राष्ट्रीय आवास बैंक
NATIONAL HOUSING BANK

RFP Reference No.: GEM/2025/B/6097193 dated April 03, 2025

Request for Proposal (RFP) for Supply, Installation and Support of Next Generation Firewall Solution (NGFW) at National Housing Bank

The replies to the pre-bid queries received are placed herewith.

राष्ट्रीय आवास बैंक, नई दिल्ली
सू०प्र०वि०
I. T. Deptt.
National Housing Bank, New Delhi

Bidder-1			
S. No.	**Relevant Clause of the RFP**	**Query**	**Bank Response to the Query**
1	Annexure XX : Technical Specifications, (Page 80) C. Performance Requirements 7. The Next-Generation Firewall (NGFW) must be equipped with a minimum of 32 GB of RAM from day1	Modern NGFWs utilize dedicated ASICs and security processors to offload resource-intensive tasks such as IPS, SSL decryption, and application control, minimizing dependency on general-purpose RAM. With this architecture, a 16 GB RAM configuration is technically sufficient to support high throughput, high session handling, and full-stack threat protection. Kindly consider revising the requirement to 16 GB to accommodate technically efficient, scalable, and cost-effective solutions without compromising security performance.	No change in clause, please be guided as per RFP terms and conditions
2	Annexure XX : Technical Specifications, (Page 80) B. General Specifications 15. At least 600 concurrent SSL VPN / Remote access users from day1 and at least 2500 Site to site VPN tunnel available from day1	The requirement of 600 concurrent SSL VPN users and 2500 site-to-site VPN tunnels appears significantly high. We request clarification on the actual number of remote users, planned site locations, and tunnel distribution per site to ensure alignment with operational needs. Nowadays, firewalls with hardware-accelerated encryption, optimized VPN processing with high session-handling capabilities can efficiently support remote access and site-to-site VPN connectivity without performance impact, even at a lower count. Over-specifying these values may unnecessarily limit competitive participation. Kindly consider revising the requirement to reflect validated user and site counts, or or to a lower, justifiable count, such as 500 SSL VPN users and 2000 site-to-site tunnels, to promote fair competition without compromising capability or scalability.	No change in clause, please be guided as per RFP terms and conditions
3	Annexure XX : Technical Specifications (Page 80) C. Performance Requirements 5. Solution architecture should have Control Plane separated from the Data Plane w.r.t routing and resource separation	The requirement for separation of the Control Plane and Data Plane with respect to routing and resource allocation should be defined as logical separation, as modern architectures enforce isolation through dedicated processing threads, memory segmentation, and secure system partitions. This approach provides the necessary operational integrity and performance while maintaining architectural flexibility, without the need for physical separation.	Solution architecture should have Control Plane separated from the Data Plane w.r.t routing and resource separation. This can be implemented via physical or logical separation.
4	Annexure XX : Technical Specifications, (Page 80) C. Performance Requirements 1. The firewall solution shall deliver a minimum of 6.5 Gbps after enabling Threat Prevention	The specified 6.5 Gbps Threat Prevention throughput may not adequately address the rising volume of encrypted and application-level traffic typical in today's enterprise networks. Increasing the requirement to at least 9 Gbps would ensure sustained performance even with all security features active, particularly in high-load scenarios and accounting for future scalability and organizational needs. Additionally, to better align the specifications with practical performance needs, it is recommended to include SSL/TLS inspection with IPS throughput of a minimum 8 Gbps to maintain visibility into encrypted traffic, and IPSec VPN throughput of at least 50 Gbps to support efficient, low-latency communication across multiple sites.	No change in clause, please be guided as per RFP terms and conditions
5	Annexure XX : Technical Specifications C. Performance Requirements 8. Must have minimum 400 GB of SSD storage to store the configuration and logs locally in case of non-availability or connectivity issue with centralized logging server.	The currently specified 400 GB SSD storage may be insufficient for storing high-volume log data, especially in environments with significant traffic and extended retention requirements. Increasing the minimum storage capacity to 900 GB will ensure adequate space for logs, configurations, and historical data, enabling comprehensive analysis, compliance auditing, and scalability as organizational needs grow. Kindly consider this change, as it aligns with best practices for maintaining visibility and operational continuity in evolving enterprise networks.	No change in clause, please be guided as per RFP terms and conditions

