

S. No	Solution Name	Maximum Mark Allocated	Maximum Mark Obtained	Respective Solution Compliance (%)
1	Core Next Generation Firewall	730	0	0.00%
2	Firewall for perimeter / internet security	910	0	0.00%
3	Third Party Firewall	850	0	0.00%
4	Email Security	350	0	0.00%
5	Network security policy management (NSPM)	1160	0	0.00%
GRAND TOTAL		4000	0	

Instructions

Maximum Marks	Compliance (S/C)	Maximum Mark
10	S (Standard):	This indicates that the requirement is covered by the standard product functionality. It includes features available out-of-the-box, as well as those achievable through parametrization or rules configuration.
3	C (Customization):	Requirements marked as C (Customization) go beyond what is available or possible through standard product configuration. Customization involves: Development of custom code Creation of new functionalities or interfaces Modifications that may impact upgrade paths or require specific deployment and testing cycles User interface enhancements or custom-built screens Creation of entirely new functionality not supported by the base product

S.No	Instruction
1	Bidder must mandatorily mention the exact page number & clause or section reference from their submitted technical proposal or OEM product documentation which demonstrate compliance with each criteria (specification). Any Response marked as compliance without a valid page reference/section reference, shall be treated as in-complete and may be liable for rejection/scoring penalties
2	Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product
3	All Regulatory guidelines requirements as on the date of Bid Submission should be complied from day 1. Bidder/OEM is also required to comply with all the guidelines (regulatory & statutory) issued during the contract period
4	In case bidder has provided the response which is neither "S" or "C". The requirement shall be considered as "No"or "N", the bid shall be liable for rejection
5	All the above mentioned features should be available form the day 1.

Core Firewall					
S. No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	Solution should be purpose build hardware appliance with Access & Threat prevention controls. The next generation firewall gateway must be capable of supporting these next generation security applications on a unified platform - Stateful Inspection Firewall, Next Gen Firewall, Intrusion Prevention System, Application Control, URL filtering, Anti – Bot and Anti – Virus, DNS Security, HTTPS Inspection, IPsec VPN, Security Policy Management, Monitoring and Logging, Logging and Status, Event Correlation and Reporting, Compliance & Best Practices, Networking & Clustering. These security controls must be exclusively supported, supplied by and managed by the vendor from Day 1.	10	Select	0	
2	Proposed NGFW should not be proprietary ASIC based in nature or FGPA based & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats.	10	Select	0	
3	Appliance must have 1 x RJ45 Separate/OOB management port, 2x10G SFP+ Sync port, 1 x USB , dedicated console port.	10	Select	0	
4	The appliance must be fully populated with at least 4x1G RJ45 ports & 8x10G SFP+, 4x25G SFP28, 2x40G SFP interfaces with transceivers from day 1.	10	Select	0	
5	The appliance hardware should be a multicore CPU architecture.	10	Select	0	
6	The Next Generation Threat Prevention Throughput must be at least 35 Gbps and the said data should be available in public document / datasheet	10	Select	0	
7	The device should be latest and stable model released from OEM and should not go end of support and end of life for next 7 years.	10	Select	0	
8	NGFW must support at least the following from day 1: •750K connections per second •45M concurrent connections	10	Select	0	
9	Firewall must support NAT 66 and NAT 64 functionality from day 1	10	Select	0	
10	The firewall solution should support Internet Key Exchange (IKE) Version 1 (IKEv1) or Version 2 (IKEv2) for IPSEC VPN	10	Select	0	
11	Solution must support gateway high availability and load sharing with state synchronization.	10	Select	0	
12	The proposed solution of appliances should support the dynamic routing protocols with BGP & OSPF	10	Select	0	
13	The proposed solution must support different actions in the policy such as deny/drop, allow/accept etc.	10	Select	0	
14	Solution should have hardened OS for the appliance with dedicated on-prem management appliance/software.	10	Select	0	
15	Firewall must have redundant hot swappable fan and redundant hot swappable power supply to remove any single point of failure.	10	Select	0	
16	NG Firewall should support Identity based controls for Granular user, group based visibility and policy enforcement	10	Select	0	
17	Application control database must contain more than 7000 known applications. The proposed solution must allow free custom application signatures for Homegrown and custom applications.	10	Select	0	
18	NG Firewall should support the Identity based logging, application detection and usage controls	10	Select	0	
19	Should enable securities policies to identify, allow, block or limit application regardless of port, protocol etc.	10	Select	0	
20	The Firewall shall provide static as well as hide Network Address Translation (NAT) and Port Address Translation (PAT) functionality using automatic and manual NAT	10	Select	0	
21	The communication between the management servers and the security gateways must be encrypted.	10	Select	0	
22	Solution must support Configuration of dual stack gateway on a bond interface, OR on a sub-interface of a bond interface	10	Select	0	
23	IPS module must be based on the following detection mechanisms: exploit signatures, protocol anomalies, application controls and behavior-based detection	10	Select	0	
24	IPS module must provide at pre-defined profiles/policies that can be used immediately	10	Select	0	
25	IPS module must support a software-based fail-open mechanism, configurable based on thresholds of security gateways CPU and memory usage	10	Select	0	
26	IPS application must have a centralized event correlation and reporting mechanism	10	Select	0	
27	IPS must support network exceptions based on source, destination, service or a combination of the three.	10	Select	0	
28	The administrator must be able to activate new protections, based on configurable parameters (performance impact, threat severity, confidence level, client protections, server protections)	10	Select	0	
29	IPS must provide an automated mechanism to activate or manage new signatures from updates	10	Select	0	
30	IPS must have a mechanism to convert SNORT signatures and upload in the IPS signatures database.	10	Select	0	

Core Firewall					
S. No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
31	IPS must have options to create profiles for either client or server-based protections, or a combination of both.	10	Select	0	
32	Threat Protection detection engine be capable of detecting and preventing a wide variety of threats (e.g. network probes/reconnaissance, C&C, VoIP attacks, buffer overflows, P2P attacks etc.).	10	Select	0	
33	Solution should support an integrated Anti-Bot and Anti-Virus application on the next generation firewall	10	Select	0	
34	Anti-bot application should be able to detect and stop suspicious abnormal network behavior	10	Select	0	
35	Anti-Bot application should use a multi-tiered detection engine, which includes the reputation of IPs, URLs and DNS addresses and detect patterns of bot communications	10	Select	0	
36	Anti-Bot and Anti-Virus should have real time updates from a cloud-based reputation service.	10	Select	0	
37	The solution should have detection and prevention capabilities for DNS tunneling attacks	10	Select	0	
38	Antivirus engine must be integrated on the NGFW platform with inspection of 50+ file type	10	Select	0	
39	Anti-virus application must be able to prevent access to malicious websites	10	Select	0	
40	Anti-Virus must be able to scan archive files. Anti-Virus policies must be centrally managed with granular policy configuration and enforcement	10	Select	0	
41	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.	10	Select	0	
42	Management platform should provide autonomous threat prevention security policy.	10	Select	0	
43	Management and Firewall should be two separate dedicated systems.	10	Select	0	
44	NGFW appliances must be managed from a centralized dedicated management system VM based.	10	Select	0	
45	Device Management system includes Centralized Management, logging, compliance, best practices, reporting and event correlation functionality. All Licenses and component should be factored from Day 1	10	Select	0	
46	Device Management system should provide the real time health status of all the firewall modules for CPU & memory utilization, state table, total no. of concurrent connections and the connections per second counter. It must provide a security rule hit counter in the security policy.	10	Select	0	
47	Solution should consist of dedicated Management Server (VM Based or Hardware Based)	10	Select	0	
48	Solution must be able to segment the rule base in a layered structure. Solution must be able to segment the rule base to allow structure flexibility to align with dynamic networks. Support layer sharing within Threat Prevention policy	10	Select	0	
49	The proposed solution must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance	10	Select	0	
50	Solution must have capabilities for multi-domain management and support the concept of global security policy across domains, if needed in future.	10	Select	0	
51	The firewall and management should follow a physical segregation, and firewall should not cease to function when management becomes inaccessible/inactive or gest into failed state. The firewall should continue to function.	10	Select	0	
52	The solutions should be capable of providing insights within the existing policies to optimize it further in an auto manner by providing proactive prompts.	10	Select	0	
53	The solution should be able to build policies directly through Ansible & Terraform for specific segments	10	Select	0	
54	Should allow the report to be exported into the formats such as PDF, HTML, CSV etc. and logs must be exported in the CSV format.	10	Select	0	
55	The solution should be able to protect & inspect threats for QUIC protocol	10	Select	0	
56	The deployment of the entire solution should be carried out by OEM Professional Services team	10	Select	0	
57	The solution should possess Common Criteria EAL 4+ or Network Device Protection Profile (NDPP) certified under common criteria program and FIPS 140-2 validation, ensuring compliance with rigorous security standards.	10	Select	0	
58	AI-Powered Inline IPS & Threat Prevention				
58.1	A. The IPS engine MUST utilize inline, signature-less Machine Learning (ML) models directly within the data path to detect and block zero-day, polymorphic, and AI-generated exploits in real time (<10ms latency overhead).	10	Select	0	
58.2	B. The solution MUST support local, heuristic-based IPS inspection to detect mutated vulnerability exploits (e.g., AI-crafted variants of known CVEs) without requiring immediate cloud signature lookups.	10	Select	0	
58.3	C. The IPS engine MUST employ AI/ML behavioral analysis to detect and block low-and-slow, evasive Command and Control (C2) traffic and beaconing behavior associated with automated malware.	10	Select	0	

