The Nainital Bank Limited
Information Security Cell, Railway Bazar, Haldwani, 263139
Ph.: 05946-251550 E-Mail: ciso.office@nainitalbank.co.in

Sealed Quotation for conducting Firewall Rule Review & Configuration-Hardening Review

A. OBJECTIVE: The primary objective of this engagement is to identify and address vulnerabilities within The Nainital Bank's Mobile Application, ensuring its resilience against potential cyber threats and unauthorized access. The comprehensive VAPT and Application Security Assessment will help in identifying security gaps, weaknesses, and potential entry points for malicious actors.

ELIGIBILITY CRITERIA

Sr	Eligibility Criteria	Support Documents to be submitted
1	The vendor should be Company/Firm/ Organization registered in India	Certificate of Incorporation & Commencement of Business (whichever applicable) should be submitted
2	The vendor should have a valid CERT-In empanelment.	Cert-in empanelment document.
3	The vendor should not be banned/blacklisted/ debarred by any Bank/PSU/GOI Department/Indian Financial Institute	An undertaking letter to be enclosed by vendor
4	Vendor Should have conducted Firewall Rule Review & Configuration-Hardening Review for at least two Banks in last 4 years (other than cooperative banks)	Copy of purchase order and Client certificate.
5	Vendor should have at least 4 years' experience in offering Information Security Services such as Security assessment, defining security policies procedures & baselines, Risk Assessment, security consulting assignments to clients in India.	Copy of relevant certificate/ purchase order and Client certificate.

Last Date of Submission of Quotation:
The last date for submission of sealed Quotation (through courier / by hand) is 05-June-2025 at below address-

Chief Information Security Officer
Information Security Cell
The Nainital Bank Limited
Railway Bazar, Haldwani,
District Nainital, Uttarakhand-263139

For any clarifications, please contact **Mr. Pankaj Adhikari** at +91 9456108588.

B. COMMERCIAL FORMAT: Annexure II

C. FREQUENCY: The frequency for conducting Firewall Rule Review & Configuration-Hardening Review would be one time. However, the Bank at its own discretion can change the frequency.

D. RIGHT TO REJECT: Bank reserves the absolute and unconditional right to reject the response to this inquiry if it is not in accordance with its requirements and no further correspondence will be entertained by the Bank in the matter.

ANNEXURE I - SCOPE OF WORK

Firewall Configuration and Hardening Review

The Firewall Configuration and Hardening Review should cover the assessment of firewall security policies, configuration settings, rule base analysis, and compliance with industry best practices and regulatory standards. Upon completion of the review and submission of the report, the Bank may, at its discretion, request in writing for Compliance verification on closure of observations.

Review Activities:
The Firewall Configuration and Hardening Review should be comprehensive and include, but not be limited to, the following activities:

1. Firewall Rule Base Review
   a. Review of firewall rules to ensure they follow the principle of least privilege.
   b. Identification of redundant, shadowed, or overly permissive rules.
   c. Verification of network segmentation and access control policies.

2. Configuration and Hardening Review
   a. Assessment of firewall operating system and firmware versions for vulnerabilities.
   b. Evaluation of management interface security and access controls.
   c. Analysis of logging and monitoring settings.
   d. Review of authentication mechanisms (e.g., multi-factor authentication, admin access controls).

3. Security Policy Assessment
   a. Verification of firewall policies against industry standards (e.g., NIST, CIS, ISO 27001).
   b. Review of IPS/IDS configurations and anomaly detection settings.
   c. Ensuring appropriate NAT (Network Address Translation) configurations.

4. Threat and Vulnerability Analysis
   a. Identification of potential misconfigurations leading to security gaps.
   b. Testing firewall resilience against common attack vectors (e.g., spoofing, DoS/DDoS, unauthorized access attempts).
   c. Verification of proper response mechanisms for detected threats.

5. Network Architecture Review
   a. Assessment of DMZ (Demilitarized Zone) security.
   b. Review of VPN configurations and remote access security controls.
   c. Ensuring proper implementation of network segmentation.

6. Compliance and Best Practices Evaluation
   a. Validation of adherence to regulatory and compliance standards such as PCI-DSS, GDPR, and RBI guidelines.
   b. Ensuring firewalls meet organizational security policies and audit requirements.
   c. Recommendations for improvement and remediation actions.