राष्ट्रीय आवास बैंक, नई दिल्ली
सू०प्र०वि
I. T. Deptt.
National Housing Bank, New Delhi

6	Minimum Eligibility Criteria: Point 3 The Bidder should have supply, installation and support of Firewall in at least one Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates (>100 Cr.) in India not older than 5 years. The Bidder should submit details like name of contact person, along with his phone number for above projects.	Minimum Eligibility Criteria: The Bidder should have supply, installation and support of Firewall in at least one Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates (>100 Cr.) in India not older than 5 years with a minimum PO value of 5 crore. The Bidder should submit details like name of contact person, along with his phone number for above projects.	No change in clause, please be guided as per RFP terms and conditions
7	Minimum Eligibility Criteria: Point 5 Bidder should have a Minimum Annual Turnover of Rs. 45 lakhs (for non-MSME bidder) and NIL (for MSME and startup companies' bidder) for last three financial years.	Minimum Eligibility Criteria: Point 5 Bidder should have a Minimum Annual Turnover of Rs. 200 crores (for non-MSME bidder) and NIL (for MSME and startup companies' bidder) for last three financial years.	No change in clause, please be guided as per RFP, terms and conditions
8	Minimum Eligibility Criteria: Point 7 Bidder should have valid ISO 9001:2015, ISO/IEC 27001 certificates	Minimum Eligibility Criteria: Point 7 Bidder should have valid ISO 9001:2015 & CMMI Level3 certificates	No change in clause, please be guided as per RFP terms and conditions
Bidder-2			
1	Page No. 5 **(Scope of Work)** (e.) Bank may ask bidder to integrate additional tool with firewall. Bidder should integrate the same at no cost to the Bank.	We kindly request the authorities to please provide further clarification on the additional tools that may need to be integrated with the firewall. Could you specify which tools are expected for integration?	Required to integrate with SOAR and log forwarding to SIEM. SOAR, SIEM details will be shared with the successful bidder.
2	Page No. 5 **(Scope of Work)** (b.) The solution should be deployed in on prem Bank's **DR site in HA mode**	We kindly request if the authorities could confirm whether this is a completely new setup or an upgrade to an existing solution. Additionally, could you clarify if this setup has any dependencies on the DC site/setup?	Please be guided as per RFP terms and conditions
3	Page No. 5 **(Scope of Work)** (k.) The Bidder must arrange one day Training of OEM to the Bank's Technical teams. Bank may ask the training to bidder at any point of time, bidder has to align technical resources to do so at no extra cost to the bank.	We kindly request if the authorities could kindly specify whether the training should be conducted by the OEM or by OEM-certified resources. Additionally, can the training be conducted virtually, or does it need to take place at a specific location?	Training should be conducted by the OEM or by OEM-certified resources. Virtual training may be considered
4	Page No. 6 (**Deliverables)** (b.) The Bidder shall deliver hardware in 6 weeks and install/configure licenses/software and integrate with existing network of the Bank in 8 weeks	We kindly request the authorities to provide more details regarding the number of policies (if migration is required) or the configuration scope. This will help us better assess if the timeline of 2 weeks for integration is feasible.	The details will be shared with the successful bidder
5	General Query	We request it if the authorities could clarify whether the bidder is responsible for providing the hardware for the management server, or if the Bank will be provisioning it.	Bank will provide only the VM with storage for the management server, all others including OS, DB, Middleware, licenses, all softwares etc to be provided by the bidder
6	The Bidder shall deliver hardware in 6 weeks and install/configure licenses/software and integrate with existing network of the Bank in 8 weeks	Please help with the details of existing network architecture	The details of the existing network architecture will be shared with the successful bidder
7	The bidder shall rack mount, install, configure, and integrate the items and resolve issues, if any, with Bank's existing network viz. LAN/WAN etc.	As per our understanding, Rack , power and cooling will be provided by Bank. Please confirm.	Rack, Power and Cooling will be provided by Bank
Bidder-3			

