experience & Support Infrastructure:** …….. …….. 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. …….. ……..	**D. Experience & Support Infrastructure:** …….. …….. The bidder must have experience in Support for Firewall / NIPS of Data Centre /or Disaster Recovery Centre for a period of last -5- Years (as on RFP date) in at least One large bank(s) / Financial Institutions /Government Organizations/ Public Sector Undertakings (PSUs) / Telecom Sector in India. …….. ……..

6	**D. Experience & Support Infrastructure:** …….. …….. 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. …….. ……..	**D. Experience & Support Infrastructure:** …….. …….. The bidder should have direct support offices in Mumbai and Hyderabad and technically qualified engineers who have expertise in support and installation of the proposed product. In case bidder does not have office in either Mumbai or Hyderabad then they must submit a declaration for opening the office in these cities within 30 days of the PO date. …….. ……..
7	…….. …….. **18. Delivery** 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. …….. ……..	…….. …….. **18. Delivery** 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. 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 @ **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. …….. ……..
8	…….. …….. Annexure 20 – Declaration regarding Local Content (LC) for Telecom Product, Services or Works …….. ……..	**Annexure stands deleted**

9	**Masked / 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. …….. ……..	**Masked / Commercial Bid:** …….. …….. I. In the case of additional requirements desired by the Bank, the Bank can place the order for additional 25% of the over and above the quantity for which Order is placed with a selected bidder **during the warranty period of 3 years.** …….. ……..

1. Technical Specifications of Active Components:

The proposed product/appliance should comply with the technical specifications requirement as mentioned under:

1. Firewall (Mumbai - 2, Hyderabad – 2)	
Make _____	**Model** _____
[Any Make other than Checkpoint & Cisco]	

S/N	Required Minimum Specifications (Per Device)	Bidder's compliance (Yes / No)	If yes, detail description how the solution /component would be compliant
A	**General Requirements**		
1	The proposed Firewall hardware/solution must be appliance based and should facilitate multi-application environment which should support current network traffic as well as future growth		
2	The proposed Firewall hardware/solution platform should be based on security-hardened, purpose built operating system architecture that is optimized for packet and application level content processing.		
3	The proposed Firewall hardware/solution should prevent inheriting common OS vulnerabilities and should be resided on flash disk/Hard disk/SSD.		
4	The proposed Firewall hardware/solution should provide a Http, Https, SSH, Telnet, SNMP based management console for managing and configuring various components of the appliance.		
5	The proposed Firewall hardware/solution should be able to facilitate administration audit by logging detailed activities to event log for management, configuration changes, updates which also enable Admin to boot firmware on the earlier revision / configuration in case of any errors		
6	The proposed Firewall hardware/solution administrator authentication should be facilitated by local database, PKI & remote server such as Radius, LDAP, AD, SAML and TACACS+/AAA etc servers. It should have the ability to dynamically fall back to the local user database in case of external/remote LDAP, AD, SAML and TACACS+/AAA etc Server outages.		
7	The proposed Firewall hardware/solution system should have provision of Web Content Filter, Application Control, Antivirus systems and Intrusion Prevention in the same solution		

8	The proposed Firewall hardware/solution should based on multi-core CPU's to protect & scale against dynamic latest security threats		
9	The proposed Firewall hardware/solution should be able detect & prevent the Bot communication with command and control centre of attacker.		
10	The proposed Firewall hardware/solution should have a Multi-tier engine to i.e. detect & prevent command and control centre of attacker IP/URL and DNS.		
11	The Proposed Firewall hardware/solution should have a Unified Policy Frame work for application, user, data awareness etc. in a single rule.		
12	The communication between all the components of the proposed Firewall hardware/solution system (firewall module, logging & policy management server, and the GUI/WEBUI Console etc.) should be encrypted with SSL or PKI.		
13	The proposed firewall hardware/solution should be integrated with privileged identity management (PIM) & Security Incident & Event Management (SIEM) solutions.		
B	**Networking , System and Performance Requirements:**		
1	The proposed Firewall hardware/solution should have IPSec functionality and should have integrated solution for IPSec.		
2	The proposed Firewall hardware/solution framework should have IPsec VPN (site to site VPN) functionalities for secure remote access to corporate application over internet.		
3	The proposed Firewall hardware/solution IPSec VPN should support the Authentication Header / ESP Protocols.		
4	The proposed Firewall hardware/solution IPsec ISAKMP methods should support Diffie-Hellman Group 1,2,5,14 & 19 , MD5 & SHA Hash, RSA & Manual Key Exchange Authentication, 3 DES/AES-256 Encryption of the Key Exchange Material and algorithms like RSA-1024 /2048 or latest methods & algorithms as per industry standards.		
5	The proposed Firewall hardware/solution should support ipv6 NAT functionality NAT64 & NAT46 and should be configurable as 1:1, 1: many, many: 1, many: many, flexible NAT (overlapping IPs), Reverse NAT, PAT with Masquerading supported		

6	The proposed Firewall hardware/solution should have Hardware Sensor for Monitoring capabilities.		
7	The proposed Firewall hardware/solution should support minimum 60 Gbps of production performance (http based) / multiprotocol combined, Firewall & IPS throughput.		
8	The proposed Firewall hardware/solution should support minimum 40 Million concurrent sessions with application visibility.		
9	The proposed Firewall hardware/solution should support minimum 0.4 Million new connections per second.		
10	The proposed Firewall hardware/solution should support Static, Policy Base, Identity based, Multicast routing and Dynamic routing for RIP1 & 2, OSPF, OSPFv3, BGP4, RIPing or equivalnts.		
11	The proposed Firewall hardware/solution should support Static, Policy Based, and Multicast routing or equivalents.		
12	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.		
13	Each Appliance of the proposed Firewall hardware/solution should have following interface apart from ports mentioned above a. OOB Port for management of Device or Console Ports b. USB Ports c. Console Port etc.		
14	Each Appliance of the proposed Firewall hardware/solution should be capable of handling existing and future security policies/rules.		
15	The proposed Firewall hardware/appliance/solution should support minimum 4096 VLAN tagging (IEEE 802.1q)		
16	The proposed Firewall 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.		
17	The proposed Firewall hardware/solution should not limit on assigning CPU & memory to the OS for better performance		
18	The Warranty and AMC should include all the components supplied as part of the Proposed Firewall hardware/appliance/solution. including trans receivers, breakout cables etc.		
C	**Firewall Requirements**		
1	The proposed Firewall hardware/solution should support deployment modes as; “Route Mode” or “Transparent Mode”.		
2	The proposed Firewall hardware/solution shall be able to handle VoIP traffic securely with “pinhole opening” and support SIP, SCCP, MGCP and H.323 ALGs or equivalents		
3	The proposed Firewall hardware/solution should support Stateful inspection with optional Policy based NAT (Static OR Dynamic).		
4	The proposed Firewall hardware/solution should support Inbound Port Forwarding with inbound Load Balancing		
5	The proposed Firewall hardware/solution Should support Ipv6 ACL to implement security Policy for Ipv6 traffic		
6	The proposed Firewall hardware/solution should be supported for filtering all internet based applications like Telnet, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, BGP, IMAP, NFS etc or equivalents.		
7	The proposed Firewall hardware/solution should be able to inspect HTTP and FTP traffic when these are deployed using nonstandard port(i.e when HTTP is not using standard port TCP/80)		
8	The proposed Firewall hardware/solution should provide out of box Categories based on Application types, Security Risk level etc.		
9	The proposed Firewall hardware/solution should be able to filter traffic even if the packets are fragmented.		
10	The proposed Firewall hardware/solution must support custom granular reporting, event management & dashboard for events on it.		
11	The proposed Firewall hardware/solution should support application detection and usage control.		

12	The proposed Firewall hardware/solution should provide clear indications that highlight regulations with serious indications of potential breaches with respect to access policies intrusion, malwares, BOT, URL, Applications etc.		
13	The proposed Firewall hardware/solution should have capability to define time based rules/policy.		
14	The proposed firewall should support capability to configure correlation rule where multiple rules/events can be combined together for better efficacy.		
15	The proposed firewall should support capability to identify asymmetric routing.		
16	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.)		
D	**Network Intrusion Detection & Prevention System Requirements:**		
1	The proposed Firewall hardware/solution should have a built-in Signature and Anomaly based IPS engine on the same unit and Anomaly based detection should be based on thresholds		
2	The proposed Firewall hardware/solution should provide Ipv4 and Ipv6 rate-based DOS protection with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding (source/destination) etc..		
3	The proposed Firewall hardware/solution Administrator should be able to configure DoS policies that are used to associate DoS settings with traffic that reaches an interface based on defined services, source and destinations IP/Range		

4	The proposed Firewall hardware/solution should have configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types.		
5	The proposed Firewall hardware/solution security check updates do not require reboot of the unit		
6	The proposed Firewall hardware/solution should supports attack recognition inside Ipv6 encapsulated packets		
7	The proposed Firewall hardware/solution should support all existing signatures by default and all future signature released from time to time with Regular Expressions		
9	The IPS signature updates and intelligence database update on The proposed Firewall hardware/solution should be automatic without any reboot on the appliance.		
10	The proposed Firewall hardware/solution should support the filtering of TCP/IP based applications with standard TCP/UDP ports or deployed with customs ports		
11	The proposed Firewall hardware/solution must provide state engine support for all common protocols of the TCP/IP stack		
12	The proposed Firewall hardware/solution must provide filtering capability that includes parameters like source addresses, destination addresses, source and destination port numbers, protocol type		
13	Application Control Databases of the proposed Firewall hardware/solution should have sizable application and widget control list.		
14	The proposed Firewall hardware/solution should be able to detect & Prevent Unique communication patterns used by BOTs i.e. Information about Botnet family		
15	The proposed Firewall hardware/solution should be able to detect & Prevent attack types such as spam sending click fraud or self-distribution, that are associated with Bots		
16	The proposed Firewall hardware/solution should have an option of configuring file type recognition along with following actions i.e. Scan, Block, Pass on detecting the Known Malware		
17	The Malware prevention engine of the proposed Firewall hardware/solution should be able to detect & prevent the Spyware, Ransomware & Adware for pattern based blocking at the gateways.		

18	The proposed Firewall hardware/solution should be able to discover the Bot infected machine		
19	The proposed Firewall hardware/solution should be able to provide with Forensic tools which give details like Infected Users/Device, Malware type, Malware action etc.		
20	The proposed firewall hardware/solution Anti-virus scanning should support proactive and stream mode or equivalent		
21	The proposed Firewall hardware/solution should be able to create a protection scope for the inspection		
22	The proposed Firewall hardware/solution should have an option of configuring Exception		
23	In the proposed Firewall hardware/solution Anti-spyware for pattern based blocking at the gateway		
24	In the proposed Firewall hardware/solution known Malware scanning should not be restricted by the any specific limit on the size of the of the file(s)		
25	The proposed Firewall hardware/solution should have configurable option to inspect, bypass or blocked various file-types as per organization need.		
26	The Malware scanning should be performed by the proposed Firewall hardware/solution for the traffic flows with the protocols for HTTP, HTTPS, FTP, POP3,& SMTP etc.		
27	The proposed Firewall hardware/solution should prevent the users to access the malware hosting websites and/or web resources		
28	The proposed Firewall hardware/solution with Malware & Bot Prevention engines should be supplied with the readily available support for the ingestion of threat intelligence feeds in a common threat language called as STIX (Structured Threat Information expression) or any other internationally supported format		
29	The proposed Firewall hardware/solution with Malware & Bot Prevention engines should be supplied with the readily available support for the ingestion of threat intelligence feeds from other security & SIEM solution deployed at bank's data centre.		
30	The proposed Firewall hardware/solution should support for detection of reconnaissance attempts such as IP address sweep, port scanning etc.		