Core Firewall					
S. No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
59	Generative AI Application Access Control & Forwarding				
59.1	The firewall solution shall provide application-aware visibility and policy enforcement capabilities for Generative AI, LLM, and AI-powered services	10	Select	0	
59.2	The solution MUST support the ability to block or allow access to specific Generative AI sub-features based on URL or application-aware visibility (e.g., <i>Allow access to chat</i> but <i>completely block HTTP POST/File Upload paths</i> to AI domains).	10	Select	0	
59.3	ICAP / Service Chaining Support: The firewall MUST support ICAP (Internet Content Adaptation Protocol) or standard policy-based routing to seamlessly decrypt and forward outbound Generative AI-destined traffic to the bank's external, third-party DLP solution for inspection.	10	Select	0	
60	Hardware Architecture & SSL/TLS 1.3 Inspection				
60.1	The appliance MUST feature dedicated hardware acceleration (ASICs or specialized network processors) to ensure that running inline AI/ML IPS inspection and application-aware visibility tracking does not degrade core firewall throughput.	10	Select	0	
60.2	The vendor MUST provide certified performance benchmarks demonstrating sustained SSL/TLS 1.3 decryption throughput with <i>all</i> IPS engines and application control features concurrently enabled.	10	Select	0	
61	AI Log Governance & Compliance				
61.1	For any traffic dropped or flagged by heuristic/ML IPS models, the firewall management platform MUST generate detailed contextual logs explaining the nature of the anomaly to satisfy banking compliance audits (e.g., DORA, NIST).	10	Select	0	
61.2	The vendor MUST contractually guarantee that any decrypted network metadata or telemetry forwarded to the vendor's cloud threat intelligence infrastructure will not be used to train multi-tenant or public AI models.	10	Select	0	
62	Post-Quantum Cryptography (PQC) Technical Specifications				
62.1	Crypto-Agility Architecture: The firewall hardware and operating system MUST demonstrate complete "crypto-agility," allowing for modular software or firmware updates to swap, rotate, or deprecate cryptographic algorithms without requiring a physical hardware or appliance replacement.	10	Select	0	
62.2	Post-Quantum VPN Support (RFC 9370): For site-to-site and remote-access VPNs, the firewall MUST support IKEv2 hybrid key exchanges that combine classical algorithms (e.g., ECDH) with NIST-standardized Post-Quantum Cryptography (PQC) Key Encapsulation Mechanisms (KEM), specifically ML-KEM (FIPS 203).	10	Select	0	
62.3	PQC Digital Signatures: The IPS and firewall authentication mechanisms MUST natively support—or have a committed product roadmap to support—NIST-standardized post-quantum signature algorithms, including ML-DSA (FIPS 204) and SLH-DSA (FIPS 205), for secure certificate handling.	10	Select	0	
62.4	PQC TLS 1.3 Inspection & Detection: The firewall's decryption engine MUST be capable of parsing TLS 1.3 ClientHello extensions to detect, log, and control hybrid post-quantum cipher suites passing through the perimeter, ensuring deep visibility into enterprise PQC traffic.	10	Select	0	
62.5	Hardware Sizing for Large PQC Keys: The vendor MUST provide certified performance impact data demonstrating that the appliance's compute architecture can handle the significantly increased packet sizes, public key lengths, and mathematical overhead required by lattice-based PQC algorithms without dropping active banking sessions or degrading latency.	10	Select	0	
63	Solution should have centralized management at both DC and DR and can manage both DC and DR firewalls from both DC and DR managements	10	Select	0	
Total		730		0	

Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

Network Security Policy Management					
S. No.	Minimum Technical Specifications	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
A	General Requirement				
1	Product should support all the major Firewalls and devices.	10	Select	0	
2	Product should support both Public & Private Cloud technologies	10	Select	0	
3	Solution should support leading AAA & NAC solution, support should include policy visibility, change monitoring, risk analysis and regulatory compliance	10	Select	0	
4	Solution should support integration with ACI to fetch managed APIC configurations	10	Select	0	
5	Solution should support integration with ITSM tool over the APIs.	10	Select	0	
B	Administration, Manageability and Reporting				
6	Solution should be based on single device architecture; all modules of the proposed solution should be installed on same physical/Virtual appliance and the access should be web/GUI based	10	Select	0	
7	Solution should be capable to customize the reports through GUI mode such as changes in the time duration of unused rules, object etc.	10	Select	0	
8	Solution should support Role based operation, allows groups of firewalls, users, and permissions, including granular permission for report viewing and device action	10	Select	0	
9	Solution should support mapping user roles to Active Directory/ LDAP groups	10	Select	0	
10	Solution should have a client less Web interface i.e. no client software installation be installed to access the GUI	10	Select	0	
11	Solution should support retrieve user information from LDAP	10	Select	0	
12	Solution should provide reporting and charting on the available Out of the box parameters	10	Select	0	
13	Solution should have pre-configured reports and charts on the available Out of the box parameters	10	Select	0	
14	Solution should support of scheduling emails with customized reports on the available Out of the box parameters	10	Select	0	
15	Search all tickets related to a rule	10	Select	0	
16	Enhanced out of the box sample dashboard with trending on tickets opened recently, tickets' risk level, average SLA for tickets, tickets about to exceed their SLA, portion of tickets matching to changes and more	10	Select	0	
17	Solution should support the ability to customize application permissions for individual users or roles.	10	Select	0	
18	Solution should capture real time changes within the network device/business applications and display the same.	10	Select	0	
19	Solution support API for integration with DevOps Tool. Solution should have RBAC which provides specific permission as per the requirement	10	Select	0	
20	Solution should visualize security zones as part of the Business application diagram i.e. Traffic from Zone to Zone (External to Internal)	10	Select	0	
21	The solution should have an application dashboard tab to provide the below abilities to:				
21.1	Quickly and easily view a summary of security rules.	10	Select	0	
21.2	Show/verify application's connectivity.	10	Select	0	
21.3	Apply or discard changes to an application/connectivity.	10	Select	0	
21.4	Decommission an application/server.	10	Select	0	
21.5	Edit application/ rules information	10	Select	0	
21.6	Export application/rules information	10	Select	0	
21.7	Create a clone of the application/server.	10	Select	0	
22	The solution should support custom fields for applications/ use rule documentation for application information/manageability	10	Select	0	
C	Solution Capability				
23	Solution should run risk analysis by analyzing all possible traffic across Firewalls, ACI and NSX Infrastructure	10	Select	0	
24	Solution should be capable of running Risk Identification from Non-Secured to Secured Zones enforcing strong network segmentation	10	Select	0	
25	Solution should support. Topology aware risk Identification in multi-layer environment. For E.g. Check whether telnet is allowed from internal network to DMZ across all multi-vendor Firewalls	10	Select	0	
26	Solution should support Traffic-based Discovery e.g.: "is TCP/139 (Microsoft NetBIOS) allowed?	10	Select	0	