1	Annexure XX : Technical Specifications, (Page 80) C. Performance Requirements 1. The firewall solution shall deliver a minimum of 6.5 Gbps after enabling Threat Prevention	The specified 6.5 Gbps Threat Prevention throughput may not adequately address the rising volume of encrypted and application-level traffic typical in today's enterprise networks. Increasing the requirement to at least 9 Gbps would ensure sustained performance even with all security features active, particularly in high-load scenarios and accounting for future scalability and organizational needs. Additionally, to better align the specifications with practical performance needs, it is recommended to include SSL/TLS inspection with IPS throughput of a minimum 6 Gbps to maintain visibility into encrypted traffic, and IPSec VPN throughput of at least 25 Gbps to support efficient, low-latency communication across multiple sites. **Request to amend the clause as :** **1. The firewall solution shall deliver a minimum of 9 Gbps after enabling Threat Prevention and 6 Gbps of SSL inspection throughput and IPSec VPN throughput of at least 25 Gbps.**	No change in clause, please be guided as per RFP terms and conditions
2	Annexure XX : Technical Specifications, (Page 80) C. Performance Requirements 7. The Next-Generation Firewall (NGFW) must be equipped with a minimum of 32 GB of RAM from day1	Modern NGFWs utilize dedicated ASICs and security processors to offload resource-intensive tasks such as IPS, SSL decryption, and application control, minimizing dependency on general-purpose RAM. With this architecture, a 16 GB RAM configuration is technically sufficient to support high throughput, high session handling, and full-stack threat protection. **Kindly consider revising the requirement to 16 GB to accommodate technically efficient, scalable, and cost-effective solutions without compromising security performance.**	No change in clause, please be guided as per RFP terms and conditions
3	Annexure XX : Technical Specifications, (Page 80) B. General Specifications 15. At least 600 concurrent SSL VPN / Remote access users from day1 and at least 2500 Site to site VPN tunnel available from day1	The requirement of 600 concurrent SSL VPN users and 2500 site-to-site VPN tunnels appears significantly high. We request clarification on the actual number of remote users, planned site locations, and tunnel distribution per site to ensure alignment with operational needs. Nowadays, firewalls with hardware-accelerated encryption, optimized VPN processing with high session-handling capabilities can efficiently support remote access and site-to-site VPN connectivity without performance impact, even at a lower count. Over-specifying these values may unnecessarily limit competitive participation. **Kindly consider revising the requirement to reflect validated user and site counts, or or to a lower, justifiable count, such as 500 SSL VPN users and 2000 site-to-site tunnels, to promote fair competition without compromising capability or scalability.**	No change in clause, please be guided as per RFP terms and conditions
4	Annexure XX : Technical Specifications (Page 80) C. Performance Requirements 5. Solution architecture should have Control Plane separated from the Data Plane w.r.t routing and resource separation	The requirement for separation of the Control Plane and Data Plane with respect to routing and resource allocation should be defined as logical separation, as modern architectures enforce isolation through dedicated processing threads, memory segmentation, and secure system partitions. This approach provides the necessary operational integrity and performance while maintaining architectural flexibility, without the need for physical separation.	Solution architecture should have Control Plane separated from the Data Plane w.r.t routing and resource separation. This can be implemented via physical or logical separation.