31	The proposed Firewall hardware/solution should have Multi-Layer Threat Prevention suite with following or any latest industry standard prevention suits controllers embedded. a. Prevention against Malware b. Prevention against Bot & Botnets. c. Prevention against malware hosting, URL, prevention against risky web2.0 apps d. Widgets like anonymizers, TOR, P2P, Bit Torrents, etc.		
E	**URL Filtering**		
1	The proposed Firewall hardware/solution should be able to create policy based on URLs specifying in the rules.		
2	The proposed Firewall hardware/solution should be able to define URL category based on Risk level.		
F	**Application Visibility and Awareness**		
1	The proposed Firewall hardware/solution should support Identity based controls for Granular user, group and machine based visibility and policy enforcement.		
2	The proposed Firewall hardware/solution should support the Identity based logging, application detection and usage controls		
3	The proposed Firewall hardware/solution should enable securities policies to identify, allow, block or limit application regardless of port, protocol etc.		
4	The proposed Firewall hardware/solution should have Categories like Business Applications, IM, File Storage and Sharing, Mobile Software, Remote Administration, SMS Tools, Search Engine, Virtual Worlds, Webmail etc.		
5	The proposed Firewall hardware/solution must delineate specific instances of peer2peer traffic (Bit torrent, emule, neonet, etc.), messaging (AIM, YIM, Facebook Chat, etc.) & Proxies (ultrasurf, ghostsurf, freegate, etc.).		
6	The proposed Firewall hardware/solution must delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability etc.		
7	In the proposed Firewall hardware/solution Identity Access should be able to distinguish between employee and other like guests and contractors.		

8	The proposed Firewall hardware/solution should have provide out of box Categories based on Application types, Security Risk level etc. Should include filtering of application names based on Application types, Security Risk level etc.		
9	The proposed Firewall hardware/solution Application Control Library should covering most of the Web 2.0 or higher application signatures		
G	**High Availability Requirements:**		
1	The proposed Firewall hardware/solution HA solution should support state full session maintenance in the event of a fail-over to a standby unit/s. The failover between modes must be without any manual intervention, completely transparent to the user and application traffic without session drops. It must synchronize the Sessions, Decryption Certificate, Threat and Application Signature etc. ensuring seamless operations		
2	The proposed Firewall hardware/solution HA solution should support both Active/Active and Active/Passive load balancing with state full failover for both firewall & VPN features.		
3	The proposed Firewall hardware/solution High Availability should be supported in the Firewall from the day one and without any extra license		
4	The proposed Firewall hardware/solution upgrade of HA pair should be seamless without any downtime.		
5	The proposed Firewall hardware/solution HA solution deployed should support hitless upgrade for both Major and Minor codes		
6	The proposed Firewall hardware/solution must be capable to detect device, link and path failure		
7	Dual (redundant) AC power supply with Indian standard compatible power cords as well as C19-C20 or C13-C14 Power cord.		
8	Hot Swapability:- The proposed Firewall hardware must have redundant and Hot swappable power supply and Redundant fan.		
9	The proposed Firewall hardware appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades. Firewall Appliance should have on-box storage capacity for OS images & log storage		
10	The proposed Firewall hardware/solution should support minimum 2X400 GB HDD/SSD from day 1		

11	The proposed firewall hardware/solution should be rack mountable and supplied with rack mounting kit along with support side rails		
12	The proposed Firewall hardware/solution offered product part codes have to be General Availability Part codes and not custom built. There should be reference of Products to the public website of the OEM.		
H	**Administration, Management , Centralized Logging & Reporting**		
1	In the proposed Firewall hardware/solution Management Should support automation & Orchestration using Open REST API Support.		
2	Firewall Management system should provide the real time health status of all the proposed Firewall hardware/solution modules on the dashboard for CPU & memory utilization, state table, total # of concurrent connections, the connections/second counter, interface usage, application usage, VLAN usage and the amount of traffic traversing through firewall.		
3	The proposed Firewall hardware/solution should support creation of Unified Policy in Single Dashboard. Policy creation for Access Controls including Application Identification, User Identification, Host and Threat Prevention within same dashboard window.		
4	The proposed Firewall hardware/solution should be able to able to provide auditing view/ report for Firewall Policy/Rule/Objects Modifications, Addition, Deletion or other network changes.		
5	Local access to the proposed Firewall hardware/solution modules should support role based access		
6	The proposed Firewall hardware/solution must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes.		
7	The proposed Firewall hardware/solution administration station must provide a means for exporting the firewall rules set and configuration in readable format preferably in CSV, Excel and XML.		
8	In the proposed Firewall hardware/solution Role based administration with multiple administrators & Separation of duties should be supported. Configurations conflict should be avoided when multiple administrators works together.		

9	In the proposed Firewall hardware/solution Management should provide role based access on policy configuration to cater separation of duties.		
10	In the proposed Firewall hardware/solution Management should have log indexing capability for faster log search & log optimization.		
11	The proposed Firewall hardware/solution Management software must provide a means of viewing, filtering and managing the log data.		
12	The proposed Firewall hardware/solution logs must contain information about the firewall policy rule that triggered the log.		
13	The proposed Firewall hardware/solution should support for taking immediate action within logging pane in case of any critical DOS, Threat attempt		
14	The proposed Firewall hardware/solution Management should alert administrator in case if any configuration error or Misconfiguration before policy or rule deployed.		
15	The centralized management solution of the proposed Firewall hardware/solution should support integration with external/remote server such as Microsoft AD or LDAP, NAC/IDAM, SAML and TACACS+/AAA etc Server.		
16	The proposed Firewall hardware/solution should be able to ingest the Intelligence shared over STIX / TAXII / API from the SIEM solution		
17	In the proposed Firewall hardware/solution Management framework and monitoring solution should monitor compliance status of the Threat Prevention devices in the real time. It is expected, the solution to provide real-time and continuous assessment of configuration framework.		
18	The proposed Firewall hardware/solution should provide clear indications that highlight regulations with serious indications of potential breaches with respect to Access Policies, Intrusion, Malwares, BOT, URL, Applications etc.		
19	The proposed Firewall hardware/solution should indicate automatically where improvements are needed and ongoing continuous assessment rather than manual intervention for meeting up compliance.		
20	The management software of the proposed Firewall hardware/solution should support the following for rule optimization		

	a. Unused Rules Calculation for specific time-period based on Firewall Traffic Logs. b. Analysis on Covered/Shadow/Hidden Rules c. Analysis on Rules Consolidation (Merging of similar kind of rules) d. Analysis on Redundant Rules e. Tightening of Overly Permissive Rules (Any-Any) f. Analysis on Unattached/Unused Objects to simplify objects management g. Analysis on Rule-Reordering to improve the performance of the Firewall h. Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets or any other cases not defined above.		
21	All proposed Firewall hardware/solution components NGFW, Logging, Reporting etc. should be managed from centralised management framework and if not then Bidder need to provide additional components if any		
22	Bidder should include additional software and licenses for compliance feature framework and need to integrate with the management framework of the proposed Firewall hardware/solution.		
23	Detailed Event analysis for Threat Prevention Controls Anti-Malware, Anti-Bot, IPS, Application Control etc. need to be provided with Real-Time and Historical reporting all the components of the proposed Firewall hardware/solution.		
24	Centralized Management Server of the proposed Firewall hardware/solution should be deployed in VM (VM to be provided by Bank) and all necessary license should be provided from day one.		
25	Centralized Management Server of the proposed firewall hardware should be deployed in VM with HA. All necessary license should be provided by Bidder from day one.		
26	The proposed Firewall hardware/solution should not be deployed as a software for windows/Linux machine.		
27	The proposed Firewall solution Virtual OS must support VMWare ESXi 7.0 or above.		
28	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.		

29	The proposed Firewall hardware/solution must integrate with centralized logging & reporting solution of same OEM for better reporting and archival of Logs. In Case management fails to send logs , the proposed Firewall hardware should directly send the logs to SIEM and centralized logging servers.		
30	The proposed Firewall hardware/solution also should have feature to integrate with syslog & SNMP server v2c, v3 and should support SNMP TRAPS.		
31	The proposed Firewall hardware/solution management 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.		
32	The Historical Reports of the proposed Firewall hardware/solution shall be available for multiple timeframe i.e. hourly, daily, weekly, monthly as well as customized period in the solution.		
33	The proposed Firewall hardware/solution must provide granular reporting, event management & dashboard for events		
34	The proposed Firewall hardware/solution must have drill down dashboard option which can take out as PDF/Word/Excel/CSV if required.		
35	The proposed Firewall hardware/solution must support custom granular reporting, event management & dashboard for events on it.		
36	The proposed firewall hardware/solution Management should be integrated with privileged identity management (PIM) & Security Incident & Event Management (SIEM) solutions.		

I	**Licensing Requirement**		
1	The proposed Firewall hardware/solution should have enterprise license without any restrictions.		
2	The proposed Firewall hardware/solution should be on Distributed Architecture for Threat Prevention along with Dedicated Management, Logging and Reporting Framework.		
3	In the proposed Firewall hardware/solution if any third party product required to achieve the functionality should be provided with the necessary enterprise version license of software/appliance.		
4	Every Gateway Security control (like Firewall or any other feature required to meet above specification) must not have any licensing restriction on number of users and must be supplied for unlimited users unless specified otherwise.		
J	**Certification**		
1	Security effectiveness of the proposed Firewall hardware/solution should be recommended/certified by NSS / Forrester NGFW last published test report		
K	**Service ,Support & Training**		
1	The proposed Firewall hardware/appliance/solution should be under 6 Hrs CTR support.		
2	The proposed Firewall hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC)		
3	The OEM must provide 24 X 7 X 365 highest level of technical support. The Bidder Must Ensure that the dedicated login credentials to Bank with highest level permissions to search knowledge base, downloading of the patches, documents and to manage the device. Bank should be able to raise tickets directly to OEMs online submission portal for all product related issues with priority case handling.		
4	"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."		

