TENDER DOCUMENT

FOR

THE WORK OF SUPPLY, INSTALLATION, TESTING, COMMISSIONING AND MAINTENANCE OF NEXT GENERATION FIREWALL (NGFW)

IN

NCDC, NEW DELHI

NCDC

Assisting Cooperatives. Always!

राष्ट्रीय सहकारी विकास निगम

4, सिरी इंस्टीट्यूशनल एरिया, हौज़ खास, नई दिल्ली-110016

National Cooperative Development Corporation

4, Siri Institutional Area, Hauz Khas New Delhi- 110016

वेबसाईट: http://www.ncdc.in

निविदा की लागत - मुफ्त

सूचकांक
INDEX

National Cooperative Development Corporation
(General Administration Division)

No. NCDC: 2-1/2020-Genl. **Date: 26.05.2020**

TENDER NOTICE

National Cooperative Development Corporation (NCDC), 4, Siri Institutional Area, Hauz Khas, New Delhi – 110016 invites sealed tender from well-established firms / agencies having relevant experience, in two bids format (Technical & Financial bid) for the work of Supply, Installation, Testing, Commissioning and Maintenance of NEXT GENERATION FIREWALL in NCDC, Head Office from Original Equipment's Manufacturer (OEM) or its authorized vendors capable of carrying out the above work and having already carried out similar work in reputed organizations. **The prospective bidder shall fulfill the following mandatory eligibility criteria (attach documentary evidence for all the criteria):**

i. **The Firms/ agencies should have minimum annual turnover of ₹250 Lakhs in each of the last 3 consecutive financial years (2017-18, 2018-19 & 2019-20).** (Copy of Financial Statements viz trading account, profit & loss account, balance sheet duly signed by CA be enclosed).

ii. The Firms/ agencies must have experience of having successfully completed as per below in Government Departments / Public Sector Undertakings / Autonomous Bodies / Financial Institutions and other reputed Private Firms during the last 3 years prior to 31.03.2020:

Atleast **three** similar job each costing not less than 21.24 lakhs

Or

Atleast **two** similar job each costing not less than 31.86 lakhs

Or

Atleast **one** similar job each costing not less than 42.48 lakhs

iii. **The OEM of NGFW must be in the Leader's quadrant of the Enterprise Firewalls Gartner Magic Quadrant for consecutive last 5 years.**

iv. The bidder should be a registered company in India as per applicable statute and be in existence for at least 3 years. Should have valid PAN and GST registration.

v. The firm/ company should have its own office in Delhi/ NCR region.

2. Prospective Bidder shall submit their offers in the bidding document specified for the purpose at National Cooperative Development Corporation (NCDC), 4-Siri Institutional Area, Hauz Khas, New Delhi-110016, 4th Floor, West Wing from 11.00 AM to 3.00 P.M. on all working days (Monday to Friday). The bid document is also available free of cost on NCDC's website www.ncdc.in. Each page of the tender document should be signed by the bidder before submission.
3. The bidding document is required to be submitted in two parts viz. 'Technical Bid' and 'Financial Bid' in separate sealed envelopes put into one bigger envelop super scribed as **"Tender for the work of Supply, Installation, Testing, Commissioning and Maintenance of NGFW in NCDC, Head Office".**
4. The offer (duly filled in & signed), in sealed covers, duly marked "Supply, Installation, Testing, Commissioning and Maintenance of NGFW in NCDC, Head Office" must reach the office of Executive Director (Genl. Admin.), NCDC **by 3.00 PM on 18/06/2020** and the Technical Bids shall be opened at 3:30 PM on same day in the office of Executive Director (GA) by tender committee. Bidders or there authorized representative may present at the meeting held for opening of Pre-qualification bid/ Technical Bid.
5. The tender should be accompanied with earnest money deposit (EMD) amounting to **₹1,50,000/- (Rupees One lakh fifty thousand only)** in the form of demand draft in favor of **National Cooperative Development Corporation payable at New Delhi.** The tenders without EMD shall be rejected.
6. The price bid of only those firms shall be opened whose technical bid are found to be acceptable as per eligibility criteria mentioned in the tender document. The time and date of opening of price bid shall be fixed and intimated to the eligible firms separately.
7. The Corporation reserves the right to accept any or reject all the tenders without assigning any reasons thereof.