राष्ट्रीय आवास बैंक, नई दिल्ली
सू०प्र०वि०
I. T. Deptt.
National Housing Bank, New Delhi

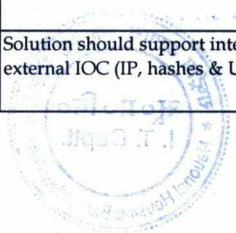
5	Annexure XX : Technical Specifications C. Performance Requirements 8. Must have minimum 400 GB of SSD storage to store the configuration and logs locally in case of non-availability or connectivity issue with centralized logging server.	The currently specified 400 GB SSD storage may be insufficient for storing high-volume log data, especially in environments with significant traffic and extended retention requirements. Increasing the minimum storage capacity to 900 GB will ensure adequate space for logs, configurations, and historical data, enabling comprehensive analysis, compliance auditing, and scalability as organizational needs grow. **Kindly consider this change, as it aligns with best practices for maintaining visibility and operational continuity in evolving enterprise networks.**	No change in clause, please be guided as per RFP terms and conditions
6	Clause 8.15 (Page no.13) Period of Validity of Bids: Prices and other terms offered by Bidders must be valid for a period of 06 months from the date of submission of commercial Bid for acceptance by NHB.	Prices and other terms offered by Bidders must be valid for a period of 03 months **from the date of submission of commercial Bid** for acceptance by NHB. Due to Dollar effect and fluctutation, Price retention for a period of 06 months will only depend on respective OEM	No change in clause, please be guided as per RFP terms and conditions
Bidder-4			
1	Annexure XX : Technical Specifications, (Page 80) C. Performance Requirements 1. The firewall solution shall deliver a minimum of 6.5 Gbps after enabling Threat Prevention	The specified 6.5 Gbps Threat Prevention throughput may not adequately address the rising volume of encrypted and application-level traffic typical in today's enterprise networks. Increasing the requirement to at least 9 Gbps would ensure sustained performance even with all security features active, particularly in high-load scenarios and accounting for future scalability and organizational needs. Additionally, to better align the specifications with practical performance needs, it is recommended to include SSL/TLS inspection with IPS throughput of a minimum 6 Gbps to maintain visibility into encrypted traffic, and IPSec VPN throughput of at least 25 Gbps to support efficient, low-latency communication across multiple sites. Request to amend the clause as : 1. The firewall solution shall deliver a minimum of 9 Gbps after enabling Threat Prevention and 6 Gbps of SSL inspection throughput and IPSec VPN throughput of at least 25 Gbps.	No change in clause, please be guided as per RFP terms and conditions
2	Annexure XX : Technical Specifications, (Page 80) C. Performance Requirements 7. The Next-Generation Firewall (NGFW) must be equipped with a minimum of 32 GB of RAM from day1	Modern NGFWs utilize dedicated ASICs and security processors to offload resource-intensive tasks such as IPS, SSL decryption, and application control, minimizing dependency on general-purpose RAM. With this architecture, a 16 GB RAM configuration is technically sufficient to support high throughput, high session handling, and full-stack threat protection. Kindly consider revising the requirement to 16 GB to accommodate technically efficient, scalable, and cost-effective solutions without compromising security performance.	No change in clause, please be guided as per RFP terms and conditions

राष्ट्रीय आवास बैंक, नई दिल्ली
सू०प्र०वि०
I. T. Deptt.
National Housing Bank, New Delhi