2. NIPS Type A: (Mumbai - 2, Hyderabad - 2)			
Make _____		**Model** _____	
Sr. No.	**Required Minimum Specifications**	**Bidder's compliance (Yes / No)**	**If yes, detail description how the solution /component would be compliant**
A	**Solution Requirement**		
1	The proposed NIPS hardware/appliance/solution must have Intrusion Prevention System, Anti-Bot, Anti-Virus, Anti-Malware, Anti-Spyware, Vulnerability Protection, URL Filtering, Zero-Day or unknown threat prevention, DNS Security service functionality by default.		
2	The communication between all the components of the proposed NIPS hardware/appliance/solution (IPS module, logging & policy and Web GUI Console) should be encrypted with SSL or PKI		
3	The proposed NIPS hardware/appliance/solution should provide seamless failover among devices for all components and should be completely automatic without session disconnect.		
4	The proposed NIPS hardware/appliance/solution should provide protection against various types of cyber-attacks evasive attacks, scripting attacks etc.		
5	The proposed NIPS hardware/appliance/solution should have capability to store Logs and configuration of all devices, centrally in the solution and should also have capability to send logs of all devices to the generic central log collection & management servers.		
6	The proposed NIPS hardware/appliance/solution must support the complete STACK of IP V4 and IP V6 services		
7	The detection engine of the proposed NIPS hardware/appliance/solution should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).		
8	The proposed NIPS hardware/appliance/solution must be capable of dynamically tuning IPS sensors (Like: selecting rules/signatures,		

	configuring policies, updating policies, etc.) with minimal human intervention	
9	The proposed NIPS hardware/solution must be appliance based and should facilitate multi-application environment which should support current network traffic as well as future growth	
10	The proposed NIPS hardware/solution administrator authentication should be facilitated by local database, PKI & remote server such as Radius, LDAP, AD, SAML and TACACS+/AAA. It should have the ability to dynamically fall back to the local user database in case of external/remote Radius, LDAP, AD, SAML and TACACS+/AAA Server outages.	
B	**System Hardware and Interface Requirement**	
1	In the proposed NIPS hardware/appliance/solution all ports should be populated with required transceivers. Apart from each appliance should have additional ports for sync, HA and other functionalities.	
2	The proposed NIPS hardware/appliance/solution should have Console port.	
3	The proposed NIPS hardware/appliance/solution should have separate dedicated management 1G Ethernet interface for Out of Band Management. None of the monitoring ports should be used for this purpose.	
4	The proposed NIPS hardware/solution should be rack mountable and supplied with rack mounting kit along with support side rails.	
5	The proposed NIPS hardware/appliance/solution should have hardware health monitoring capabilities and should provide different parameters through SNMP	
6	The proposed NIPS hardware/appliance/solution should support VLAN tagging (IEEE 802.1q)	
7	The proposed NIPS hardware/appliance/solution should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy and higher throughput/Bandwidth.	
8	The proposed NIPS hardware/solution should not limit on assigning CPU & memory to the OS for better performance	
9	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.**	
10	The proposed NIPS hardware/appliance/solution should be based on multi-core cpu's to protect & scale against dynamic latest security threats	
11	The proposed NIPS hardware/appliance/solution should have minimum 2X400 GB SSD/HDD from Day 1	
12	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.	
13	The proposed NIPS hardware/appliance/solution should support VLAN tagging (IEEE 802.1q)	
14	The Warranty and AMC should include all the components supplied as part of the Proposed NIPS hardware/appliance/solution. including trans receivers, breakout cables etc.	
C	**Performance Requirement**	
1	The proposed NIPS hardware/appliance/solutions IPS Inspection throughput (HTTP Based) should have minimum 60 Gbps.	
2	The proposed NIPS hardware/appliance/solution should be running all internet protocols etc., traffic flowing through different zones with all the features enabled and running	
3	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.	
4	The proposed NIPS hardware/appliance/solution should support minimum 40 million concurrent connections	

5	The proposed NIPS hardware/appliance/solution should support minimum 0.4 million new sessions per second processing	
6	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.	
7	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.	
8	The proposed Firewall hardware/solution should supports all existing IPS attack signatures by default and all future signature released from time to time with Regular Expressions	
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.)	
10	Each Appliance of the proposed NIPS hardware/solution should be capable of handling all existing and future security policies/rules.	
D	**Feature Requirement**	
1	The proposed NIPS hardware/appliance/solution should have capability to keep track the network connections, identify the threats, detect and prevent the threat and relate the threat with corresponding end points (IP address, user, software program etc.	

2	The proposed NIPS hardware/appliance/solution should able to get enterprise visibility of internet access like URL access, Malicious website/server visits, country details etc.	
3	The proposed NIPS hardware/appliance/solution should provide segmentation and each segment can be deployed with different policy/rules based on traffic analysis of particular segment.	
4	The proposed NIPS hardware/appliance/solution should support application layer controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	
5	The proposed NIPS hardware/appliance/solution should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location.	
6	In the proposed NIPS hardware/appliance/solution the detection engine must incorporate multiple approaches for detecting threats, including a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques. Identify and explain each type of detection mechanism supported.	
7	The proposed NIPS hardware/appliance/solution should allow Custom user-defined signatures with Regular Expressions	
8	The proposed NIPS should support capability to configure correlation rule where multiple rules/events can be combined together for better efficacy.	
9	The proposed NIPS hardware/appliance/solution Should support to enable/disable each individual signature. Each signature should allow granular tuning	
E	**Detection and Prevention Requirement**	
1	The proposed NIPS hardware/appliance/solution should support different mode of deployment in following modes: a) IDS b) TAP Mode c) Inline	
2	The proposed NIPS hardware/appliance/solution should accurately detect intrusion attempts and discern between the various types and risk levels	

	including unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, hybrids, and zero-day attacks, Worm, Phishing, Spyware, Virus, Trojan, P2P, VoIP, Backdoor, Reconnaissance, Bandwidth Hijacking, Cross-site scripting, SQL Injection etc.	
3	The proposed NIPS hardware/appliance/solution should employ all seven-layer (of OSI model) protocol analysis.	
4	The proposed NIPS hardware/appliance/solution should support vulnerability based and not exploit based signatures. Detects and blocks all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability)	
5	The proposed NIPS hardware/appliance/solution should support a wide variety of techniques to perform traffic inspection including (a) TCP stream reassembly, b) Does IP defragmentation, c) Bi- directional inspection, d) Protocol Anomaly Detection, e) Protocol tunnelling, f) Signatures g) Behaviour anomaly h) Reputation	
6	The proposed NIPS hardware/appliance/solution should have the ability to identify application traversing on the network and allow or block specific application on the network.	
7	The proposed NIPS hardware/appliance/solution should support source reputation based analysis and should obtain through the cloud the reputation for each host involved in an attack and uses the reputation score of the source host as one of the factor for blocking the host	
8	The proposed NIPS hardware/appliance/solution should support malware protection by performing file reputation analysis of malicious files	
9	The proposed NIPS hardware/appliance/solution should have the ability to inspect traffic in the virtual environment and if any additional hardware are required to achieve it, should be provided	
10	The proposed NIPS hardware/appliance/solution support provide advanced botnet protection using heuristic detection methods	
11	The proposed NIPS hardware/appliance/solution should provide advanced botnet protection using multi event behaviour based detection mechanism.	

12	The proposed NIPS hardware/appliance/solution should protect against DOS/DDOS attacks.	
13	The proposed NIPS hardware/appliance/solution Should support the ability to limit the number of TCP/UDP/ICMP active connections or connection rate from a host	
14	The proposed NIPS hardware/appliance/solution should have —self-learning" capability to monitor the network traffic and develops a baseline profile or recommendations. It should have the ability to constantly update this profile or recommendations to keep an updated view of the network for each segment.	
15	The proposed NIPS hardware/appliance/solution should support active blocking of traffic based on pre-defined rules to thwart attacks before any damage is done, i.e. before compromise occurs	
16	The proposed NIPS hardware/appliance/solution should have the ability to control traffic based on geographical locations. For e.g. a policy can be created to block traffic coming or going to a particular country.	
17	The proposed NIPS hardware/appliance/solution should have the ability to block connection from outside based on the reputation of the IP address that is trying to communicate with the network	
18	The proposed NIPS hardware/solution should be able to ingest the Intelligence shared over STIX / TAXII / API from the SIEM solution	
19	The proposed NIPS hardware/appliance/solution should protect against evasion techniques	
20	The proposed NIPS hardware/appliance/solution should support a wide range of response actions as a) Block traffic, b) Ignore, c) TCP reset, e) Log traffic, f) Packet capture, g) User defined scripts, h) Email alert, i) SNMP alert, j) syslog alert etc.	
21	The proposed NIPS hardware/appliance/solution should accurately detect the following Attack categories:	

	Malformed traffic, Invalid Headers, Vulnerability exploitation, URL obfuscation, Asymmetric Traffic etc.	
22	The proposed NIPS hardware/appliance/solution must support vulnerability based and exploit based signatures. It should detect and block all known high risk exploits and the underlying vulnerability (not just one exploit of that vulnerability)	
23	The proposed NIPS hardware/appliance/solution should get Signatures, Patches & updates being received from OEM should be from trusted sites	
24	The proposed NIPS hardware/appliance/solution should handle following traffic inspection & support following: Ipv6, Ipv4, Tunnelled: 4in6, 6in4, 6to4,Bi-directional inspection, Detection of Shell Code, Buffer overflows, Advanced evasion protection Application Anomalies, P2P attacks, TCP segmentation and IP fragmentation Rate-based threats, Statistical anomalies	
25	The proposed NIPS hardware/appliance/solution should have the ability to identify/block individual applications (eg. Facebook or skype) running on one protocol (eg HTTP or HTTPs)	
26	The proposed NIPS hardware/appliance/solution should have application intelligence for commonly used TCP/IP protocols, not limited to telnet, ftp, http, https etc	
27	The proposed NIPS hardware/appliance/solution should support Block attacks based on IP reputation, DNS Inspection and Sink-Holing, Geo-location, URL Inspection / intelligence	
28	The proposed NIPS hardware/appliance/solution should have the feature for importing SNORT signatures.	
29	The proposed NIPS hardware/appliance/solution should support basic attack protection features listed below but not limited to : Maximum no of protections against attacks that exploit weaknesses in the TCP/IP protocol suite a. NIPS should enable rapid detection of network attacks b. TCP reassembly for fragmented packet protection c. SYN cookie protection, SYN Flood, Half Open Connections and NUL Packets etc.	

	d. Protection against IP spoofing e. Malformed packet protection f. Asymmetric Packet Transmission	
30	The proposed NIPS hardware/appliance/solution should be able to block Instant Messaging like Yahoo, MSN, ICQ, Skype (SSL and HTTP tunnelled) etc.	
31	The proposed NIPS hardware/appliance/solution should provide visibility into how network bandwidth is consumed to aid in troubleshooting network outages and detecting Advanced Malware related DoS & DDoS activity from within the network	
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.	
33	The proposed NIPS hardware/appliance/solution should be capable of whitelisting trusted applications from being inspected and not an entire segment to avoid business applications from being affected & in turn productivity	
F	**High Availability Requirements:**	
1	The proposed NIPS hardware/appliance/solution must support active-active OR Active-Standby High Availability. The HA should be out of the box solution and should not require any third party or additional software/hardware for the same	
2	The proposed NIPS hardware/appliance/solution should provide seamless failover among devices for all components and should be completely automatic without any sort of manual intervention	
3	The High Availability should be supported in the proposed NIPS hardware/appliance/solution from the day one and without any extra license	