Network Security Policy Management					
S. No.	Minimum Technical Specifications	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
27	Solution should support customization of risk database by creating user defined risk items	10	Select	0	
28	Solution should support Threshold based Risk Identification e.g.: "Over 256 IP addresses are allowed to send Outbound e-mail directly"	10	Select	0	
29	Solution should allow whitelisting the Risky Traffic	10	Select	0	
30	Solution should support defining an expiry date for Whitelisted traffic, for example "a given Risky Rule should be whitelisted for a period of 1 month"	10	Select	0	
31	Solution should support visibility for URL Categories in T5Q, risks & policy optimization on firewalls	10	Select	0	
32	Solution should enable dashboards and customizable reports for baseline compliance and dashboard for any SLA violation.	10	Select	0	
33	Solution should generate a baseline configuration compliance report that compares device configurations to predefined baselines and reports exceptions for all the above mentioned brands of Firewalls	10	Select	0	
34	Solution should alert for all the policy / Configuration changes made on the Firewalls	10	Select	0	
35	Solution should provide info on-				
35.1	Redundant special case rules	10	Select	0	
35.2	Unused rule items	10	Select	0	
35.3	Disabled rules	10	Select	0	
35.4	Time-Inactive rules	10	Select	0	
35.5	Duplicate object and services	10	Select	0	
35.6	Rules without logging	10	Select	0	
35.7	Rules with non-compliant comments	10	Select	0	
35.8	Rules with empty comments	10	Select	0	
35.9	Rules about to expire	10	Select	0	
36	Solution should report on how to tighten overly permissive rules E.g. Rules having ANY source, ANY destination, Any service should break down to get an actual traffic passing through that rule	10	Select	0	
37	Solution should provide information on rule Reordering with Actionable modification recommendation	10	Select	0	
38	Suggest the Rule Reordering with an expected improvements on the performance/utilization of the firewall	10	Select	0	
39	Solution should provide report on Object usage within the Rule for Clean-up	10	Select	0	
40	Solution should provide report on both unattached and unused objects	10	Select	0	
41	Solution should suggest consolidation of Rules for optimizing the rules set for better manageability, audit and performance	10	Select	0	
42	Solution should generate an enterprise-wide Interactive network map by analyzing routing information of routers/switches and Firewalls. For end-to-end topology solution should integrate with all L3 routers, switches, Load balancers and SDN platforms	10	Select	0	
43	The solution should support SD-WAN devices routing and topology (including VPN tunnels), provide increased coverage for the network map integration	10	Select	0	
44	Solution should visualize the traffic flow over the network map	10	Select	0	
45	Solution should support routing-only query to assess how the network traffic is routed within in the network map	10	Select	0	
46	Solution should support route lookup from a selected device directly to a chosen destination to quickly troubleshoot any connectivity issues arising in daily operations	10	Select	0	
47	To understand end-to-end traffic flow within ACI fabric for connectivity between VRFs in the same tenant and in different tenants, and between VRFs in a common tenant and other tenants, solution should support Inter-VRF contract, imported contract, Hot formed contract	10	Select	0	
48	Solution should support running connectivity query analysis in multiple-firewall multiple-vendor environment	10	Select	0	
49	Solution's Traffic Simulation query should support application name or service-based query to find out the relevant blocked and allowed policies on the Firewalls	10	Select	0	
50	Solution should have GUI to customize Hardening/Baseline Profiles all the supported devices	10	Select	0	

Network Security Policy Management					
S. No.	Minimum Technical Specifications	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
51	Solution should allow Customization of request-form fields/ source fields /destination fields /service fields	10	Select	0	
52	Solution should support out of the box CSV upload feature to raise the Firewall change request	10	Select	0	
53	Solution should perform optimization on the traffic lines requested by the user i.e. When a requester opens a change request with several similar (or contained) traffic lines, solution should group them into one requested traffic line to avoid implementing identical or containing rules on devices	10	Select	0	
54	Solution should Auto-detect and should close the request automatically if the requested traffic is already allowed	10	Select	0	
55	Solution should Allow change planning through a simulation of traffic path and finds all the rules in all the firewalls that blocks the requested traffic	10	Select	0	
56	Solution should accurately detect the firewalls in path for the requested traffic using Network Topology Map	10	Select	0	
57	Solution should have enhanced Visual Flow to access out of the box change Workflows	10	Select	0	
58	Solution should support adding custom fields in the Request Template to feed in different kind of information in the Change request for e.g.: Location name, Manager name, Contact details etc.	10	Select	0	
59	Solution should have provision to configure the solution to allow users to view only specific Change Request templates to improve information security, as sensitive information defined in some templates should not b seen by unauthorized users	10	Select	0	
60	Solution should support configuring different logics basis on different conditions via GUI to process the tickets differently. For example: a conditional logic should be configured to send all the FW change tickets of X location to Y (location) IT Security team for an approval. This should be done within the GUI to avoid any customization in the existing workflows	10	Select	0	
61	Solution should support automatically identify the business impact of the Change Request and assess the risk as per the built-in best practices risk database	10	Select	0	
62	Solution should support automatically detect violations of regulatory requirements introduced by Change Request, before implementing on the devices	10	Select	0	
63	Solution should provide an Optimal Implementation Design such as "modification of an existing Policies instead of creating a new policy to allow the required Traffic"	10	Select	0	
64	Solution should detect and recommend relevant zones for requested traffic during the work order stage for zone-based Firewalls	10	Select	0	
65	Solution should support creation of objects at the Device Group level or at the Shared level	10	Select	0	
66	Solution should support automatic implementation and removal of policies on all firewall devices	10	Select	0	
67	Solution should support automatic implementation and removal of policies all the way.	10	Select	0	
68	Solution should support automatic implementation of new policies using URL categories all the way	10	Select	0	
69	The solution should support automatic implementation of FQDN based policies on firewalls	10	Select	0	
70	Solution should support automatic CLI creation for new policies and should push them directly	10	Select	0	
71	Solution should support automatic removal of an ACLs	10	Select	0	
72	Solution should support automatically Implementation and removal of policies of firewalls	10	Select	0	
73	Solution should support automatic Implementation & removal of Contracts	10	Select	0	
74	Solution should support automatic Implementation. removal of policies on distributed firewalls	10	Select	0	
75	Solution should support detecting and documenting changes made on firewalls in real time	10	Select	0	
76	Solution should automatically validate the change requests to save time and effort in validating recommended policy implementation	10	Select	0	
77	Solution should support Auto-correlating Change Requests to detected Change	10	Select	0	
78	Solution should provide timestamp of every stage of the complete Change Life Cycle	10	Select	0	
79	Solution should support unrequested change detection i.e. Identify unrequested or unauthorized changes to systems	10	Select	0	
80	Solution should have Rule Removal workflow which should allow to select the rule directly off the firewall policy with auto removal capability. Rule usage (last use date, frequency of use) information is automatically collected and included in the ticket, for easier approval/rejection of the change request	10	Select	0	

Network Security Policy Management					
S. No.	Minimum Technical Specifications	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
81	Solution should have a dedicated Drop Traffic Workflow with auto implementation capability (Adding drop rule) which should provide Business Continuity by an automatic detection of past change requests that allowed traffic that is now about to be removed, for efficient and error-free implementation	10	Select	0	
82	Solution should have Request Recertification Workflow which should inform all related ticket requestors of the Impending rule removal/modification to handle the approval and documentation process	10	Select	0	
83	Solution should have Rule Modification Workflow which should allow to select the rule directly off the firewall policy. Rule usage (last use date, frequency of use) Information should automatically be collected and included in the ticket, for easier approval/rejection for the modification	10	Select	0	
84	The solution must support parallel approval workflows out of the box. In scenarios where multiple independent approvals are required simultaneously	10	Select	0	
85	Solution should have a workflow which should executes automatically from change request submission to resolution i.e., Change Planning, risk assessment, recommending changes as well as auto implementation of rule can all be performed automatically without any would be needed human intervention.	10	Select	0	
86	Solution should have dedicated workflow to populate the organizational security policy to new devices i.e. enabling bulk update of tens or hundreds of rules using a single change request	10	Select	0	
87	Solution should have a capability to Search all the Firewall tickets related to a given rule configured on firewall	10	Select	0	
88	Solution should support defining the roles to view and use the Request Templates by users	10	Select	0	
89	Solution should support automated provisioning of application connectivity including decommissioning of Firewall rules from application or server prospective to enhance cyber-security posture	10	Select	0	
90	Solution should have a capability to discover Application Connectivity based network Traffic and NetFlow/Sflow.	10	Select	0	
91	The Application Discovery should provide instant so visibility into application through a graphical connectivity diagram of the servers associated to those business critical applications.	10	Select	0	
92	Solution to discover, map, and visualize application flows across both traditional and micro-segmented networks, meeting this requirement.	10	Select	0	
93	Solution should support an integration with leading Vulnerability scanners to present vulnerabilities in the Business Application context and hence support in prioritizing patching of vulnerabilities basis on their impact on application criticality	10	Select	0	
94	Solution should also be able to correlate the firewall configuration risks to the relevant application flovess allowing us to mitigate cyber-attack caused due to device misconfigurations	10	Select	0	
95	Solution should automatically identify all the applications which are going to get impacted during server or Application Migration and Decommissioning. If it is decided to decommission a server or an application, then solution should delete only the relevant rules automatically from all the firewalls without impacting other connectivity	10	Select	0	
96	Solution should be able to discover the application flovess automatically or build them via Firewall policies and map them with the relevant firewall security policies to assess & avoid impact of security change on Application availability	10	Select	0	
97	The solution can be used to push security rules to the cloud and analyze rule utilization. Based on the analysis, the solution should identify connectivity flows and security rules	10	Select	0	
98	Solution should provide firewall and network administrators an easy and convenient way to access the NSPM solution, to quickly take care of security policy management maintenance tasks listed below:-				
98.1	Troubleshoot network connectivity issues	10	Select	0	
98.2	Check the status of change requests and approve changes	10	Select	0	
98.3	Identify business applications affected by routine server or firewall maintenance, or server migrations	10	Select	0	