3	Annexure XX : Technical Specifications, (Page 80) B. General Specifications 15. At least 600 concurrent SSL VPN / Remote access users from day1 and at least 2500 Site to site VPN tunnel available from day1	The requirement of 600 concurrent SSL VPN users and 2500 site-to-site VPN tunnels appears significantly high. We request clarification on the actual number of remote users, planned site locations, and tunnel distribution per site to ensure alignment with operational needs. Nowadays, firewalls with hardware-accelerated encryption, optimized VPN processing with high session-handling capabilities can efficiently support remote access and site-to-site VPN connectivity without performance impact, even at a lower count. Over-specifying these values may unnecessarily limit competitive participation. Kindly consider revising the requirement to reflect validated user and site counts, or or to a lower, justifiable count, such as 500 SSL VPN users and 2000 site-to-site tunnels, to promote fair competition without compromising capability or scalability.	No change in clause, please be guided as per RFP terms and conditions
4	Annexure XX : Technical Specifications (Page 80) C. Performance Requirements 5. Solution architecture should have Control Plane separated from the Data Plane w.r.t routing and resource separation	The requirement for separation of the Control Plane and Data Plane with respect to routing and resource allocation should be defined as logical separation, as modern architectures enforce isolation through dedicated processing threads, memory segmentation, and secure system partitions. This approach provides the necessary operational integrity and performance while maintaining architectural flexibility, without the need for physical separation.	Solution architecture should have Control Plane separated from the Data Plane w.r.t routing and resource separation. This can be implemented via physical or logical separation.
5	Annexure XX : Technical Specifications C. Performance Requirements 8. Must have minimum 400 GB of SSD storage to store the configuration and logs locally in case of non-availability or connectivity issue with centralized logging server.	The currently specified 400 GB SSD storage may be insufficient for storing high-volume log data, especially in environments with significant traffic and extended retention requirements. Increasing the minimum storage capacity to 900 GB will ensure adequate space for logs, configurations, and historical data, enabling comprehensive analysis, compliance auditing, and scalability as organizational needs grow. Kindly consider this change, as it aligns with best practices for maintaining visibility and operational continuity in evolving enterprise networks.	No change in clause, please be guided as per RFP terms and conditions
Bidder-5			
1	Total Minimum Passing Technical Marks: 100	Criteria and Point system for the evaluation of the Technical Bids is not mentioned in the RFP document. As per the Bid Evaluation Methodology, bids will be evaluated based on Least Cost Based System (LCBS) i.e. Lowest Financial Bid. Kindly share the scoring criteria.	Bidder meeting the Minimum Eligibilty Criteria and Technical specifications will be given 100 marks and Bidders not meeting the Minimum Eligibilty Criteria and Technical specifications will be given 0 marks
2	Page No.: 33 The Bidder should have supply, installation and support of Firewall in at least one Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates (>100 Cr.) in India not older than 5 years. The Bidder should submit details like name of contact person, along with his phone number for above projects	As per the scope of work mentioned in the RFP, NHB should select an experienced and technically qualified bidders for smooth execution of the project. We request you to kindly amend this clause as: The Bidder should have supply, installation and support of Firewall in at least one Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates (>100 Cr.) in India not older than 5 years having a minimum order value of INR 1 Crore. The Bidder should submit details like name of contact person, along with his phone number for above projects.	No change in clause, please be guided as per RFP terms and conditions