4	The upgrade of HA pair in proposed NIPS hardware/appliance/solution should be seamless without any downtime	
5	The proposed NIPS hardware/appliance/solution deployed should support hitless upgrade for both Major and Minor codes in HA.	
6	All components of the proposed NIPS hardware/appliance/solution should be in HA	
7	The proposed NIPS hardware/appliance/solution must support active-active or Active-Standby High Availability without session loss. The HA should be out of the box solution and should not require any third party or additional software/hardware for the same	
8	The proposed NIPS hardware/appliance/solution should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc.	
9	In the proposed NIPS hardware/appliance/solution Centralized Management should provide high availability at site level for enabling DR deployment	
10	The proposed NIPS hardware/appliance/solution should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc. Firewall Appliance should have on-box storage capacity for OS images & log storage	
11	The proposed NIPS hardware/appliance/solution should have hot swappable redundant power supplies (Minimum dual power supply). Dual (redundant) AC power supply with Indian standard compatible power cords as well as C19-C20 or C13-C14 Power cord.	
12	The proposed Firewall hardware/solution should support minimum 2X400 GB HDD/SSD from day 1	
13	The proposed firewall hardware/solution should be rack mountable and supplied with rack mounting kit along with support side rails	
14	The proposed Firewall hardware/solution offered product part codes have to be General Availability Part codes and not custom built. There should be reference of Products to the public website of the OEM.	
G	**Administration, Management, Centralised Logging and Reporting Feature Requirement**	

1	The proposed NIPS hardware/appliance/solution should support Real-Time Monitoring, Management & Log Collection (with storage) should not be distributed to more than ONE server/appliance	
2	In the proposed NIPS hardware/appliance/solution, the centralized monitoring and management system should have multiple administrators who have administrative rights based on their roles and should keep Audit Trail of the Changes etc. performed by such administrator.	
3	In the proposed NIPS hardware/appliance/solution the secondary (SLAVE) Management Server should support the MASTER role once the Disaster recovery is triggered for any or multiple management domains in the Management Server	
4	In the proposed NIPS hardware/appliance/solution should be able to support large scale WAN deployment with following important Criteria for Real-Time Monitoring, Management & Log Collection etc. a. Any changes or commands issued by an authenticated user should be logged to a database of the management system. b. Any changes or commands issued by an authenticated user should be logged to a database of the management system	
9	The proposed NIPS hardware/solution also should have feature to integrate with syslog & SNMP server v2c, v3 or higher and should support SNMP TRAPS.	
10	The proposed NIPS hardware/appliance/solution must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes.	
11	In the proposed NIPS hardware/appliance/solution management platform must provide a highly customizable dashboard.	
12	The proposed NIPS hardware/appliance/solution must provide simplified provisioning for addition of new IPSs where by a standard IPS policy could be pushed into the new IPS.	

13	The proposed NIPS hardware/appliance/solution administration station must provide a means for exporting the IPS rules set and configuration in readable format.	
14	The proposed NIPS hardware/appliance/solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward	
15	In the proposed NIPS hardware/appliance/solution Management console should be capable of producing extensive graphics metric for analysis. Further, users should be able to drill down into these graphical reports to view pertinent details.	
16	The proposed NIPS hardware/appliance/solution should support for role based administration of IPS	
17	The proposed NIPS hardware/appliance/solution should support granular management. Should allow policy to be assigned per device, port, VLAN tag, IP address/range	
18	The proposed NIPS hardware/appliance/solution administration software must provide a means of viewing, filtering and managing the log data	
19	In the proposed NIPS hardware/appliance/solution logs must contain information about the IPS policy rule that triggered the log	
20	Centralized Security Management should include for all the proposed NIPS security controls but not limited to: a. Real Time Security Monitoring b. Logging c. Reporting functions based on 1. Security event risk level, 2. Date/time, 3. Event name 4. Source IP 5. Destination IP 6. Response Taken 7. Sensor Identity 8. Severity, etc. d. NIPS solution must provide a minimum basic statistics about the health of the IPS and the amount of traffic traversing the IPS	

	e. NIPS Solution should support for configuration rollback f. NIPS Solution should support Real time traffic statistics & Historical report with g. Attacks and threat reports, etc. h. Customized reports on HTML, CSV ,PDF, Excel and XML format etc.	
21	The proposed NIPS hardware/appliance/solution Audit Trail should contain at a minimum below information for any Policy/Rule/Objects Modifications, Addition , Deletion or other network changes but not limited to a. The name of the administrator making the change b. The change made c. Time of change made d. Comments/Remarks	
22	The proposed NIPS hardware/appliance/solution management platform must provide multiple report output types or formats, such as PDF, HTML, CSV, Excel and XML.	
23	The proposed NIPS hardware/appliance/solution management system should provide detailed Event analysis for IPS and also should provide Syslog output to integrate with other major SIEM tools and specifically should support RSA SIEM tool current and future versions	
24	The proposed NIPS hardware/appliance/solution should support for real time analysis of all traffic the IPS may encounter (all possible SOURCE, DEST, SERVICE, including groups) etc.	
25	The proposed NIPS hardware/appliance/solution should manage the NIPS appliances from a central management console	
26	The proposed NIPS hardware/appliance/solution management platform should supports policy configuration, command, control, and event management functions.	
27	The proposed NIPS hardware/solution administrator authentication of Management console should be facilitated by local database, PKI & remote server such as Radius, LDAP, AD, SAML and TACACS+/AAA. It should have the ability to dynamically fall back to the local user	

	database in case of external/remote Radius, LDAP, AD, SAML and TACACS+/AAA Server outages.	
28	The proposed NIPS hardware/appliance/solution Management console should have the ability to allow access to specific hosts by enabling GUI Access and defining the list of authorized hosts/networks	
29	In the proposed NIPS hardware/appliance/solution signature updates and intelligence database update on NIPS and should be automatic without any reboot on proposed NIPS hardware/appliance	
30	The proposed NIPS hardware/appliance/solution management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows	
31	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.	
32	In the proposed NIPS hardware/solution Historical Reports shall be available for multiple timeframe i.e. hourly, daily, weekly, monthly as well as customized period in the solution.	
33	Centralized Management Server for the proposed NIPS hardware/solution should be deployed in VM (VM to be provided by Bank) and all necessary license should be provided from day one.	
34	The management software for the proposed NIPS hardware/solution should support	

	integration with industry standard EMS tools or any third party Tool	
35	In the proposed NIPS hardware/appliance/solution Centralized Management should provide high availability at site level for enabling DR deployment	
36	It should be possible to manage the entire proposed NIPS hardware/appliance/solution from Primary & Secondary management server/appliance placed at DC and DR. Management solution should have the capability to be deployed in geographically different location enabling DR deployment	
37	The proposed NIPS hardware/appliance/solution should have adequate local storage in order to keep the various logs	
38	The proposed NIPS hardware/appliance/solution should be able to perform entire packet capture of the infected traffic and sent to the other application for analysis	
39	The management software for the proposed NIPS hardware/solution should support the following for rule optimization a. Unused Rules Calculation for specific time-period based on NIPS Traffic Logs. b. Analysis on Covered/Shadow/Hidden Rules c. Analysis on Rules Consolidation (Merging of similar kind of rules) d. Analysis on Redundant Rules e. Tightening of Overly Permissive Rules (Any-Any) f. Analysis on Unattached/Unused Objects to simplify objects management g. Analysis on Rule-Reordering to improve the performance of the NIPS h. Analysis on Disabled/Expired Rules for enhanced visibility on the NIPS Rules sets or any other cases not defined above.	
40	The proposed NIPS hardware/appliance/solution Centralized Management Server should be deployed with HA in VM (to be provided by Bank) and all necessary license should be provided from day one by Bidder.	
41	The proposed NIPS hardware/appliance/solution should be manageable from the centralized	

	management framework from DC and DR with support for managing Minimum 4 NIPS systems	
H	**Licensing Requirement**	
1	The proposed NIPS hardware/appliance/solution should have enterprise license without any restrictions.	
2	The proposed NIPS hardware/appliance/solution should be able to achieve all the features and functionalities mentioned in the RFP and accordingly, all the required licenses should be provided as part of overall solution.	
3	Every Gateway Security control (like Firewall , NIPS or any other feature required to meet above specification) must not have any licensing restriction on number of users and must be supplied for unlimited users unless specified otherwise.	
4	Any third party product required to achieve the functionality should be provided with the necessary enterprise version license of software/appliance and necessary hardware, database and other relevant software or hardware etc. should be provided with proposed NIPS hardware/appliance/solution	
I	**Other**	
1	The proposed NIPS hardware/appliance/solution should must identify network related malicious activity, log information about such activity, report it to SIEM dashboard and attempt to block or stop it.	
2	The proposed NIPS hardware/appliance/solution Should have Intrusion prevention sensors delivering context-aware, IPS device should perform state full pattern recognition to identify vulnerability-based attacks through the use of multi-packet inspection across all protocols.	
3	The proposed NIPS hardware/appliance/solution must perform protocol decoding and validation for network traffic including: IP, TCB UDP, and ICMP.	
4	The proposed NIPS hardware/appliance/solution should identify attacks based on observed deviations in the normal RFC behaviour of a protocol or service.	
5	The proposed NIPS hardware/appliance/solution should identify attacks running inside of these	

	tunnelling protocols such as GRE, IP-in-IP, MPLS, and Ipv4/Ipv6.	
6	The proposed NIPS hardware/appliance/solution should have ability to setup exceptions to filter out, fine-tune or adjust the actions for specific attacker or destination IP on a per signature basis.	
7	The proposed NIPS hardware/appliance/solution should be Capable to detect device failure link failure.	
8	The proposed NIPS hardware/appliance/solution should have an option to add exceptions for network and services.	
9	The proposed NIPS hardware/appliance/solution should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, performance impact, Release date, Industry Reference, Confidence level etc.	
10	The proposed NIPS hardware/appliance/solution should be integrated with Privileged Identity Management (PIM) & Security Incident & Event Management (SIEM) Solutions.	
11	The proposed NIPS hardware/appliance/solution should have Categories based on Application types, Security Risk level etc.	
12	If during the contract, solution is not performing as per specifications in this RFP, Bidder has to upgrade/enhance the devices or place additional devices and reconfigure the system without any cost to bank	
K	**Service, Support & Training**	
1	The proposed NIPS hardware/appliance/solution should be under 6 Hrs CTR support.	
2	The proposed NIPS hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC)	
3	The OEM must provide 24 X 7 X 365 highest level of technical support. The Bidder Must Ensure that the dedicated login credentials to Bank with highest level permissions to search knowledge base, downloading of the patches, documents and to manage the device. Bank should be able to raise tickets directly to OEMs online submission portal for all product related issues with priority case handling.	

4	"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."	