Firewalls Covered Under This Review:

Sr	Firewall Vendor	Device Name	Model	Serial Number	OS Version
	Cisco	NNTB-DC-CORE-FW1	Firepower 2140 Threat Defense	JMX2452Z01P	7.1.0.1
	Cisco	NNTB-DC-CORE-FW2	Firepower 2140 Threat Defense	JMX2452Z01N	7.1.0.1
	FortiGate	NNTB-INT-FW1	Fortigate-601E	FG6H1ETB20906190	v7.2.7 build 1577
	FortiGate	NNTB-INT-FW2	Fortigate-601E	FG6H1ETB20906144	v7.2.7 build 1577
	Cisco	NNTB-DR-CORE-FW1	Firepower 2140 Threat Defense	JMX2503X26C	7.1.0.1
	Cisco	NNTB-DR-CORE-FW2	Firepower 2140 Threat Defense	NA	7.1.0.1
	FortiGate	NNTB-INT-DR-FW1	Fortigate-601E	FG6H1ETB20906425	v7.2.7 build 1577
	FortiGate	NNTB-INT-DR-FW2	Fortigate-601E	FG6H1ETB20906207	v7.2.7 build 1577

Firewall Rule Review & Configuration-Hardening Review Schedule: Vendor has to undertake Firewall Rule Review & Configuration-Hardening Review in scheduled manner as described below:

- Conduct Firewall Rule Review & Configuration-Hardening Review as per the scope, Evaluation & Submission of Preliminary Reports of findings and discussions on the finding.
- Submission of Final Report.

1. Conduct Firewall Rule Review & Configuration-Hardening Review as per the scope defined in annexure I without disturbing operations
    a. The Bank will call upon the successful Bidder/Vendor, on placement of the order, to carry out demonstration and/or walkthrough, and/or presentation and demonstration of all or specific aspects of the Firewall Rule Review & Configuration-Hardening Review activity.
    b. Firewall Rule Review & Configuration-Hardening Review schedule to be provided 5 working days prior to the start of activity along with the team member details with technical qualification and experience. A dedicated Project Manager shall be nominated, who will be the single point of contact for Firewall Rule Review & Configuration-Hardening Review Activity for Nainital Bank.
    c. Consultant shall have a walkthrough meeting with the concerned application team and under the process flow and architecture of the application including its modules, interfaces and user roles.
    d. Consultant shall raise the prerequisites with the Bank's team and shall start the work on fulfilment of prerequisites.
    e. Execute Vulnerability Assessment and Penetration testing of Bank's IT Infrastructure and Applications as per the scope on the written permission of the Bank and in the presence of Bank's Officials.
    f. In case of compliance verification, verifying the observations for closure of findings.

2. Detailing the Security Gaps
    a. Detailing the System setup used, and the tests conducted in assessment.
    b. Critical vulnerabilities observed during Firewall Rule Review & Configuration-Hardening Review along with recommendations should be immediately brought to the notice of Bank without waiting for the completion of Firewall Rule Review & Configuration-Hardening Review. On closure of critical vulnerability, verification of closure shall have to be performed.
    c. Analysis of the findings and Document the security gaps i.e. vulnerability, security flaws, loopholes, threats, etc. observed during the course of the Firewall Rule Review & Configuration-Hardening Review activity as per the scope of work.
    d. Document recommendations and solutions for addressing these security gaps and categorize the identified security gaps based on their criticality.
    e. Chart a roadmap for the Bank to ensure compliance and address these security gaps.

3. Addressing the Security Gaps
    a. Recommend Actionable fixes for systems vulnerabilities in design or otherwise for application systems and network infrastructure. If recommendations for Risk Mitigation /Removal could not be implemented as suggested, alternate solutions to be provided.
    b. Suggest changes/modifications in the Security Policies implemented along with Security Architecture including Network and Applications of the Bank to address the same.
    c. The Draft report of the Firewall Rule Review & Configuration-Hardening Review findings should be submitted to the Bank for Management comment within 15 days of start of audit.

4. Submission of Final Reports
    a. The Service Provider should submit the final report of Firewall Rule Review & Configuration-Hardening Review findings as per the report format mentioned in Deliverables. All the Firewall Rule Review & Configuration-Hardening Review reports submitted should be signed by technically qualified persons and he/she should take ownership of document, and he/she is responsible and accountable for the document/report submitted to the Bank.
    b. The final report has to be submitted within -1- months of submission of the initial draft report.
    c. Service provider will also submit the Executive Summary Report of the Bank's Internet facing environment.

5. Acceptance of the Report
    a. The Report shall be accepted on complying with the formats of Firewall Rule Review & Configuration-Hardening Review Report as mentioned in the Scope and acceptance of the audit findings.
6. Deliverables:

a. The deliverables for Firewall Rule Review & Configuration-Hardening Review activity are as follows:
   i. Execution of Vulnerability Assessment and Penetration Testing and Application Security Testing for the identified network devices, security devices, servers, applications, websites, interfaces (part of application) etc. as per the Scope mentioned in this scope and Analysis of the findings and guidance for resolution of the same
   ii. Verification of closure of critical vulnerability.
   iii. Perform compliance verification of closure of findings.
   iv. Draft Firewall Rule Review & Configuration-Hardening Review Report followed by final report.
   v. Compliance verification