3	Page No.: 22 The payments shall be released subject to submission of PBG and invoice as per this RFP. Payment terms are as follows: a. 90% payment will be released to selected bidder against delivery, Installation and operationalization of Firewall post sign-off of successful implementation by the Bank and balance 10% retention amount after completion of contract period (60 months). The 10% retention amount may be released against submission of equivalent amount of Bank Guarantee for the period of contract (60 months).	The payment terms are not favourable, since the successful bidder will submit a PBG @5% then retaining 10% of the contract value for enitre contract period (60 months) should be removed. We request you to kindly amend the payment terms as: The payments shall be released subject to submission of PBG and invoice as per this RFP. Payment terms are as follows: a. 90% payment will be released to selected bidder against delivery b. 10% on Installation and operationalization of Firewall post sign-off of successful implementation by the Bank ~~and balance 10% retention amount after completion of contract period (60 months). The 10% retention amount may be released against submission of equivalent amount of Bank Guarantee for the period of contract (60 months).~~ c. Quarterly payment against manpower.	No change in clause, please be guided as per RFP terms and conditions
4	Page No.: 24 (11.9) Bidder must deploy manpower having requisite qualification, experience, skill set etc. for the project/contract.	1. We request you to kindly share the total number of resources along with their requisite qualification, experience, skill set etc. 2. Kindly confirm the payment terms for manpower 3. Please include the manpower requirement in the price bid format.	No manpower to be deployed, if in case of any issue and not resolved remotely then the experienced qualified resourse to be deployed online/onsite to rectify the issue without additional cost to the Bank.
7	(i) The Vendor's aggregate liability, in connection with the obligations undertaken as a part of this Project, whether arising under this Project regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), other than the circumstances mentioned in the sub-clause (ii) below, shall be limited to _____ times of the total contract value.	Proposed Changes: (i) The Vendor's aggregate liability, in connection with the obligations undertaken as a part of this Project, whether arising under this Project regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), other than the circumstances mentioned in the sub-clause (ii) below, shall be limited to 5% of the total contract value provided these are beyond the supplier's control or delays attributed to NBH. (ii) The Vendor's liability in case of claims against NHB resulting from infringement of patents, trademarks, copyrights, or such other Intellectual Property Rights or breach of confidentiality obligations committed by the Vendor shall be capped at the total contract value and shall not be unlimited. (iii) Under no circumstances, NHB shall be liable to the Vendor for direct, indirect, incidental, consequential, special, or exemplary damages arising from termination of this Agreement, even if he has been advised of the possibility of such damages. However, NHB shall provide the Vendor with prior notice and an opportunity to cure any alleged breaches before termination. (iv) Under no circumstances, the Vendor shall be liable to NHB for any indirect and remote damages, including but not limited to loss of profits, business interruptions, or reputational harm, save and except the claims related to IPR infringement and breach of confidentiality obligations	No change in clause, please be guided as per RFP terms and conditions
8	5. Scope of Work Page No:5 P a g e | - 5 - a.) This RFP is for inviting bids for Next-Generation Firewall (NGFW) from OEMs other than CISCO, as CISCO firewall products are deployed in the Bank's DR site in other layer/s. Any bids received having products from OEM CISCO shall be summarily rejected.	Please share the current architecture. We assume in current architecture , Cisco is deployed at perimeter layer, pls confirm. Pls also calrify that, is there any exisitng firewall in any other layer. Pls share the details.	The details of the existing network architecture will be shared with the successful bidder
9	5. Scope of Work Page No:5 e) The Bidder is responsible for integrating the firewall solution with SIEM, SOAR and other necessary solutions of the bank. Bank may ask bidder to integrate additional tool with firewall. Bidder should integrate the same at no cost to the Bank.	Integration with any solution require additional effort and time which has financial implication also along with that, we need to check the compatibility / feasibility of integration with various tools. Hence we request you to kindly share the details of the solution/tools which need to be integrate with firewall.	Required to integrate with SOAR and log forwarding to SIEM. SOAR, SIEM details will be shared with the successful bidder.