3. NIPS Type B: (Mumbai - 2, Hyderabad - 2)			
Make _____		**Model** _____	
Sr. No.	**Required Minimum Specifications**	**Bidder's compliance (Yes / No)**	**If yes, detail description how the solution /component would be compliant**
A	**Solution Requirement**		
1	The proposed NIPS hardware/appliance/solution must have Intrusion Prevention System, Anti-Bot, Anti-Virus, Anti-Malware, Anti-Spyware, Vulnerability Protection, URL Filtering, Zero-Day or unknown threat prevention, DNS Security service functionality by default.		
2	The communication between all the components of the proposed NIPS hardware/appliance/solution (IPS module, logging & policy and Web GUI Console) should be encrypted with SSL or PKI		
3	The proposed NIPS hardware/appliance/solution should provide seamless failover among devices for all components and should be completely automatic without session disconnect.		
4	The proposed NIPS hardware/appliance/solution should provide protection against various types of cyber-attacks evasive attacks, scripting attacks etc.		
5	The proposed NIPS hardware/appliance/solution should have capability to store Logs and configuration of all devices, centrally in the solution and should also have capability to send logs of all devices to the generic central log collection & management servers.		
6	The proposed NIPS hardware/appliance/solution must support the complete STACK of IP V4 and IP V6 services		
7	The detection engine of the proposed NIPS hardware/appliance/solution should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).		
8	The proposed NIPS hardware/appliance/solution must be capable of dynamically tuning IPS sensors (Like: selecting rules/signatures, configuring		

	policies, updating policies, etc.) with minimal human intervention		
9	The proposed NIPS hardware/solution must be appliance based and should facilitate multi-application environment which should support current network traffic as well as future growth		
10	The proposed NIPS hardware/solution administrator authentication should be facilitated by local database, PKI & remote server such as Radius, LDAP, AD, SAML and TACACS+/AAA. It should have the ability to dynamically fall back to the local user database in case of external/remote Radius, LDAP, AD, SAML and TACACS+/AAA Server outages.		
B	**System Hardware and Interface Requirement**		
1	In the proposed NIPS hardware/appliance/solution all ports should be populated with required transceivers. Apart from each appliance should have additional ports for sync, HA and other functionalities.		
2	The proposed NIPS hardware/appliance/solution should have Console port.		
3	The proposed NIPS hardware/appliance/solution should have separate dedicated management 1G Ethernet interface for Out of Band Management. None of the monitoring ports should be used for this purpose.		
4	The proposed NIPS hardware/solution should be rack mountable and supplied with rack mounting kit along with support side rails.		
5	The proposed NIPS hardware/appliance/solution should have hardware health monitoring capabilities and should provide different parameters through SNMP		
6	The proposed NIPS hardware/appliance/solution should support VLAN tagging (IEEE 802.1q)		
7	The proposed NIPS hardware/appliance/solution should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy and higher throughput/Bandwidth.		

8	The proposed NIPS hardware/solution should not limit on assigning CPU & memory to the OS for better performance		
9	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.		
10	The proposed NIPS hardware/appliance/solution should be based on multi-core cpu's to protect & scale against dynamic latest security threats		
11	The proposed NIPS hardware/appliance/solution should have minimum 2X400 GB SSD/HDD from Day 1		
12	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.		
13	The proposed NIPS hardware/appliance/solution should support VLAN tagging (IEEE 802.1q)		
14	The Warranty and AMC should include all the components supplied as part of the Proposed NIPS hardware/appliance/solution. including trans receivers, breakout cables etc.		
C	**Performance Requirement**		
1	The proposed NIPS hardware/appliance/solutions IPS Inspection throughput (HTTP Based) should have minimum 30 Gbps		
2	The proposed NIPS hardware/appliance/solution should be running all internet protocols etc., traffic flowing through different zones with all the features enabled and running		
3	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.		

4	The proposed NIPS hardware/appliance/solution should support minimum 20 million concurrent connections		
5	The proposed NIPS hardware/appliance/solution should support minimum 0.35 million new sessions per second processing		
6	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.		
7	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.		
8	The proposed Firewall hardware/solution should supports all existing IPS attack signatures by default and all future signature released from time to time with Regular Expressions		
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.)		
10	Each Appliance of the proposed NIPS hardware/solution should be capable of handling existing and future security policies/rules.		
D	**Feature Requirement**		
1	The proposed NIPS hardware/appliance/solution should have		

	capability to keep track the network connections, identify the threats, detect and prevent the threat and relate the threat with corresponding end points (IP address, user, software program etc.		
2	The proposed NIPS hardware/appliance/solution should able to get enterprise visibility of internet access like URL access, Malicious website/server visits, country details etc.		
3	The proposed NIPS hardware/appliance/solution should provide segmentation and each segment can be deployed with different policy/rules based on traffic analysis of particular segment.		
4	The proposed NIPS hardware/appliance/solution should support application layer controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.		
5	The proposed NIPS hardware/appliance/solution should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location.		
6	In the proposed NIPS hardware/appliance/solution the detection engine must incorporate multiple approaches for detecting threats, including a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques. Identify and explain each type of detection mechanism supported.		
7	The proposed NIPS hardware/appliance/solution should allow Custom user-defined signatures with Regular Expressions		
8	The proposed NIPS should support capability to configure correlation rule where multiple rules/events can be combined together for better efficacy.		
9	The proposed NIPS hardware/appliance/solution Should support to enable/disable each individual signature. Each signature should allow granular tuning		
E	**Detection and Prevention Requirement**		
1	The proposed NIPS hardware/appliance/solution should support different mode of deployment in following modes:		

	a) IDS b) TAP Mode c) Inline		
2	The proposed NIPS hardware/appliance/solution should accurately detect intrusion attempts and discern between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, hybrids, and zero-day attacks, Worm, Phishing, Spyware, Virus, Trojan, P2P, VoIP, Backdoor, Reconnaissance, Bandwidth Hijacking, Cross-site scripting, SQL Injection etc.		
3	The proposed NIPS hardware/appliance/solution should employ all seven-layer (of OSI model) protocol analysis.		
4	The proposed NIPS hardware/appliance/solution should support vulnerability based and not exploit based signatures. Detects and blocks all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability)		
5	The proposed NIPS hardware/appliance/solution should support a wide variety of techniques to perform traffic inspection including (a) TCP stream reassembly, b) Does IP defragmentation, c) Bi- directional inspection, d) Protocol Anomaly Detection, e) Protocol tunnelling, f) Signatures g) Behaviour anomaly h) Reputation		
6	The proposed NIPS hardware/appliance/solution should have the ability to identify application traversing on the network and allow or block specific application on the network.		
7	The proposed NIPS hardware/appliance/solution should support source reputation based analysis and should obtain through the cloud the reputation for each host involved in an attack and uses the reputation score of the source host as one of the factor for blocking the host		
8	The proposed NIPS hardware/appliance/solution should support malware protection by performing file reputation analysis of malicious files		

9	The proposed NIPS hardware/appliance/solution should have the ability to inspect traffic in the virtual environment and if any additional hardware are required to achieve it, should be provided		
10	The proposed NIPS hardware/appliance/solution support provide advanced botnet protection using heuristic detection methods		
11	The proposed NIPS hardware/appliance/solution should provide advanced botnet protection using multi event behaviour based detection mechanism.		
12	The proposed NIPS hardware/appliance/solution should protect against DOS/DDOS attacks.		
13	The proposed NIPS hardware/appliance/solution Should support the ability to limit the number of TCP/UDP/ICMP active connections or connection rate from a host		
14	The proposed NIPS hardware/appliance/solution should have —self-learning" capability to monitor the network traffic and develops a baseline profile or recommendations. It should have the ability to constantly update this profile or recommendations to keep an updated view of the network for each segment.		
15	The proposed NIPS hardware/appliance/solution should support active blocking of traffic based on pre-defined rules to thwart attacks before any damage is done, i.e. before compromise occurs		
16	The proposed NIPS hardware/appliance/solution should have the ability to control traffic based on geographical locations. For e.g. a policy can be created to block traffic coming or going to a particular country.		
17	The proposed NIPS hardware/appliance/solution should have the ability to block connection from outside based on the reputation of the IP address that is trying to communicate with the network		
18	The proposed NIPS hardware/solution should be able to ingest the Intelligence shared over STIX / TAXII / API from the SIEM solution		

19	The proposed NIPS hardware/appliance/solution should protect against evasion techniques		
20	The proposed NIPS hardware/appliance/solution should support a wide range of response actions as a) Block traffic, b) Ignore, c) TCP reset, e) Log traffic, f) Packet capture, g) User defined scripts, h) Email alert, i) SNMP alert, j) syslog alert etc.		
21	The proposed NIPS hardware/appliance/solution should accurately detect the following Attack categories: Malformed traffic, Invalid Headers, Vulnerability exploitation, URL obfuscation, Asymmetric Traffic etc.		
22	The proposed NIPS hardware/appliance/solution must support vulnerability based and exploit based signatures. It should detect and block all known high risk exploits and the underlying vulnerability (not just one exploit of that vulnerability)		
23	The proposed NIPS hardware/appliance/solution should get Signatures, Patches & updates being received from OEM should be from trusted sites		
24	The proposed NIPS hardware/appliance/solution should handle following traffic inspection & support following: Ipv6, Ipv4, Tunnelled: 4in6, 6in4, 6to4,Bi-directional inspection, Detection of Shell Code, Buffer overflows, Advanced evasion protection Application Anomalies, P2P attacks, TCP segmentation and IP fragmentation Rate-based threats, Statistical anomalies		
25	The proposed NIPS hardware/appliance/solution should have the ability to identify/block individual applications (eg. Facebook or skype) running on one protocol (eg HTTP or HTTPs)		
26	The proposed NIPS hardware/appliance/solution should have		

	application intelligence for commonly used TCP/IP protocols, not limited to telnet, ftp, http, https etc		
27	The proposed NIPS hardware/appliance/solution should support Block attacks based on IP reputation, DNS Inspection and Sink-Holing, Geo-location, URL Inspection / intelligence		
28	The proposed NIPS hardware/appliance/solution should have the feature for importing SNORT signatures.		
29	The proposed NIPS hardware/appliance/solution should support basic attack protection features listed below but not limited to : Maximum no of protections against attacks that exploit weaknesses in the TCP/IP protocol suite g. NIPS should enable rapid detection of network attacks h. TCP reassembly for fragmented packet protection i. SYN cookie protection, SYN Flood, Half Open Connections and NUL Packets etc. j. Protection against IP spoofing k. Malformed packet protection l. Asymmetric Packet Transmission		
30	The proposed NIPS hardware/appliance/solution should be able to block Instant Messaging like Yahoo, MSN, ICQ, Skype (SSL and HTTP tunnelled) etc.		
31	The proposed NIPS hardware/appliance/solution should provide visibility into how network bandwidth is consumed to aid in troubleshooting network outages and detecting Advanced Malware related DoS & DDoS activity from within the network		
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.		
33	The proposed NIPS hardware/appliance/solution should be capable of whitelisting trusted applications from being inspected and not an entire segment to avoid business applications from being affected & in turn productivity		