b. The Firewall Rule Review & Configuration-Hardening Review Report should contain the following: -
   i. Identification of Auditee (Address & contact information)
   ii. Dates and Locations of Firewall Rule Review & Configuration-Hardening Review
   iii. Terms of reference
   iv. Standards followed including confirmation of testing as per International Best practices and OWASP Web/Mobile application security guidelines.
   v. Summary of audit findings including identification tests, tools used, and results of tests performed (like vulnerability assessment, penetration testing, application security assessment, website assessment, etc.)
      1. Tools used and methodology employed
      2. Positive security aspects identified
      3. List of vulnerabilities identified
      4. Description of vulnerability
      5. Risk rating or severity of vulnerability
      6. Category of Risk: Very High (Critical) / High / Medium / Low
      7. Test cases used for assessing the vulnerabilities
      8. Illustration of the test cases
      9. Applicable screenshots.
   vi. Analysis of vulnerabilities and issues of concern
   vii. Recommendations for corrective action
   viii. Personnel involved in the audit

The Service Provider may further provide any other required information as per the approach adopted by them and which they feel is relevant to the audit process. All the gaps, deficiencies, vulnerabilities observed shall be thoroughly discussed with respective bank officials before finalization of the report.

The Firewall Rule Review & Configuration-Hardening Review Report should comprise the following sub reports: -

Firewall Rule Review & Configuration-Hardening Review Report – Executive Summary: The vendor should submit a report to summarize the Scope, Approach, Findings and recommendations, in a manner suitable for senior management. Vendor will also detail the positive findings (No Gap found) for various tests conducted.

Firewall Rule Review & Configuration-Hardening Review Report – Core Findings along with Risk Analysis: The vendor should submit a report bringing out the core findings of the Firewall Rule Review & Configuration-Hardening Review conducted for network devices, security devices, servers and websites.

Firewall Rule Review & Configuration-Hardening Review Report – Detailed Findings/Checklists: The detailed findings of the Firewall Rule Review & Configuration-Hardening Review would be brought out in this report which will cover in details all aspects viz. identification of vulnerabilities/threats in the systems (specific to equipment's/resources indicating name and IP address of the equipment with Office and Department name), identifications of threat sources, identification of Risk, Identification of inherent weaknesses, Servers/Resources affected with IP Addresses etc. Report should classify the observations into Critical /Non-Critical category and asses the category of Risk Implication as Very High (Critical) /High/Medium/Low Risk based on the impact. The various checklist formats, designed and used for conducting the Firewall Rule Review & Configuration-Hardening Review activity as per the scope, should also be included in the report separately for Servers (different for different OS), application, Network equipment's, security equipment's etc., so that they provide minimum domain wise baseline security standard /practices to achieve a reasonably secure IT environment for technologies deployed by the Bank. The Reports should be substantiated with the help of snap shots/evidence /documents etc. from where the observations were made.

Firewall Rule Review & Configuration-Hardening Review Report – In Depth Analysis of findings /Corrective Measures & Recommendations along with Risk Analysis: - The findings of the entire Firewall Rule Review & Configuration-Hardening Review Process should be critically analyzed and controls should be suggested as corrective /preventive measures for strengthening / safeguarding the IT assets of the Bank against existing and future threats in the short /long term. Report should contain suggestions/recommendations for improvement in the systems wherever required. If recommendations for Risk Mitigation /Removal could not be implemented as suggested, alternate solutions to be provided. Also, if the formal procedures are not in place for any activity, evaluate the process & the associated risks and give recommendations for improvement as per the best practices. Separate reports should be provided for common infrastructure assets and Applications.

Documentation Format

- All documents will be handed over in soft copy format.
- Soft copies of all the documents properly encrypted in MS Word /MS Excel /PDF format also to be submitted in
- Soft copies along with the hard copies.
- All documents shall be in plain English.

Project Timelines:

The vendor shall furnish a schedule of assessment within -7- days of issuance of Purchase order. Firewall Rule Review & Configuration-Hardening Review schedule has to be mutually agreed by both the parties. In certain situations, Bank may be required to defer the scheduled activity due to non-availability of the production environment for Firewall Rule Review & Configuration-Hardening Review for whatever may be the reason. In such a situation, Firewall Rule Review & Configuration-Hardening Review activity has to be deferred however the same has to be within the overall contract validity period.

Final Firewall Rule Review & Configuration-Hardening Review report has to be submitted within -1- months of issuance of the initial Draft report after considering the Management comments on the Draft report.

ANNEXURE II - COMMERCIAL

Sr	Service Type	Firewall Model	Total Instances	Commercials (Price) per Instance	Commercials (Total)
1	Firewall Configuration and Hardening Review	Cisco Firepower 2140 Threat Defense	4		
2	Firewall Configuration and Hardening Review	Fortigate-601E	4		
			Grand- Total		
Note: Cost shall include all travelling, lodging, and other expenses.					

Note:
Price: (should be Exclusive of Taxes) (Price should include Travelling, Lodging and other expenses)

Selection Criteria –
The Vendor should be qualified in all technical aspects required for the banking security standards.
The least accumulative Total in all received quotations will be considered as L1.