10	5. Scope of Work Page No:5 g.In case the Bank decides to migrate the firewall/change the firewall placement to Perimeter/Internal, the Bidder should support the migration activity at no extra cost to the bank.	Kindly share the architecture for traffic flow understanding. Migration is additional effort , kindly consider it as separate line item in Price Bid.	No change in clause, please be guided as per RFP terms and conditions. Architecture details will be shared with the successful bidder.
11	5. Scope of Work Page No:5 h. In case the bank revamps its current architecture or completely migrates to another network technology/New location due to any reason, the bidder shall make necessary changes in its solution to adapt to new deployment without any additional cost to the Bank.	Migration to new architecture or migration to new location required complete recofiguration of firewalls kindly consider this activity as separate line item in Price Bid	No change in clause, please be guided as per RFP terms and conditions
12	5. Scope of Work Page No:5 K. The Bidder must arrange one day Training of OEM to the Bank's Technical teams. Bank may ask the training to bidder at any point of time, bidder has to align technical resources to do so at no extra cost to the bank.	We assume that training is one time activity during entire contract duration. Kindly confirm.	Yes training is one time activity
13	6. Deliverables Page No:6 c. The bidder shall rack mount, install, configure, and integrate the items and resolve issues, if any, with Bank's existing network viz. LAN/WAN etc.	As per our understanding the bidder scope is limited to delivery, Installation and operationalization of Firewall. Kindly confirm.	Supply, Installation,operationalization of Firewall and Support during the contract period. It is mentioned in RFP under the Scope of Work on page 5 that "Bidder has to provide support for update/upgrade activity as and when new stable patch is available"
Bidder-6			
A	Eligibility Criteria		
3	The provided hardware should not be end of support for next 7 years. It should continue to provide updates whenever applicable.	**Request bank to amend this clause as :** The provided hardware should not be end of support for next 5 years. It should continue to provide updates whenever applicable.	No change in clause, please be guided as per RFP terms and conditions
B	General Specifications		
3	Solution shall provide features and licenses for contractual period of 5 years for Firewall, IPS, Site to Site VPN, SSL VPN, SD-WAN, Granular Application control, Anti-Malware, IPS, URL filtering, DNS Security, Identity Awareness and Anti-Bot on same appliance managed through a separate centralized management console or integrated management console. Licenses should cover requirements as mentioned in S. No. A.1 for a period of 5 years.	Request Bank to provide clarity : In case of separate centralized management console, does bank will provide the VM infrastructure to host the management console or bidder has to factor the infrastructure for deploying Centralized Management console.	Bank will provide only the VM with storage for the management server, all others including OS, DB, Middleware, licenses, all softwares etc to be provided by the bidder
D	Protocol, User and Application support		
10	Should have more than minimum 4000 pre-defined distinct application signature (excluding custom application signatures) as application detection mechanism to optimize security effectiveness and should be able to create new application categories for operational efficiency	**Request bank to modify this clause as :** Should have more than minimum 5000+ pre-defined distinct application signature (excluding custom application signatures) as application detection mechanism to optimize security effectiveness and should be able to create new application categories for operational efficiency **Larger number of application signatures helps bank to address more applications and better granular policy control.**	No change in clause, please be guided as per RFP terms and conditions
F	Threat Prevention Feature Set		
2	Should support more than 14,000 IPS signatures or more.	**Request Bank to modify this clause as:** Should support more than 20,000+ IPS signatures or more. For better protection capability on IPS features which will help bank to address more vulenarbilities	No change in clause, please be guided as per RFP terms and conditions
3	Solution should support integration with external IOC (IP, hashes & URL's) feeds.	**Request Bank to amend this clause as:** Solution should support integration with external IOC (IP, URL's or hashes) feeds.	No change in clause, please be guided as per RFP terms and conditions



14	Application control database must contain more than 4000 pre-define application signatures (not custom signatures). The proposed solution must allow free custom application signatures for Homegrown and custom applications.	**Request Bank to modify this clause as :** Application control database must contain more than 5000+ pre-define application signatures (not custom signatures). The proposed solution must allow free custom application signatures for Homegrown and custom applications. **Larger number of application signatures helps bank to address more applications and better granular policy control.**	No change in clause, please be guided as per RFP terms and conditions
I	Administration, Management, Logging & Reporting		
1	The Firewall Management Solution, log server and reporting server can be either hardware appliance or VM based solution at On-prem only.	**Request Bank to clarfiy** does bank need standalone server for management, Logging & Reporting or bank need server as standby in case primary management , log server & reporting servers fails , also request to clarify does bank will provide VM infrastructure for this or bidder has to factor the VM infra for management console.	Bank will provide only the VM with storage for the management server, all others including OS, DB, Middleware, licenses, all softwares etc to be provided by the bidder
3	In case of VM based management solution, all other third-party licenses including OS, software components, databases etc. for running the solution has to be provided by the bidder for the entire duration of the project. All licenses shall be Enterprise class and solution has to be configured by the bidder to cater to smooth operation of the whole solution should be scalable to use more storage and compute if required.	**Request Bank to clarify** what would be the log retanation period, accordinlgy bidder can factor the storage and compute for vm based management console.	log retenation period will be as per Bank Policy/regulatory guidelines. Bank will provide only the VM with storage for the management server, all others including OS, DB, Middleware, licenses, all softwares etc to be provided by the bidder
	Recommened Features : Request bank to consider which will enhance the protection and security for your environment.	**Comments with brief use case**	
1	The proposed solution should support get visibility and control into DNS Security over TLS requests, by decrypting the DNS payload contained within the encrypted DNS request. Also the solution able to block DNS record types such as SVCB & HTTPS in NGFW	This features is very useful to bank where you can detect and prevent DNS threats those are based on record type SVCB & HTTPS. DNS over TLS is a popular mechanism to hide malicious domain queries. This is often used by attackers. Majority of customer allows comunication over 80 & 443. Since the traffic is encrypted, domain queries & response are not detected by basic DNS security solution. DNS over TLS will ensure such malicious behaviour is detected and blocked by NGFW.	Addition of new clause may not be considered
2	The Proposed solution should have support of predictive analytics and ML to disrupt attacks that use DNS for Payload infiltration, data theft and Command & Control by automatically blocking unknown malicious domains.	This feature is very useful for Bank to protect from attacker Techniques like Strategically Aged Domains and Malicious Newly Registered Domains (NRD) to overcome DNS blacklists. PaloAlto Predictive analytics that protect users from connecting to domains that were reserved and left dormant for months before use by malicious actors as well as identify domains registered by malicious actors at the time of registration	Addition of new clause may not be considered
3	The proposed NGFW solution should provide ability to create security policy based on Source IP Address mentioned in XFF headers for inbound traffic. This will ensure where the firewall can see threats with source IP information from where the actual attack has initiated, this can help SOC Team for better threat visibility and to know the source of infection.	This feature helps Bank for inbound traffic inspection. Most state sponsored adverseries are using CDN to hide their locations. Security policy based on XFF will help safeguard Bank infrastructure against such malicious activities.	Addition of new clause may not be considered