F	High Availability Requirements:		
1	The proposed NIPS hardware/appliance/solution must support active-active OR Active-Standby High Availability. The HA should be out of the box solution and should not require any third party or additional software/hardware for the same		
2	The proposed NIPS hardware/appliance/solution should provide seamless failover among devices for all components and should be completely automatic without any sort of manual intervention		
3	The High Availability should be supported in the proposed NIPS hardware/appliance/solution from the day one and without any extra license		
4	The upgrade of HA pair in proposed NIPS hardware/appliance/solution should be seamless without any downtime		
5	The proposed NIPS hardware/appliance/solution deployed should support hitless upgrade for both Major and Minor codes in HA.		
6	All components of the proposed NIPS hardware/appliance/solution should be in HA		
7	The proposed NIPS hardware/appliance/solution must support active-active or Active-Standby High Availability without session loss. The HA should be out of the box solution and should not require any third party or additional software/hardware for the same		
8	The proposed NIPS hardware/appliance/solution should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc.		
9	In the proposed NIPS hardware/appliance/solution Centralized Management should provide high availability at site level for enabling DR deployment		
10	The proposed NIPS hardware/appliance/solution should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc. Firewall Appliance should have on-box storage capacity for OS images & log storage		

11	The proposed NIPS hardware/appliance/solution should have hot swappable redundant power supplies (Minimum dual power supply). Dual (redundant) AC power supply with Indian standard compatible power cords as well as C19-C20 or C13-C14 Power cord.		
12	The proposed Firewall hardware/solution should support minimum 2X400 GB HDD/SSD from day 1		
13	The proposed firewall hardware/solution should be rack mountable and supplied with rack mounting kit along with support side rails		
14	The proposed Firewall hardware/solution offered product part codes have to be General Availability Part codes and not custom built. There should be reference of Products to the public website of the OEM.		
G	**Administration, Management, Centralised Logging and Reporting Feature Requirement**		
1	The proposed NIPS hardware/appliance/solution should support Real-Time Monitoring, Management & Log Collection (with storage) should not be distributed to more than ONE server/appliance		
2	In the proposed NIPS hardware/appliance/solution, the centralized monitoring and management system should have multiple administrators who have administrative rights based on their roles and should keep Audit Trail of the Changes etc. performed by such administrator.		
3	In the proposed NIPS hardware/appliance/solution the secondary (SLAVE) Management Server should support the MASTER role once the Disaster recovery is triggered for any or multiple management domains in the Management Server		
4	In the proposed NIPS hardware/appliance/solution should be able to support large scale WAN deployment with following important Criteria for Real-Time Monitoring, Management & Log Collection etc. c. Any changes or commands issued by an authenticated user should be		

	logged to a database of the management system. d. Any changes or commands issued by an authenticated user should be logged to a database of the management system		
9	The proposed NIPS hardware/solution also should have feature to integrate with syslog & SNMP server v2c, v3 or higher and should support SNMP TRAPS.		
10	The proposed NIPS hardware/appliance/solution must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes.		
11	In the proposed NIPS hardware/appliance/solution management platform must provide a highly customizable dashboard.		
12	The proposed NIPS hardware/appliance/solution must provide simplified provisioning for addition of new IPSs where by a standard IPS policy could be pushed into the new IPS.		
13	The proposed NIPS hardware/appliance/solution administration station must provide a means for exporting the IPS rules set and configuration in readable format.		
14	The proposed NIPS hardware/appliance/solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward		
15	In the proposed NIPS hardware/appliance/solution Management console should be capable of producing extensive graphics metric for analysis. Further, users should be able to drill down into these graphical reports to view pertinent details.		
16	The proposed NIPS hardware/appliance/solution should support for role based administration of IPS		
17	The proposed NIPS hardware/appliance/solution should support granular management. Should allow policy		

	to be assigned per device, port, VLAN tag, IP address/range		
18	The proposed NIPS hardware/appliance/solution administration software must provide a means of viewing, filtering and managing the log data		
19	In the proposed NIPS hardware/appliance/solution logs must contain information about the IPS policy rule that triggered the log		
20	Centralized Security Management should include for all the proposed NIPS security controls but not limited to: i. Real Time Security Monitoring j. Logging k. Reporting functions based on 1. Security event risk level, 2. Date/time, 3. Event name 4. Source IP 5. Destination IP 6. Response Taken 7. Sensor Identity 8. Severity, etc. l. NIPS solution must provide a minimum basic statistics about the health of the IPS and the amount of traffic traversing the IPS m. NIPS Solution should support for configuration rollback n. NIPS Solution should support Real time traffic statistics & Historical report with o. Attacks and threat reports, etc. p. Customized reports on HTML, CSV ,PDF, Excel and XML format etc.		
21	The proposed NIPS hardware/appliance/solution Audit Trail should contain at a minimum below information for any Policy/Rule/Objects Modifications, Addition , Deletion or other network changes but not limited to e. The name of the administrator making the change f. The change made g. Time of change made h. Comments/Remarks		
22	The proposed NIPS hardware/appliance/solution management platform must provide multiple report output		

	types or formats, such as PDF, HTML, CSV, Excel and XML.		
23	The proposed NIPS hardware/appliance/solution management system should provide detailed Event analysis for IPS and also should provide Syslog output to integrate with other major SIEM tools and specifically should support RSA SIEM tool current and future versions		
24	The proposed NIPS hardware/appliance/solution should support for real time analysis of all traffic the IPS may encounter (all possible SOURCE, DEST, SERVICE, including groups) etc.		
25	The proposed NIPS hardware/appliance/solution should manage the NIPS appliances from a central management console		
26	The proposed NIPS hardware/appliance/solution management platform should supports policy configuration, command, control, and event management functions.		
27	The proposed NIPS hardware/solution administrator authentication of Management console should be facilitated by local database, PKI & remote server such as Radius, LDAP, AD, SAML and TACACS+/AAA. It should have the ability to dynamically fall back to the local user database in case of external/remote Radius, LDAP, AD, SAML and TACACS+/AAA Server outages.		
28	The proposed NIPS hardware/appliance/solution Management console should have the ability to allow access to specific hosts by enabling GUI Access and defining the list of authorized hosts/networks		
29	In the proposed NIPS hardware/appliance/solution signature updates and intelligence database update on NIPS and should be automatic without any reboot on proposed NIPS hardware/appliance		
30	The proposed NIPS hardware/appliance/solution management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows		
31	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.		
32	In the proposed NIPS hardware/solution Historical Reports shall be available for multiple timeframe i.e. hourly, daily, weekly, monthly as well as customized period in the solution.		
33	Centralized Management Server for the proposed NIPS hardware/solution should be deployed in VM (VM to be provided by Bank) and all necessary license should be provided from day one.		
34	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.		
35	In the proposed NIPS hardware/appliance/solution Centralized Management should provide high availability at site level for enabling DR deployment		
36	It should be possible to manage the entire proposed NIPS hardware/appliance/solution from Primary & Secondary management server/appliance placed at DC and DR. Management solution should have the capability to be deployed in geographically different location enabling DR deployment		
37	The proposed NIPS hardware/appliance/solution should have adequate local storage in order to keep the various logs		
38	The proposed NIPS hardware/appliance/solution should be able to perform entire packet capture of the infected traffic and sent to the other application for analysis		

39	The management software for the proposed NIPS hardware/solution should support the following for rule optimization a. Unused Rules Calculation for specific time-period based on NIPS Traffic Logs. b. Analysis on Covered/Shadow/Hidden Rules c. Analysis on Rules Consolidation (Merging of similar kind of rules) d. Analysis on Redundant Rules e. Tightening of Overly Permissive Rules (Any-Any) f. Analysis on Unattached/Unused Objects to simplify objects management g. Analysis on Rule-Reordering to improve the performance of the NIPS h. Analysis on Disabled/Expired Rules for enhanced visibility on the NIPS Rules sets or any other cases not defined above.		
40	The proposed NIPS hardware/appliance/solution Centralized Management Server should be deployed with HA in VM (to be provided by Bank) and all necessary license should be provided from day one by Bidder.		
41	The proposed NIPS hardware/appliance/solution should be manageable from the centralized management framework from DC and DR with support for managing Minimum 4 NIPS systems		
H	**Licensing Requirement**		
1	The proposed NIPS hardware/appliance/solution should have enterprise license without any restrictions.		
2	The proposed NIPS hardware/appliance/solution should be able to achieve all the features and functionalities mentioned in the RFP and accordingly, all the required licenses should be provided as part of overall solution.		
3	Every Gateway Security control (like Firewall , NIPS or any other feature required to meet above specification) must not have any licensing restriction on number of users and must be supplied for unlimited users unless specified otherwise.		
4	Any third party product required to achieve the functionality should be provided with the necessary enterprise version license of software/appliance and necessary hardware, database and other relevant		

	software or hardware etc. should be provided with proposed NIPS hardware/appliance/solution		
I	**Other**		
1	The proposed NIPS hardware/appliance/solution should must identify network related malicious activity, log information about such activity, report it to SIEM dashboard and attempt to block or stop it.		
2	The proposed NIPS hardware/appliance/solution Should have Intrusion prevention sensors delivering context-aware, IPS device should perform state full pattern recognition to identify vulnerability-based attacks through the use of multi-packet inspection across all protocols.		
3	The proposed NIPS hardware/appliance/solution must perform protocol decoding and validation for network traffic including: IP, TCB UDP, and ICMP.		
4	The proposed NIPS hardware/appliance/solution should identify attacks based on observed deviations in the normal RFC behaviour of a protocol or service.		
5	The proposed NIPS hardware/appliance/solution should identify attacks running inside of these tunnelling protocols such as GRE, IP-in-IP, MPLS, and Ipv4/Ipv6.		
6	The proposed NIPS hardware/appliance/solution should have ability to setup exceptions to filter out, fine-tune or adjust the actions for specific attacker or destination IP on a per signature basis.		
7	The proposed NIPS hardware/appliance/solution should be Capable to detect device failure link failure.		
8	The proposed NIPS hardware/appliance/solution should have an option to add exceptions for network and services.		
9	The proposed NIPS hardware/appliance/solution should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, performance impact, Release date, Industry Reference, Confidence level etc.		

10	The proposed NIPS hardware/appliance/solution should be integrated with Privileged Identity Management (PIM) & Security Incident & Event Management (SIEM) Solutions.		
11	The proposed NIPS hardware/appliance/solution should have Categories based on Application types, Security Risk level etc.		
12	If during the contract, solution is not performing as per specifications in this RFP, Bidder has to upgrade/enhance the devices or place additional devices and reconfigure the system without any cost to bank		
K	**Service, Support & Training**		
1	The proposed NIPS hardware/appliance/solution should be under 6 Hrs CTR support.		
2	The proposed NIPS hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC)		
3	The OEM must provide 24 X 7 X 365 highest level of technical support. The Bidder Must Ensure that the dedicated login credentials to Bank with highest level permissions to search knowledge base, downloading of the patches, documents and to manage the device. Bank should be able to raise tickets directly to OEMs online submission portal for all product related issues with priority case handling.		
4	"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."		