Network Security Policy Management					
S. No.	Minimum Technical Specifications	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
98.4	Identify all applications associated with a specific IP address, together with the relevant contact people for each application and other application-specific Information	10	Select	0	
D	Availability				
99	Solution should Support for Geographical distributed device architecture where remote agents can be configured to fetch Device Configuration & Logs locally and then be compressed before sending them to Central Manager for an analysis	10	Select	0	
Total		1160		0	

Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

Perimeter/ Internet Firewall					
S. No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	Entire Solution of NGFW firewall with Firewall, App Control, IPS, Anti-Malware (Bot, Virus), DNS Security with logging enabled on each appliance	10	Select	0	
2	Entire Solution of NGFW firewall should meet the minimum specified requirements on each appliance.	10	Select	0	
3	Throughput Inspection /threat prevention throughput 35 Gbps minimum with Firewall, App Control, IPS, Anti-Malware (Bot, Virus/Spam) with logging enabled in Enterprise Mix / Application Mix traffic New Sessions-750K connections per second Concurrent Sessions - 30 M The proposed Firewall should also provide URLF, DNS Security feature.	10	Select	0	
4	The appliance must be fully populated with at least 10x10G SFP+ ports and 4 x 25G SFP28 Fiber Ports, transceivers and interfaces from day 1. Additionally, Bidder to provide Port 2 x 10/25G port capacity and 2 x 40G/100G port capacity from day 1	10	Select	0	
5	Power on demand – Redundant fan and hot swappable AC/DC power supplies	10	Select	0	
6	Protocols to be support from Day 1 – Static, RIP v2, OSPFv2/v3 , BGP v4	10	Select	0	
7	Integrated functions to be enabled from Day 1 – Firewall, Application Awareness, IPS, and Zero Day Threat Prevention.	10	Select	0	
8	Virtual Domains/ Virtua Instances/Virtual systems/ etc. - The firewall appliance/platform shall provide minimum 10 number of virtual systems/domains/vdosm from Day 1	10	Select	0	
9	OEM provides single point of contact for customer management, escalation backed by senior product specialists throughout the contract period.	10	Select	0	
10	NGFW gateway architecture should have Control Plane separated from the Data Plane, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc.) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc.).	10	Select	0	
11	Dashboard view and real-time graph of CPU, Session usage activity. Dashboard should have the option to view the CPU usages for management activities for other activities	10	Select	0	
12	Minimum NG Threat prevention throughput in real world/production/Application Mix environment. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA.	10	Select	0	
13	Support Active/Active and Active/Passive deployment mode and should support session state synchronization among Next Generation Firewalls in a high availability.	10	Select	0	
14	Support Dual Stack IPv4 / IPv6 application control and threat inspection support in: transparent mode (IPS Mode), Layer 2, Layer 3, Should be able operate mix of multiple modes	10	Select	0	
15	Should support functionality for Full Mesh deployment architecture.	10	Select	0	
16	Support & implement Zones, IP address, Port numbers, User id, Application id and threat protection profile on the "proposed Next Generation Firewall/ proposed Next Generation Firewall Management console" for rule or the policy configuration	10	Select	0	
17	Native network traffic classification which identifies applications across all ports irrespective of port/protocol/ evasive tactics.	10	Select	0	
18	Ability to create custom application signatures and categories on Next Generation Firewall. Also the device should have capability to provide detailed information about applications	10	Select	0	
19	Handle (alert, block or allow) unknown/unidentified applications like unknown UDP & TCP	10	Select	0	
20	GUI/CLI based packet capture utility within its management console with capability of creating packet capture filters for IPv4 and IPv6 traffic and ability to define the packet or byte count	10	Select	0	
21	Ability to manage Next Generation Firewall with management deployed in high availability	10	Select	0	
22	Disallow root access to Next Generation Firewall system for all users (including super users) at all times	10	Select	0	
23	All the proposed threat functions like IPS/vulnerability protection, etc. should work in isolated air gapped environment without any need to connect with Internet.	10	Select	0	
24	Should have protocol decoder-based analysis which can statefully decodes the protocol and then intelligently applies signatures to detect network and application exploits	10	Select	0	
25	Intrusion prevention signatures should be built based on the vulnerability itself, A single signature should stop multiple exploit attempts on a known system or application vulnerability.	10	Select	0	

Perimeter/ Internet Firewall					
S. No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
26	IPS must have options to create profiles for either client or server based protections, or a combination of both.	10	Select	0	
27	Integrated IPS capabilities with minimum 10000+ signature database. It should support importing signatures from third party tools, customizing IPS signature and creation of multiple IPS policy for different segments and zones.	10	Select	0	
28	All the protection signatures should be created by vendor base on their threat intelligence and should not use any 3rd party IPS	10	Select	0	
29	OEM should deliver new signatures for unknown attacks seen anywhere else in real-time as soon as new verdicts are available. Proposed solution should integrate with the OEM for global intelligence data that is collected from a various source that provides additional leverage for preventing successful attacks by minimizing Bank's exposure time to malicious activity	10	Select	0	
30	Add custom threat prevention signature in an automated way by converting Snort OR Suricata signatures into custom threat signatures	10	Select	0	
31	The solution must support inspection of all major protocols, like HTTP, HTTP/2 traffic inspection, from Day 1 of deployment	10	Select	0	
32	The protection signatures created base unknown malware emulation should be payload or content base signatures that cloud block multiple unknown malware that use different hash but the same malicious payload	10	Select	0	
33	Equipment Test Certification: FCC Class A, CE Class A, VCCI Class A, CB or Common Criteria Certified.	10	Select	0	
34	Identify the amount of TLS traffic, non-TLS traffic, decrypted traffic, and non- decrypted TLS traffic, number of SSL sessions in a separate section for c better visibility and troubleshooting. Next Generation Firewall should also show decryption failure (if any) reason data in GUI for troubleshooting	10	Select	0	
35	Provide the support from day 1: · Network Address Translation (NAT) · · Port Address Translation (PAT) · · Dual Stack IPv4 / IPv6 (NAT64)	10	Select	0	
36	Support IPv6 functionality: • Port oversubscription/reuse/overload • Firewall policy with User and Applications • SSL Decryption • Administration of Gateway and Management solutions	10	Select	0	
37	The proposed solution must support Policy Based forwarding/ Policy based Routing based on: - Source or Destination Address - Source or destination port - Application (not port based) - AD/LDAP user or User Group - Services or ports	10	Select	0	
38	Support the ability to create QoS policy on a per rule basis: -by source address -by destination address -by application (such as Skype, Bittorrent, YouTube, Azureus) -by static or dynamic application groups (such as Instant Messaging or P2P groups) -by port and services	10	Select	0	
39	Support DHCP Client configuration & DHCP Server configuration	10	Select	0	
40	Bidirectional Forwarding Detection (BFD)	10	Select	0	
41	Should provide VOIP Applications Security by supporting to filter SIP, H.323, MGCP and Skinny flows.	10	Select	0	
42	NGFW should support the following authentication protocols: TACACS, LDAP, Radius, and Kerberos. Solution must have inbuilt integration (AD/LDAP) for Identity based policies without any external devices. AD/LDAP integration shall work with/without any additional VM dependency.	10	Select	0	
43	Acquire User Identities from: LDAP, Captive Portal, NACs (XML or API), Terminal Services	10	Select	0	
44	Allow single policy rule creation for application control, user based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS and scheduling.	10	Select	0	