राष्ट्रीय आवास बैंक, नई दिल्ली
सू०प्र०वि०
I. T. Deptt.
National Housing Bank, New Delhi

4	The NGFW must provide immediate visibility into Covert communication traversing in Bank environment without any manual effort and additional configurations required. This should be Plug-n-Play feature. Applications bypassing traditonal security policy & running on non standard ports in the Bank environment. The Firewall must able to provide comprehensive report with Source/Destinaion IP, Application name (real application name & not protocol), source & destination Zone, data transfer amount & file name transfer. So Bank team can take preventive action accordingly. Example DNS ,HTTPS application running on any other port then 53 or 443.	This feature is very useful to Bank for visibility of non-standard port using in knonw applications, accordingly bank can take preventive actions. (example DNS ,HTTPS application running on any other port then 53 or 443). Threat actors use standard port to hide covert communication across infrastructure. Typically port 53, 80, 443 etc are allowed on most of the networks. Threat actors channel covert communication into these generic ports to hide themselves. It is extremely important for RBI to detect such covert communication and stop it using NGFW.	Addition of new clause may not be considered
5	The proposed NGFW solution should discover application using weaker encryption protocols in RBI environment so RBI can work with Application team to update / upgrade to stronger encryption protocols. Weaker encryption protocols such as TLS 1.0 / 1.1 etc are prone to exploitation, which must be detected / prevented by NGFW. This feature must be available without the need of decypting the SSL Traffic.	This feature is very usefule to Bank: where NGFW can track down old, vulnerable TLS versions and cipher suites so that firewall admin can make informed decisions about whether to allow connections with servers and applications that may compromise your security posture.	Addition of new clause may not be considered
6	The proposed NGFW solution should provide option where firewall admin can able to restart the Managment Plane without impacting dataplane traffic for troubleshooting / correcting issues related to management plane.	This feature is very useful to Bank, restarting management plane "may" help to firewall admin to address issues such as: > The WebGUI is sluggish or unresponsive > Stale admin sessions are being displayed > An authorization code has been entered but not activated or updated for a license > Logs not showing in the WebGUI	Addition of new clause may not be considered
Bidder-7			
1	The Firewall Management Solution, log server and reporting server can be either hardware appliance or VM based solution at On-prem only.	1.Kindly check number of days log storage required.	log retenation period will be as per Bank Policy/regulatory guidelines.
Page No-83, S.no-I		2.Kindly confirm for Management solution customer required Hardware appliance or VM based solution.	Bank will provide only the VM with storage for the management server, all others including OS, DB, Middleware, licenses, all softwares etc to be provided by the bidder