4. NIPS Type C: (Mumbai - 2, Hyderabad - 2)			
Make _____		**Model** _____	
Sr. No.	**Required Minimum Specifications**	**Bidder's compliance (Yes / No)**	**If yes, detail description how the solution /component would be compliant**
A	**Solution Requirement**		
1	The proposed NIPS hardware/appliance/solution must have Intrusion Prevention System, Anti-Bot, Anti-Virus, Anti-Malware, Anti-Spyware, Vulnerability Protection, URL Filtering, Zero-Day or unknown threat prevention, DNS Security service functionality by default.		
2	The communication between all the components of the proposed NIPS hardware/appliance/solution (IPS module, logging & policy and Web GUI Console) should be encrypted with SSL or PKI		
3	The proposed NIPS hardware/appliance/solution should provide seamless failover among devices for all components and should be completely automatic without session disconnect.		
4	The proposed NIPS hardware/appliance/solution should provide protection against various types of cyber-attacks evasive attacks, scripting attacks etc.		
5	The proposed NIPS hardware/appliance/solution should have capability to store Logs and configuration of all devices, centrally in the solution and should also have capability to send logs of all devices to the generic central log collection & management servers.		
6	The proposed NIPS hardware/appliance/solution must support the complete STACK of IP V4 and IP V6 services		
7	The detection engine of the proposed NIPS hardware/appliance/solution should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).		
8	The proposed NIPS hardware/appliance/solution must be capable of dynamically tuning IPS sensors (Like: selecting rules/signatures, configuring policies, updating policies, etc.) with minimal human intervention		
9	The proposed NIPS hardware/solution must be appliance based and should facilitate multi-application environment which should support current network traffic as well as future growth		

10	The proposed NIPS hardware/solution administrator authentication should be facilitated by local database, PKI & remote server such as Radius, LDAP, AD, SAML and TACACS+/AAA. It should have the ability to dynamically fall back to the local user database in case of external/remote Radius, LDAP, AD, SAML and TACACS+/AAA Server outages.		
B	**System Hardware and Interface Requirement**		
1	In the proposed NIPS hardware/appliance/solution all ports should be populated with required transceivers. Apart from each appliance should have additional ports for sync, HA and other functionalities.		
2	The proposed NIPS hardware/appliance/solution should have Console port.		
3	The proposed NIPS hardware/appliance/solution should have separate dedicated management 1G Ethernet interface for Out of Band Management. None of the monitoring ports should be used for this purpose.		
4	The proposed NIPS hardware/solution should be rack mountable and supplied with rack mounting kit along with support side rails.		
5	The proposed NIPS hardware/appliance/solution should have hardware health monitoring capabilities and should provide different parameters through SNMP		
6	The proposed NIPS hardware/appliance/solution should support VLAN tagging (IEEE 802.1q)		
7	The proposed NIPS hardware/appliance/solution should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy and higher throughput/Bandwidth.		
8	The proposed NIPS hardware/solution should not limit on assigning CPU & memory to the OS for better performance		
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.		
10	The proposed NIPS hardware/appliance/solution should be based on multi-core cpu's to protect & scale against dynamic latest security threats		

11	The proposed NIPS hardware/appliance/solution should have minimum 2X400 GB SSD/HDD from Day 1		
12	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.		
13	The proposed NIPS hardware/appliance/solution should support VLAN tagging (IEEE 802.1q)		
14	The Warranty and AMC should include all the components supplied as part of the Proposed NIPS hardware/appliance/solution. including trans receivers, breakout cables etc.		
C	**Performance Requirement**		
1	The proposed NIPS hardware/appliance/solutions IPS Inspection throughput (HTTP Based) should have minimum 10 Gbps.		
2	The proposed NIPS hardware/appliance/solution should be running all internet protocols etc., traffic flowing through different zones with all the features enabled and running		
3	The performance requirement is for a single hardware appliance and should not be for a cluster/stack.		
4	The proposed NIPS hardware/appliance/solution should support minimum 12 million concurrent connections		
5	The proposed NIPS hardware/appliance/solution should support minimum 0.35 million new sessions per second processing		
6	In the proposed NIPS hardware/appliance/solution maximum permissible latency should be less than 200 microseconds with all the services enabled together.		
7	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.		
8	The proposed Firewall hardware/solution should supports all existing IPS attack signatures by default and all future signature released from time to time with Regular Expressions		
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.)		
10	Each Appliance of the proposed Firewall hardware/solution should be capable of handling existing and future security policies/rules.		
D	**Feature Requirement**		
1	The proposed NIPS hardware/appliance/solution should have capability to keep track the network connections, identify the threats, detect and prevent the threat and relate the threat with corresponding end points (IP address, user, software program etc.		
2	The proposed NIPS hardware/appliance/solution should able to get enterprise visibility of internet access like URL access, Malicious website/server visits, country details etc.		
3	The proposed NIPS hardware/appliance/solution should provide segmentation and each segment can be deployed with different policy/rules based on traffic analysis of particular segment.		
4	The proposed NIPS hardware/appliance/solution should support application layer controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.		
5	The proposed NIPS hardware/appliance/solution should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location.		
6	In the proposed NIPS hardware/appliance/solution the detection engine must incorporate multiple approaches for detecting threats, including a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques. Identify and explain each type of detection mechanism supported.		

7	The proposed NIPS hardware/appliance/solution should allow Custom user-defined signatures with Regular Expressions		
8	The proposed NIPS should support capability to configure correlation rule where multiple rules/events can be combined together for better efficacy.		
9	The proposed NIPS hardware/appliance/solution Should support to enable/disable each individual signature. Each signature should allow granular tuning		
E	**Detection and Prevention Requirement**		
1	The proposed NIPS hardware/appliance/solution should support different mode of deployment in following modes: a) IDS b) TAP Mode c) Inline		
2	The proposed NIPS hardware/appliance/solution should accurately detect intrusion attempts and discern between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, hybrids, and zero-day attacks, Worm, Phishing, Spyware, Virus, Trojan, P2P, VoIP, Backdoor, Reconnaissance, Bandwidth Hijacking, Cross-site scripting, SQL Injection etc.		
3	The proposed NIPS hardware/appliance/solution should employ all seven-layer (of OSI model) protocol analysis.		
4	The proposed NIPS hardware/appliance/solution should support vulnerability based and not exploit based signatures. Detects and blocks all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability)		
5	The proposed NIPS hardware/appliance/solution should support a wide variety of techniques to perform traffic inspection including (a) TCP stream reassembly, b) Does IP defragmentation, c) Bi- directional inspection, d) Protocol Anomaly Detection, e) Protocol tunnelling, f) Signatures g) Behaviour anomaly h) Reputation		
6	The proposed NIPS hardware/appliance/solution should have the ability to identify application traversing on the network and allow or block specific application on the network.		
7	The proposed NIPS hardware/appliance/solution should support source reputation based analysis and should obtain through the cloud the reputation for each		

	host involved in an attack and uses the reputation score of the source host as one of the factor for blocking the host		
8	The proposed NIPS hardware/appliance/solution should support malware protection by performing file reputation analysis of malicious files		
9	The proposed NIPS hardware/appliance/solution should have the ability to inspect traffic in the virtual environment and if any additional hardware are required to achieve it, should be provided		
10	The proposed NIPS hardware/appliance/solution support provide advanced botnet protection using heuristic detection methods		
11	The proposed NIPS hardware/appliance/solution should provide advanced botnet protection using multi event behaviour based detection mechanism.		
12	The proposed NIPS hardware/appliance/solution should protect against DOS/DDOS attacks.		
13	The proposed NIPS hardware/appliance/solution Should support the ability to limit the number of TCP/UDP/ICMP active connections or connection rate from a host		
14	The proposed NIPS hardware/appliance/solution should have —self-learning" capability to monitor the network traffic and develops a baseline profile or recommendations. It should have the ability to constantly update this profile or recommendations to keep an updated view of the network for each segment.		
15	The proposed NIPS hardware/appliance/solution should support active blocking of traffic based on pre-defined rules to thwart attacks before any damage is done, i.e. before compromise occurs		
16	The proposed NIPS hardware/appliance/solution should have the ability to control traffic based on geographical locations. For e.g. a policy can be created to block traffic coming or going to a particular country.		
17	The proposed NIPS hardware/appliance/solution should have the ability to block connection from outside based on the reputation of the IP address that is trying to communicate with the network		
18	The proposed NIPS hardware/solution should be able to ingest the Intelligence shared over STIX / TAXII / API from the SIEM solution		
19	The proposed NIPS hardware/appliance/solution should protect against evasion techniques		

20	The proposed NIPS hardware/appliance/solution should support a wide range of response actions as a) Block traffic, b) Ignore, c) TCP reset, e) Log traffic, f) Packet capture, g) User defined scripts, h) Email alert, i) SNMP alert, j) syslog alert etc.		
21	The proposed NIPS hardware/appliance/solution should accurately detect the following Attack categories: Malformed traffic, Invalid Headers, Vulnerability exploitation, URL obfuscation, Asymmetric Traffic etc.		
22	The proposed NIPS hardware/appliance/solution must support vulnerability based and exploit based signatures. It should detect and block all known high risk exploits and the underlying vulnerability (not just one exploit of that vulnerability)		
23	The proposed NIPS hardware/appliance/solution should get Signatures, Patches & updates being received from OEM should be from trusted sites		
24	The proposed NIPS hardware/appliance/solution should handle following traffic inspection & support following: Ipv6, Ipv4, Tunnelled: 4in6, 6in4, 6to4,Bi- directional inspection, Detection of Shell Code, Buffer overflows, Advanced evasion protection Application Anomalies, P2P attacks, TCP segmentation and IP fragmentation Rate-based threats, Statistical anomalies		
25	The proposed NIPS hardware/appliance/solution should have the ability to identify/block individual applications (eg. Facebook or skype) running on one protocol (eg HTTP or HTTPs)		
26	The proposed NIPS hardware/appliance/solution should have application intelligence for commonly used TCP/IP protocols, not limited to telnet, ftp, http, https etc		
27	The proposed NIPS hardware/appliance/solution should support Block attacks based on IP reputation, DNS Inspection and Sink-Holing, Geo-location, URL Inspection / intelligence		

28	The proposed NIPS hardware/appliance/solution should have the feature for importing SNORT signatures.		
29	The proposed NIPS hardware/appliance/solution should support basic attack protection features listed below but not limited to : Maximum no of protections against attacks that exploit weaknesses in the TCP/IP protocol suite m. NIPS should enable rapid detection of network attacks n. TCP reassembly for fragmented packet protection o. SYN cookie protection, SYN Flood, Half Open Connections and NUL Packets etc. p. Protection against IP spoofing q. Malformed packet protection r. Asymmetric Packet Transmission		
30	The proposed NIPS hardware/appliance/solution should be able to block Instant Messaging like Yahoo, MSN, ICQ, Skype (SSL and HTTP tunnelled) etc.		
31	The proposed NIPS hardware/appliance/solution should provide visibility into how network bandwidth is consumed to aid in troubleshooting network outages and detecting Advanced Malware related DoS & DDoS activity from within the network		
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.		
33	The proposed NIPS hardware/appliance/solution should be capable of whitelisting trusted applications from being inspected and not an entire segment to avoid business applications from being affected & in turn productivity		
F	**High Availability Requirements:**		
1	The proposed NIPS hardware/appliance/solution must support active-active OR Active-Standby High Availability. The HA should be out of the box solution and should not require any third party or additional software/hardware for the same		
2	The proposed NIPS hardware/appliance/solution should provide seamless failover among devices for all components and should be completely automatic without any sort of manual intervention		
3	The High Availability should be supported in the proposed NIPS hardware/appliance/solution from the day one and without any extra license		