Perimeter/ Internet Firewall					
S. No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
45	Offer dynamic capabilities that monitors proposed security gateways, policies and configuration settings all in real time which in turns helps Bank to easily map against security best practices and guide admins to adhere to same for strengthening the security posture of the Bank	10	Select	0	
46	The NGFW Central Management solution must support management of multiple security layers, providing superior policy efficiency and enabling you to manage security through a single pane of glass.	10	Select	0	
47	The management solution must have the native capability to optimize the security rule base and offer steps to remediate as per Bank's best practices. Solution should correlates logs from all gateways to identify suspicious activity, track trends and investigate/mitigate events – all through a single plane of glass	10	Select	0	
48	Should have separate real time logging base on all Traffic, Threats, User IDs, Data filtering, Content filtering, unknown malware analysis, Authentication, Tunneled Traffic and correlated log view base on other logging activities .	10	Select	0	
49	Report generation on a ad hoc or schedule (Daily, Weekly, Monthly, etc.) basis	10	Select	0	
50	Should allow the report to be exported into other format such as PDF, CSV, etc.	10	Select	0	
51	Should have built in report templates base on Applications, Users, Threats, Traffic	10	Select	0	
52	Proposed firewall must have the following, but not limited to: a) Firewall b) Networking c) IPSEC VPN d) SSL VPN e) IPS f) Application Control g) URL Filtering h) Anti-Bot i) Anti-malware j) Zero Day protection	10	Select	0	
53	Anti-bot application must be able to detect and stop suspicious abnormal network behavior	10	Select	0	
54	Anti-Bot application must use a multi-tiered detection engine, which includes the reputation of IPs, URLs and DNS addresses and detect patterns of bot communications	10	Select	0	
55	The Proposed Firewall should have provision for patching and updating for all its component as and when released by OEMs	10	Select	0	
56	The solution should have detection and prevention capabilities for DNS tunneling attacks	10	Select	0	
57	DNS trap feature as part of our threat prevention, assisting in discovering infected hosts generating C&C communication	10	Select	0	
58	Solution must protect from DNS Cache Poisoning and prevent users from accessing blocked domain addresses. DNS Exfiltration and Domain Generation Algorithm (DGA) to protect against the DNS tunneling. Bidder must provide additional license to achieve DNS protection.	10	Select	0	
59	Antivirus engine must be integrated on the NGFW platform with inspection of 50+ file type like .exe, .bat, .com, .dll, .vbs, .js, and .msi	10	Select	0	
60	Anti-virus application must be able to prevent access to malicious websites	10	Select	0	
61	Anti-Virus must be able to scan archive files. Anti-Virus policies must be centrally managed with granular policy configuration and enforcement	10	Select	0	
62	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.	10	Select	0	
63	Management platform should provide autonomous threat prevention security policy.	10	Select	0	
64	The solution architecture must ensure that the Hardware/VM Based Management System and the Firewall Appliance are deployed as two separate, dedicated systems. This separation is essential to: - Enhance firewall processing performance by offloading management and logging tasks - Avoid limitations in log storage and retention on the firewall appliance - Ensure scalability and operational efficiency in large or high-throughput environments	10	Select	0	
65	Firewall Management system includes Centralized Management, logging, compliance, best practices, reporting and event correlation functionality. All the required licenses is to be factored from Day 1	10	Select	0	

Perimeter/ Internet Firewall					
S. No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
66	Firewall Management system should provide the real time health status of all the firewall modules on the dashboard for CPU utilization, state table, total no. of concurrent connections and the connections per second counter. It must provide a security rule hit counter in the security policy.	10	Select	0	
67	Proposed Firewall must be able to segment the rule base in a layered structure. Solution must be able to segment the rule base to allow structure flexibility to align with dynamic networks. Support layer sharing within Threat Prevention policy	10	Select	0	
68	The proposed Firewall must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance	10	Select	0	
69	Proposed Firewall must have capabilities for multi-domain management and support the concept of global security policy across domains, if needed in future.	10	Select	0	
70	The firewall and management should follow a physical segregation, and firewall should not cease to function when management becomes inaccessible/inactive or gest into failed state. The firewall should continue to function.	10	Select	0	
71	The solution should support Threat Investigation with MITRE-Aligned Insights	10	Select	0	
72	The solution should detect the attack at the exploitation stage – i.e. before the shell code is executed and before the malware is downloaded/executed. Bidder proposed solution should integrate with the bank’s Sandboxing solution to meet the requirement	10	Select	0	
73	The solution should be able to detect ROP and other exploitation techniques.	10	Select	0	
74	The threat emulation solution should allow for "Geo Restriction" which enables emulations to be restricted to a specific country	10	Select	0	
75	Support Automatic update of Threat Prevention policy profiles to protect against the latest cyber threats using the latest technologies.	10	Select	0	
76	AI-Powered Inline IPS & Threat Prevention				
76.1	A. The IPS engine MUST utilize inline, signature-less Machine Learning (ML) models directly within the data path to detect and block zero-day, polymorphic, and AI-generated exploits in real time (<10ms latency overhead).	10	Select	0	
76.2	B. The solution MUST support local, heuristic-based IPS inspection to detect mutated vulnerability exploits (e.g., AI-crafted variants of known CVEs) without requiring immediate cloud signature lookups.	10	Select	0	
76.3	C. The IPS engine MUST employ AI/ML behavioral analysis to detect and block low-and-slow, evasive Command and Control (C2) traffic and beaconing behavior associated with automated malware.	10	Select	0	
77	Generative AI Application Access Control & Forwarding				
77.1	The firewall solution shall provide application-aware visibility and policy enforcement capabilities for Generative AI, LLM, and AI-powered services	10	Select	0	
77.2	The solution MUST support the ability to block or allow access to specific Generative AI sub-features based on URL or application-aware visibility (e.g., <i>Allow access to chat but completely block HTTP POST/File Upload paths</i> to AI domains).	10	Select	0	
77.3	ICAP / Service Chaining Support: The firewall MUST support ICAP (Internet Content Adaptation Protocol) or standard policy-based routing to seamlessly decrypt and forward outbound Generative AI-destined traffic to the bank's external, third-party DLP solution for inspection.	10	Select	0	
78	Hardware Architecture & SSL/TLS 1.3 Inspection				
78.1	The appliance MUST feature dedicated hardware acceleration (ASICs or specialized network processors) to ensure that running inline AI/ML IPS inspection and application-aware visibility tracking does not degrade core firewall throughput.	10	Select	0	
78.2	The vendor MUST provide certified performance benchmarks demonstrating sustained SSL/TLS 1.3 decryption throughput with <i>all</i> IPS engines and application control features concurrently enabled.	10	Select	0	
79	AI Log Governance & Compliance				
79.1	For any traffic dropped or flagged by heuristic/ML IPS models, the firewall management platform MUST generate detailed contextual logs explaining the nature of the anomaly to satisfy banking compliance audits (e.g., DORA, NIST).	10	Select	0	
79.2	The vendor MUST contractually guarantee that any decrypted network metadata or telemetry forwarded to the vendor's cloud threat intelligence infrastructure will not be used to train multi-tenant or public AI models.	10	Select	0	
80	Post-Quantum Cryptography (PQC) Technical Specifications				