4	The upgrade of HA pair in proposed NIPS hardware/appliance/solution should be seamless without any downtime		
5	The proposed NIPS hardware/appliance/solution deployed should support hitless upgrade for both Major and Minor codes in HA.		
6	All components of the proposed NIPS hardware/appliance/solution should be in HA		
7	The proposed NIPS hardware/appliance/solution must support active-active or Active-Standby High Availability without session loss. The HA should be out of the box solution and should not require any third party or additional software/hardware for the same		
8	The proposed NIPS hardware/appliance/solution should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc.		
9	In the proposed NIPS hardware/appliance/solution Centralized Management should provide high availability at site level for enabling DR deployment		
10	The proposed NIPS hardware/appliance/solution should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc. Firewall Appliance should have on-box storage capacity for OS images & log storage		
11	The proposed NIPS hardware/appliance/solution should have hot swappable redundant power supplies (Minimum dual power supply). Dual (redundant) AC power supply with Indian standard compatible power cords as well as C19-C20 or C13-C14 Power cord.		
12	The proposed Firewall hardware/solution should support minimum 2X400 GB HDD/SSD from day 1		
13	The proposed firewall hardware/solution should be rack mountable and supplied with rack mounting kit along with support side rails		
14	The proposed Firewall hardware/solution offered product part codes have to be General Availability Part codes and not custom built. There should be reference of Products to the public website of the OEM.		
G	**Administration, Management, Centralised Logging and Reporting Feature Requirement**		
1	The proposed NIPS hardware/appliance/solution should support Real-Time Monitoring, Management & Log Collection (with storage) should not be distributed to more than ONE server/appliance		

2	In the proposed NIPS hardware/appliance/solution, the centralized monitoring and management system should have multiple administrators who have administrative rights based on their roles and should keep Audit Trail of the Changes etc. performed by such administrator.		
3	In the proposed NIPS hardware/appliance/solution the secondary (SLAVE) Management Server should support the MASTER role once the Disaster recovery is triggered for any or multiple management domains in the Management Server		
4	In the proposed NIPS hardware/appliance/solution should be able to support large scale WAN deployment with following important Criteria for Real-Time Monitoring, Management & Log Collection etc. e. Any changes or commands issued by an authenticated user should be logged to a database of the management system. f. Any changes or commands issued by an authenticated user should be logged to a database of the management system		
9	The proposed NIPS hardware/solution also should have feature to integrate with syslog & SNMP server v2c, v3 or higher and should support SNMP TRAPS.		
10	The proposed NIPS hardware/appliance/solution must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes.		
11	In the proposed NIPS hardware/appliance/solution management platform must provide a highly customizable dashboard.		
12	The proposed NIPS hardware/appliance/solution must provide simplified provisioning for addition of new IPSs where by a standard IPS policy could be pushed into the new IPS.		
13	The proposed NIPS hardware/appliance/solution administration station must provide a means for exporting the IPS rules set and configuration in readable format.		
14	The proposed NIPS hardware/appliance/solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward		
15	In the proposed NIPS hardware/appliance/solution Management console should be capable of producing		

	extensive graphics metric for analysis. Further, users should be able to drill down into these graphical reports to view pertinent details.		
16	The proposed NIPS hardware/appliance/solution should support for role based administration of IPS		
17	The proposed NIPS hardware/appliance/solution should support granular management. Should allow policy to be assigned per device, port, VLAN tag, IP address/range		
18	The proposed NIPS hardware/appliance/solution administration software must provide a means of viewing, filtering and managing the log data		
19	In the proposed NIPS hardware/appliance/solution logs must contain information about the IPS policy rule that triggered the log		
20	Centralized Security Management should include for all the proposed NIPS security controls but not limited to: q. Real Time Security Monitoring r. Logging s. Reporting functions based on 1. Security event risk level, 2. Date/time, 3. Event name 4. Source IP 5. Destination IP 6. Response Taken 7. Sensor Identity 8. Severity, etc. t. NIPS solution must provide a minimum basic statistics about the health of the IPS and the amount of traffic traversing the IPS u. NIPS Solution should support for configuration rollback v. NIPS Solution should support Real time traffic statistics & Historical report with w. Attacks and threat reports, etc. x. Customized reports on HTML, CSV ,PDF, Excel and XML format etc.		
21	The proposed NIPS hardware/appliance/solution Audit Trail should contain at a minimum below information for any Policy/Rule/Objects Modifications, Addition , Deletion or other network changes but not limited to i. The name of the administrator making the change j. The change made k. Time of change made l. Comments/Remarks		

22	The proposed NIPS hardware/appliance/solution management platform must provide multiple report output types or formats, such as PDF, HTML, CSV, Excel and XML.		
23	The proposed NIPS hardware/appliance/solution management system should provide detailed Event analysis for IPS and also should provide Syslog output to integrate with other major SIEM tools and specifically should support RSA SIEM tool current and future versions		
24	The proposed NIPS hardware/appliance/solution should support for real time analysis of all traffic the IPS may encounter (all possible SOURCE, DEST, SERVICE, including groups) etc.		
25	The proposed NIPS hardware/appliance/solution should manage the NIPS appliances from a central management console		
26	The proposed NIPS hardware/appliance/solution management platform should supports policy configuration, command, control, and event management functions.		
27	The proposed NIPS hardware/solution administrator authentication of Management console should be facilitated by local database, PKI & remote server such as Radius, LDAP, AD, SAML and TACACS+/AAA. It should have the ability to dynamically fall back to the local user database in case of external/remote Radius, LDAP, AD, SAML and TACACS+/AAA Server outages.		
28	The proposed NIPS hardware/appliance/solution Management console should have the ability to allow access to specific hosts by enabling GUI Access and defining the list of authorized hosts/networks		
29	In the proposed NIPS hardware/appliance/solution signature updates and intelligence database update on NIPS and should be automatic without any reboot on proposed NIPS hardware/appliance		
30	The proposed NIPS hardware/appliance/solution management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows		
31	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.		
32	In the proposed NIPS hardware/solution Historical Reports shall be available for multiple timeframe i.e. hourly, daily, weekly, monthly as well as customized period in the solution.		
33	Centralized Management Server for the proposed NIPS hardware/solution should be deployed in VM (VM to be provided by Bank) and all necessary license should be provided from day one.		
34	The management software of the proposed Firewall hardware/solution should integrate with industry standard EMS product suite or any third party.		
35	In the proposed NIPS hardware/appliance/solution Centralized Management should provide high availability at site level for enabling DR deployment		
36	It should be possible to manage the entire proposed NIPS hardware/appliance/solution from Primary & Secondary management server/appliance placed at DC and DR. Management solution should have the capability to be deployed in geographically different location enabling DR deployment		
37	The proposed NIPS hardware/appliance/solution should have adequate local storage in order to keep the various logs		
38	The proposed NIPS hardware/appliance/solution should be able to perform entire packet capture of the infected traffic and sent to the other application for analysis		
39	The management software for the proposed NIPS hardware/solution should support the following for rule optimization a. Unused Rules Calculation for specific time-period based on NIPS Traffic Logs. b. Analysis on Covered/Shadow/Hidden Rules c. Analysis on Rules Consolidation (Merging of similar kind of rules)		

	d. Analysis on Redundant Rules e. Tightening of Overly Permissive Rules (Any-Any) f. Analysis on Unattached/Unused Objects to simplify objects management g. Analysis on Rule-Reordering to improve the performance of the NIPS h. Analysis on Disabled/Expired Rules for enhanced visibility on the NIPS Rules sets or any other cases not defined above.		
40	The proposed NIPS hardware/appliance/solution Centralized Management Server should be deployed with HA in VM (to be provided by Bank) and all necessary license should be provided from day one by Bidder.		
41	The proposed NIPS hardware/appliance/solution should be manageable from the centralized management framework from DC and DR with support for managing Minimum 4 NIPS systems		
H	**Licensing Requirement**		
1	The proposed NIPS hardware/appliance/solution should have enterprise license without any restrictions.		
2	The proposed NIPS hardware/appliance/solution should be able to achieve all the features and functionalities mentioned in the RFP and accordingly, all the required licenses should be provided as part of overall solution.		
3	Every Gateway Security control (like Firewall , NIPS or any other feature required to meet above specification) must not have any licensing restriction on number of users and must be supplied for unlimited users unless specified otherwise.		
4	Any third party product required to achieve the functionality should be provided with the necessary enterprise version license of software/appliance and necessary hardware, database and other relevant software or hardware etc. should be provided with proposed NIPS hardware/appliance/solution		
I	**Other**		
1	The proposed NIPS hardware/appliance/solution should must identify network related malicious activity, log information about such activity, report it to SIEM dashboard and attempt to block or stop it.		
2	The proposed NIPS hardware/appliance/solution Should have Intrusion prevention sensors delivering context-aware, IPS device should perform state full pattern recognition to identify vulnerability-based		

	attacks through the use of multi-packet inspection across all protocols.		
3	The proposed NIPS hardware/appliance/solution must perform protocol decoding and validation for network traffic including: IP, TCB UDP, and ICMP.		
4	The proposed NIPS hardware/appliance/solution should identify attacks based on observed deviations in the normal RFC behaviour of a protocol or service.		
5	The proposed NIPS hardware/appliance/solution should identify attacks running inside of these tunnelling protocols such as GRE, IP-in-IP, MPLS, and Ipv4/Ipv6.		
6	The proposed NIPS hardware/appliance/solution should have ability to setup exceptions to filter out, fine-tune or adjust the actions for specific attacker or destination IP on a per signature basis.		
7	The proposed NIPS hardware/appliance/solution should be Capable to detect device failure link failure.		
8	The proposed NIPS hardware/appliance/solution should have an option to add exceptions for network and services.		
9	The proposed NIPS hardware/appliance/solution should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, performance impact, Release date, Industry Reference, Confidence level etc.		
10	The proposed NIPS hardware/appliance/solution should be integrated with Privileged Identity Management (PIM) & Security Incident & Event Management (SIEM) Solutions.		
11	The proposed NIPS hardware/appliance/solution should have Categories based on Application types, Security Risk level etc.		
12	If during the contract, solution is not performing as per specifications in this RFP, Bidder has to upgrade/enhance the devices or place additional devices and reconfigure the system without any cost to bank		
K	**Service, Support & Training**		
1	The proposed NIPS hardware/appliance/solution should be under 6 Hrs CTR support.		
2	The proposed NIPS hardware/appliance/solution should have 24X7X365 global Technical Assistance Centre (TAC)		
3	The OEM must provide 24 X 7 X 365 highest level of technical support. The Bidder Must Ensure that the		

	dedicated login credentials to Bank with highest level permissions to search knowledge base, downloading of the patches, documents and to manage the device. Bank should be able to raise tickets directly to OEMs online submission portal for all product related issues with priority case handling.		
4	"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."		