Perimeter/ Internet Firewall					
S. No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
80.1	Crypto-Agility Architecture: The firewall hardware and operating system MUST demonstrate complete "crypto-agility," allowing for modular software or firmware updates to swap, rotate, or deprecate cryptographic algorithms without requiring a physical hardware or appliance replacement.	10	Select	0	
80.2	Post-Quantum VPN Support (RFC 9370): For site-to-site and remote-access VPNs, the firewall MUST support IKEv2 hybrid key exchanges that combine classical algorithms (e.g., ECDH) with NIST-standardized Post-Quantum Cryptography (PQC) Key Encapsulation Mechanisms (KEM), specifically ML-KEM (FIPS 203).	10	Select	0	
80.3	PQC Digital Signatures: The IPS and firewall authentication mechanisms MUST natively support—or have a committed product roadmap to support—NIST-standardized post-quantum signature algorithms, including ML-DSA (FIPS 204) and SLH-DSA (FIPS 205), for secure certificate handling.	10	Select	0	
80.4	PQC TLS 1.3 Inspection & Detection: The firewall's decryption engine MUST be capable of parsing TLS 1.3 ClientHello extensions to detect, log, and control hybrid post-quantum cipher suites passing through the perimeter, ensuring deep visibility into enterprise PQC traffic.	10	Select	0	
80.5	Hardware Sizing for Large PQC Keys: The vendor MUST provide certified performance impact data demonstrating that the appliance's compute architecture can handle the significantly increased packet sizes, public key lengths, and mathematical overhead required by lattice-based PQC algorithms without dropping active banking sessions or degrading latency.	10	Select	0	
76	The solution should support at least but not limited to File types :- - Archived: .tar, .gz, .zip, .bz2, .cab, .rar,.7z - Executable files (eg: .exe), PDF,.swf, Windows Office Document and Javascript - Additional file types: .bat,.dmg, .iso, .lnk, .pkg, .ps1	10	Select	0	
Total		910		0	

Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

Third Party Firewall					
S. No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	Entire Solution of NGFW firewall with Firewall, App Control, IPS, Anti-Malware (Bot, Virus), DNS Security with logging enabled on each appliance.	10	Select	0	
2	Throughput Inspection /threat prevention throughput-15 Gbps minimum with Firewall, App Control, IPS, Anti-Malware (Bot, Virus / Spam) with logging enabled in Enterprise Mix / Application Mix traffic New Sessions-300K per second Concurrent Sessions - 10M The proposed Firewall should also provide URLF, DNS Security feature	10	Select	0	
3	Port - 4x10/25G port capacity 2 x 40G/100G port capacity	10	Select	0	
4	Power on demand – Redundant fan and hot swappable AC/DC power supplies	10	Select	0	
5	Protocols to be support from Day 1 – Static, RIP v2, OSPFv2/v3 , BGP v4	10	Select	0	
6	Application Awareness refers to the firewall's ability to identify, control, and inspect application-level traffic, regardless of port or protocol. Identify traffic as being from specific applications (e.g., Dropbox, Oracle, Core Banking app).	10	Select	0	
7	Virtual Domains/ Virtual Instances/Virtual systems/ etc. - The firewall appliance/platform shall provide minimum 10 number of virtual systems/domains/vdosm from Day 1	10	Select	0	
8	OEM provides single point of contact for customer management, escalation backed by senior product specialists throughout the contract period.	10	Select	0	
9	NGFW gateway architecture should have Control Plane separated from the Data Plane, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc.) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc.).	10	Select	0	
10	Dashboard view and real-time graph of CPU, Memory, Session usage activity. Dashboard should have the option to view the CPU and memory usages for management activities for other activities	10	Select	0	
11	Minimum NG Threat prevention throughput in real world/production/Application Mix environment. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA.	10	Select	0	
12	Support Active/Active and Active/Passive deployment mode and should support session state synchronization among Next Generation Firewalls in a high availability.	10	Select	0	
13	The proposed FW should provide Dual Stack IPv4 / IPv6 application control and threat inspection support in: transparent mode (IPS Mode), Layer 2, Layer 3 and should be able operate mix of multiple modes from Day 1	10	Select	0	
14	Should support functionality for Full Mesh deployment architecture.	10	Select	0	
15	Support & implement Zones, IP address, Port numbers, User id, Application id and threat protection profile on the "proposed Next Generation Firewall/ proposed Next Generation Firewall Management console" for rule or the policy configuration	10	Select	0	
16	Native network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactics.	10	Select	0	
17	Ability to create custom application signatures and categories on Next Generation Firewall. Also the device should have capability to provide detailed information about applications	10	Select	0	
18	Handle (alert, block or allow) unknown/unidentified applications like unknown UDP & TCP	10	Select	0	
19	GUI/CLI based packet capture utility within its management console with capability of creating packet capture filters for IPv4 and IPv6 traffic and ability to define the packet or byte count	10	Select	0	
20	Ability to manage Next Generation Firewall with management deployed in high availability	10	Select	0	
21	Disallow root access to Next Generation Firewall system for all users (including super users) at all times	10	Select	0	

Third Party Firewall					
S. No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
22	All the proposed threat functions like IPS/vulnerability protection, etc. should work in isolated air gapped environment without any need to connect with Internet.	10	Select	0	
23	Should have protocol decoder-based analysis which can statefully decodes the protocol and then intelligently applies signatures to detect network and application exploits	10	Select	0	
24	Intrusion prevention signatures should be built based on the vulnerability itself, A single signature should stop multiple exploit attempts on a known system or application vulnerability.	10	Select	0	
25	IPS must have options to create profiles for either client or server based protections, or a combination of both.	10	Select	0	
26	Integrated IPS capabilities with minimum 10000+ signature database. It should support importing signatures from third party tools, customizing IPS signature and creation of multiple IPS policy for different segments and zones.	10	Select	0	
27	All the protection signatures should be created by vendor base on their threat intelligence and should not use any 3rd party IPS	10	Select	0	
28	OEM should deliver new signatures for unknown attacks seen anywhere else in real-time as soon as new verdicts are available. Bank should have instant access to OEM complete global intelligence data that is collected from a various sources that provides additional leverage for preventing successful attacks by minimizing Bank's exposure time to malicious activity	10	Select	0	
29	Add custom threat prevention signature in an automated way by converting Snort OR Suricata signatures into custom threat signatures	10	Select	0	
30	The solution must support inspection of all major protocols, like HTTP, HTTP/2 traffic inspection, from Day 1 of deployment	10	Select	0	
31	The protection signatures created base unknown malware emulation should be payload or content base signatures that cloud block multiple unknown malware that use different hash but the same malicious payload	10	Select	0	
32	Identify the amount of TLS traffic, non-TLS traffic, decrypted traffic, and non- decrypted TLS traffic, number of SSL sessions in a separate section for c better visibility and troubleshooting. Next Generation Firewall should also show decryption failure (if any) reason data in GUI for troubleshooting	10	Select	0	
33	Provide the support from day 1: · Network Address Translation (NAT) · · Port Address Translation (PAT) · · Dual Stack IPv4 / IPv6 (NAT64)	10	Select	0	
34	Support IPv6 functionality: • Port oversubscription/reuse/overload • Firewall policy with User and Applications • SSL Decryption • Administration of Gateway and Management solutions	10	Select	0	
35	The proposed solution must support Policy Based forwarding/ Policy based Routing based on: - Source or Destination Address - Source or destination port - Application (not port based) - AD/LDAP user or User Group - Services or ports	10	Select	0	
36	Support the ability to create QoS policy on a per rule basis: -by source address -by destination address -by application (such as Skype, Bittorrent, YouTube, Azureus) -by static or dynamic application groups (such as Instant Messaging or P2P groups) -by port and services	10	Select	0	
37	Support DHCP Client configuration & DHCP Server configuration	10	Select	0	
38	Bidirectional Forwarding Detection (BFD)	10	Select	0	
39	Acquire User Identities from: LDAP, Captive Portal, NACs (XML or API), Terminal Services	10	Select	0	

Third Party Firewall					
S. No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
40	Allow single policy rule creation for application control, user based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS and scheduling.	10	Select	0	
41	Offer dynamic capabilities that monitors proposed security gateways, policies and configuration settings all in real time which in turns helps Bank to easily map against security best practices and guide admins to adhere to same for strengthening the security posture of the Bank	10	Select	0	
42	The NGFW Central Management platform/solution must support management of multiple security layers, providing superior policy efficiency and enabling you to manage security through a single pane of glass.	10	Select	0	
43	The management solution must have the native capability to optimize the security rule base and offer steps to remediate as per Bank's best practices. Solution should correlates logs from all gateways to identify suspicious activity, track trends and investigate/mitigate events – all through a single plane of glass	10	Select	0	
44	Should have separate real time logging base on all Traffic, Threats, User IDs, Data filtering, Content filtering, unknown malware analysis, Authentication, Tunneled Traffic and correlated log view base on other logging activities .	10	Select	0	
45	Report generation on a ad hoc or schedule (Daily, Weekly, Monthly, etc.) basis	10	Select	0	
46	Should allow the report to be exported into other format such as PDF, CSV, etc.	10	Select	0	
47	Should have built in report templates base on Applications, Users, Threats, Traffic	10	Select	0	
48	Solution must have an integrated Anti-Bot and Anti-Virus application on the next generation firewall	10	Select	0	
49	Anti-bot application must be able to detect and stop suspicious abnormal network behavior	10	Select	0	
50	Anti-Bot application must use a multi-tiered detection engine, which includes the reputation of IPs, URLs and DNS addresses and detect patterns of bot communications	10	Select	0	
51	Anti-Bot and Anti-Virus must have real time updates from a cloud-based reputation service. Look for C&C traffic patterns, not just at their DNS destination	10	Select	0	
52	The solution should have detection and prevention capabilities for DNS tunneling attacks	10	Select	0	
53	DNS trap feature as part of our threat prevention, assisting in discovering infected hosts generating C&C communication	10	Select	0	
54	Solution must protect from DNS Cache Poisoning and prevent users from accessing blocked domain addresses. DNS Exfiltration and Domain Generation Algorithm (DGA) to protect against the DNS tunneling. Bidder must provide additional license to achieve DNS protection.	10	Select	0	
55	Antivirus engine must be integrated on the NGFW platform with inspection of 50+ file type like .exe, .bat, .com, .dll, .vbs, .js, and .msi	10	Select	0	
56	Anti-virus application must be able to prevent access to malicious websites	10	Select	0	
57	Anti-Virus must be able to scan archive files. Anti-Virus policies must be centrally managed with granular policy configuration and enforcement	10	Select	0	
58	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.	10	Select	0	
59	Management platform should provide autonomous threat prevention security policy.	10	Select	0	
60	Management and Firewall should be two separate dedicated systems.	10	Select	0	
61	NGFW appliances must be managed from a centralized dedicated management system (VM based - dedicated for Third Party Firewall	10	Select	0	
62	Device Management system/Centralize Management systems includes logging, compliance, best practices, reporting and event correlation functionality in the licenses.	10	Select	0	
63	Device Management system/Centralised Management Dashboard should provide the real time health status of all the firewall modules on the dashboard for CPU & memory utilization, state table, total no. of concurrent connections and the connections per second counter. It must provide a security rule hit counter in the security policy.	10	Select	0	
64	Solution should consist of dedicated Management Server (VM Based) & dedicated logging/correlation server (VM based)	10	Select	0	

Third Party Firewall					
S. No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
65	Solution must be able to segment the rule base in a layered structure. Solution must be able to segment the rule base to allow structure flexibility to align with dynamic networks. Support layer sharing within Threat Prevention policy	10	Select	0	
66	The proposed solution must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance	10	Select	0	
67	Solution must have capabilities for multi-domain management and support the concept of global security policy across domains, if needed in future.	10	Select	0	
68	The solution should support Threat Investigation with MITRE-Aligned Insights	10	Select	0	
69	The firewall and management should follow a physical segregation, and firewall should not cease to function when management becomes inaccessible/inactive or gest into failed state. The firewall should continue to function.	10	Select	0	
70	AI-Powered Inline IPS & Threat Prevention				
70.1	A. The IPS engine MUST utilize inline, signature-less Machine Learning (ML) models directly within the data path to detect and block zero-day, polymorphic, and AI-generated exploits in real time (<10ms latency overhead).	10	Select	0	
70.2	B. The solution MUST support local, heuristic-based IPS inspection to detect mutated vulnerability exploits (e.g., AI-crafted variants of known CVEs) without requiring immediate cloud signature lookups.	10	Select	0	
70.3	C. The IPS engine MUST employ AI/ML behavioral analysis to detect and block low-and-slow, evasive Command and Control (C2) traffic and beaconing behavior associated with automated malware.	10	Select	0	
71	Generative AI Application Access Control & Forwarding				
71.1	The firewall solution shall provide application-aware visibility and policy enforcement capabilities for Generative AI, LLM, and AI-powered services	10	Select	0	
71.2	The solution MUST support the ability to block or allow access to specific Generative AI sub-features based on URL or application-aware visibility (e.g., <i>Allow access to chat but completely block HTTP POST/File Upload paths</i> to AI domains).	10	Select	0	
71.3	ICAP / Service Chaining Support: The firewall MUST support ICAP (Internet Content Adaptation Protocol) or standard policy-based routing to seamlessly decrypt and forward outbound Generative AI-destined traffic to the bank's external, third-party DLP solution for inspection.	10	Select	0	
72	Hardware Architecture & SSL/TLS 1.3 Inspection				
72.1	The appliance MUST feature dedicated hardware acceleration (ASICs or specialized network processors) to ensure that running inline AI/ML IPS inspection and application-aware visibility tracking does not degrade core firewall throughput.	10	Select	0	
72.2	The vendor MUST provide certified performance benchmarks demonstrating sustained SSL/TLS 1.3 decryption throughput with <i>all</i> IPS engines and application control features concurrently enabled.	10	Select	0	
73	AI Log Governance & Compliance				
73.1	For any traffic dropped or flagged by heuristic/ML IPS models, the firewall management platform MUST generate detailed contextual logs explaining the nature of the anomaly to satisfy banking compliance audits (e.g., DORA, NIST).	10	Select	0	
73.2	The vendor MUST contractually guarantee that any decrypted network metadata or telemetry forwarded to the vendor's cloud threat intelligence infrastructure will not be used to train multi-tenant or public AI models.	10	Select	0	
74	Post-Quantum Cryptography (PQC) Technical Specifications				
74.1	Crypto-Agility Architecture: The firewall hardware and operating system MUST demonstrate complete "crypto-agility," allowing for modular software or firmware updates to swap, rotate, or deprecate cryptographic algorithms without requiring a physical hardware or appliance replacement.	10	Select	0	
74.2	Post-Quantum VPN Support (RFC 9370): For site-to-site and remote-access VPNs, the firewall MUST support IKEv2 hybrid key exchanges that combine classical algorithms (e.g., ECDH) with NIST-standardized Post-Quantum Cryptography (PQC) Key Encapsulation Mechanisms (KEM), specifically ML-KEM (FIPS 203).	10	Select	0	
74.3	PQC Digital Signatures: The IPS and firewall authentication mechanisms MUST natively support—or have a committed product roadmap to support—NIST-standardized post-quantum signature algorithms, including ML-DSA (FIPS 204) and SLH-DSA (FIPS 205), for secure certificate handling.	10	Select	0	
74.4	PQC TLS 1.3 Inspection & Detection: The firewall's decryption engine MUST be capable of parsing TLS 1.3 ClientHello extensions to detect, log, and control hybrid post-quantum cipher suites passing through the perimeter, ensuring deep visibility into enterprise PQC traffic.	10	Select	0	

Third Party Firewall					
S. No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
74.5	Hardware Sizing for Large PQC Keys: The vendor MUST provide certified performance impact data demonstrating that the appliance’s compute architecture can handle the significantly increased packet sizes, public key lengths, and mathematical overhead required by lattice-based PQC algorithms without dropping active banking sessions or degrading latency.	10	Select	0	
70	The solution should support Threat Investigation with MITRE-Aligned Insights	10	Select	0	
Total		850		0	

Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

Email Security					
S.No	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	The proposed on-premise solution should be purpose built dedicated Email Security appliance with hardened OS , that provides enterprise MTA (Message Transfer Agent) capabilities SMTP/SMTP-TLS, Antimalware, BEC/CEO fraud attack prevention, social engineering attack protection, ransomware, unknown malware threats using Sandboxing technique and anti-phishing." All the Components and Licenses is to be proposed from day 1 for hardware and it's relative components as per the Deployment	10	Select	0	
2	The proposed solution must: a) Support both incoming and outgoing messages protection b) Support deployment modes like MTA, BCC, SPAN/TAP modes c) Analyze, process and inspect at least 400,000 emails/day d) The solution must be capable of analyzing and cleaning 100+ different file types including windows executables, scripts, Java, office, office with macros, Pdf,simage/jpeg files, vbs, dll, lnk and compressed file of all types.	10	Select	0	
3	The proposed solution should scans for suspicious behavior in several parts of each email transmission, including the email header, subject line, body, attachments, and the SMTP protocol information to detect suspicious behavior related to social engineering attacks in email messages and must analyze emails for various parameters like intention, financial implication, urgency, mail header, domain information for finding out fraud.	10	Select	0	
4	The Proposed solution should be able to detect and inspect the URLs in mail body, email subject and embedded in the attachments in MS office and PDF Attachments. Solution shall be able to detect known bad URLs without relying on Sandbox analysis.	10	Select	0	
5	The proposed solution should support advanced detection technology to discover targeted threats in email messages, including spear-phishing and social engineering attacks. a. Reputation and heuristic technologies catch unknown threats and document exploits b. File hash analysis blocks unsafe files and applications c. Detects threats hidden in password-protected files d. Machine learning technology to detect emerging unknown threats	10	Select	0	
6	The proposed solution should use Multiple techniques to look for known and potential exploits to the intended office application and analyze macros. The Proposed solution should be able to detect true file types and also have capabilities to detect ransomware using sandbox.	10	Select	0	
7	The proposed solution should: a. Detect suspicious behavior related to social engineering attacks in email messages	10	Select	0	
8	Email Security solution should have multiple configuration option to define the source/downstream and the upstream/next hop of the email chain/SMTP to ensure that it only accepts traffic from defined sources.	10	Select	0	
9	There should be an option to create separate policies for incoming and outgoing emails with separate security controls.	10	Select	0	
10	The Proposed Solution should support authentication mechanisms like DKIM, DMARC & SPF checks to detect & fight against techniques used in mail phishing & spoofing.	10	Select	0	
11	The Proposed solution should support importing of custom passwords for archive files. The solution should support predefined passwords for scanning archive files. In case the password is part of the email Body, the proposed solution should read the password from mail body to open the attachment	10	Select	0	
12	The Proposed solution should be able to Deliver the email message to the recipient after replacing the suspicious attachments with a text file and tag the email message subject with a string to notify the recipient, should be able to pass and tag the email message OR The Proposed solution should be able to Deliver the email message to the recipient after removing the suspicious attachments and tag the email message subject with a string to notify the recipient, should be able to pass and tag the email message	10	Select	0	
13	Solution should support identification of mismatches in display names and email addresses	10	Select	0	
14	The solution should check for behavior analysis through machine learning capabilities to detect attacks impersonating users	10	Select	0	
15	Solution should support displaying warning banners and blocking/quarantine of emails from similar-looking domains"	10	Select	0	
16	The Proposed solution should have: a. Capability to make policy exceptions for safe senders, recipients, and X-header content, files and URL's b. Threat type classifications such as targeted malware, malware, malicious URL, suspicious file, suspicious URL, phishing, content violation etc.	10	Select	0	

Email Security					
S.No	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
17	The Proposed solution should have customizable dashboards for Attack Sources, High-Risk Messages, Detected Messages, Top Attack Sources, Quarantined Messages, Top Attachment Names, Top Attachment Types, Top Email Subjects, Processed Messages by Risk, Processing Volume, Delivery Queue, Hardware Status, sandbox Queue, Suspicious Objects from Sandbox, Email Messages with Advanced Threats	10	Select	0	
18	The Proposed Solution should able to detect Coin Miner Malware detection. Solution should support archiving feature to send copies of messages to external servers for archiving purposes. It should support manual email message submission in" .eml" format for analysis purpose.	10	Select	0	
19	Solution should have DLP capability to control files or data that requires protection from unauthorized transmission and Data Loss Prevention comes with a set of predefined & customized expressions.	10	Select	0	
20	The proposed Solution must have following features to effectively block senders of spam messages at the IP address or sender email address level: Approved and blocked senders lists , Email Reputation Services (ERS) , Directory harvest attack (DHA) protection, SMTP traffic throttling.	10	Select	0	
21	Proposed OEM should use multi layered scans/techniques to mitigate threats and should be a combination of both static as well as heuristic scanning. Solution should support Pre-Execution Machine Learning scanning feature which looks at static and heuristic file features to predict maliciousness in mail & attachment in the mail"	10	Select	0	
22	Proposed solution should have below Threat Emulation & Sandbox capability: a. At least 20 or more CUSTOM sandboxing virtual instances or emulation based sandbox on the same email security appliance to provide consolidated inspection of emails b. Custom languages supported. c. Evasive Techniques detection to prevent attackers from evading Sandboxing technology. d. Solution must be capable to sandbox file and URLs(as per the network connectivity) e. Emulation based sandbox or Support 32-bit / 64-bit Windows 2012 and above server sandbox images, and should allow at least two types of sandbox images for virtual analysis. f. Solution must support YARA Rules for malware identification g. Sandboxing should perform attachment/file analysis and ensure the detection of advanced threats. Following features must be included in the solution: Engines -Static/Dynamic Analysis, Anti-security and self preservation , Deception and social engineering, File drop, download, sharing, or replication, redirection, or data theft, Malformed, defective, or with known malware traits, Process, service, or memory object change, Rootkit, cloaking, suspicious network or messaging activity, pattern based, reputation, Heuristics & Machine learning"	10	Select	0	
23	The sandbox solution must support these file formats: .svg, .swf, .mov, .htm, .html, .xht, .xhtml, .mht, .mhtml, .shtml, .jar, .class, .doc, .dot, .docx, .dotx, .pps, .ppsx, .ppt, .pptx, .pub, .xla, .xls, .xlsx, .xlt, .xlm, .cell, .xml, .xlsb, .xltx, .hwp, .hwp, .jtd, .gul, .msg, .slk, .iqy, .csv, .odp, .ods, .odt, .docm, .dotm, .potm, .ppam, .ppsm, .pptm, .xlam, .xlsm, .xltm, .chm, .lnk, .rtf, .one, .pdf, .bat, .cmd, .js, .jse, .hta, .ps1, .vbe, .vbs, .wsf, .url, .sh, .com, .cpl, .crt, .dll, .drv, .elf, .exe, .ocx, .scr, .sys, .7z, .ace, .alz, .amg, .arj, .hqx, .bz2, .bzip2, .cab, .cpio, .cpgz, .egg, .gzip, .gz, .ics, .lha, .lharc, .lzh, .eml, .email, .msg, .rar, .sit, .sitx, .tar, .tgz, .tnef, .winmail.dat, .win.dat, .iso, .uue, .vcs, .xz, .zip	10	Select	0	
24	The proposed solution should support adding exception of suspicious objects for IP, URL, Domain and hash value.	10	Select	0	
25	The proposed Solution should be able to generate critical alerts like Service interruption , Relay MTAs connection issues , sandbox issues and important alerts like long queue, High CPU, high memory, low disk space, account locking, component update etc.	10	Select	0	
26	"The Proposed solution should be able to Deliver the email message to the recipient after replacing the suspicious attachments with a text file and tag the email message subject with a string to notify the recipient, should be able to pass and tag the email message OR The Proposed solution should be able to Deliver the email message to the recipient after removing the suspicious attachments and tag the email message subject with a string to notify the recipient, should be able to pass and tag the email message"	10	Select	0	
27	The proposed solution should have an option of backup/restore of configuration using import/export that in case of failure, the last configuration can be restored.	10	Select	0	
28	The proposed solution should support querying logs using time based filters and provide option to Track any email message that passed through email security solution. The proposed solution should have an option to generate reports on demand or set a daily, weekly, or monthly schedule.	10	Select	0	

Email Security					
S.No	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
29	It should be able to centrally manage and deploy product updates including patches, hotfixes, and firmware upgraded and should be able to centrally manage and deploy sandbox image update to managed products	10	Select	0	
30	Solution must provide granular log search filters for users to define their own search criteria also solution central management should include various methods of sharing threat intelligence data with other products or services including TAXII / Web services.	10	Select	0	
31	The proposed Solution should be able to generate critical alerts like Service interruption , Relay MTAs connection issues , sandbox issues and important alerts like long queue, High CPU, high memory, low disk space, account locking, component update etc.	10	Select	0	
32	Proposed solution should have CDR (Content Disarm and Reconstruction) capabilities to remove malicious/active content from Microsoft files and PDF files	10	Select	0	
33	Solution should support identification of mismatches in display names and email addresses.	10	Select	0	
34	solution shall detect and neutralise AI-generated threats including LLM-assisted phishing, AI-synthesised BEC narratives, and machine-generated malware engineered to evade signature and heuristic controls.	10	Select	0	
35	Solution should support displaying warning banners and blocking/quarantine of emails from similar-looking domains	10	Select	0	
		350		0	

Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product