(Krishan Kumar)
Executive Director (Genl. Admin.)

Copy To:-

1. Chief Director (MIS): With request to upload tender on NCDC website & CPP Portal of Govt. of India.

तकनीकी बोली

Technical Bid

Annexure-I

PARTICULARS OF THE FIRM

1.	Name of the firm (OEM/ authorized vendor)		
2.	Office address		
3.	Telephone No.		
4.	Mobile No.		
5.	E-mail address		
6.	Fax No.		
7.	Whether the firm proprietary/ partnership		
8.	Name & Address of partner, in case of partnership firm please enclose a copy of partnership deed/power of attorney		
9.	Date of establishment of the firm :		
10.	Annual turnover for financial years (Please attach copy(s) of audited financial statement, accounts and balance sheets for the last three years 2017-18 to 2019-20)	FY	Annual turnover (in ₹.)
		2019-20	
		2018-19	
		2017-18	
11.	Particulars of DD/Banker's Cheque towards EMD of ₹1,50,000/-		
12.	Whether OEM of NGFW in Leader's quadrant of the Enterprise Firewalls Gartner Magic Quadrant for consecutive last 5 years(Submit the Gartner report for consecutive last 5 years)		
13.	GST no. of the Firm: (photocopy to be enclosed)		
14.	PAN No: (photocopy to be enclosed)		
15.	Contact Details and Address of Firm/ Company's Office in Delhi / NCR		
16.	Any other relevant information.		

Signature of the Bidder/Firm
(Name & Address of the Bidder/Firm with seal)

(Please attach self attested separate sheet/s, if required)

Annexure-II

DETAILS OF EXPERIENCE

(Details of Experience of Similar Works Executed/Awarded During The Last Three Financial Years During The Period 01st April 2017 To 31st March 2020)

Atleast **three** similar job each costing not less than 21.24 lakhs

Or

Atleast **two** similar job each costing not less than 31.86 lakhs

Or

Atleast **one** similar job each costing not less than 42.48 lakhs

S.N.	Name, Address & Contact details of the client	Details of the work/ order	Work award cost	Work award Date	Date of Commissioning	Has NGFW been satisfactory commissioned	Remarks

Note: Please attach copies of work award letters/ performance certificates as proof of above information.

Signature of the Bidder/Firm
(Name & Address of the Bidder/Firm with seal)

(Please attach self attested separate sheet/s, if required)

TERMS & CONDITIONS

1. This Tender is open to all Original Equipment's Manufacturer (OEM) of NGFW and its authorized vendors capable of carrying out the above work and having already carried out similar work in reputed organizations.
2. The OEM of NGFW must be in the Leader's quadrant of the Enterprise Firewalls Gartner Magic Quadrant for consecutive last 5 years.
3. The Firms/ agencies should have minimum annual turnover of ₹250 Lakhs in each of the last 3 consecutive financial years (2017-18, 2018-19 & 2019-20). (Copy of Financial Statements viz trading account, profit & loss account, balance sheet duly signed by CA be enclosed).
4. The Firms/ agencies must have experience of having successfully completed Atleast three similar job each costing not less than 21.24 lakhs or Atleast two similar job each costing not less than 31.86 lakhs or Atleast one similar job each costing not less than 42.48 lakhs in Government Departments / Public Sector Undertakings / Autonomous Bodies / Financial Institutions and other reputed Private Firms during the last 3 years prior to 31.03.2020. The copies of Purchase/ Work Orders/ Satisfactory Completion Certificates are required to be enclosed with the Technical Bid.
5. The bidder should be a registered company in India as per the applicable statute and be in existence for at least 3 years. Company should have a valid GST Registration, PAN Number allotted by the respective authorities. Self-attested copy of company registration certificate, GST, PAN number. Copy of Article of Association and Memorandum of Association are required to be submitted.
6. The envelope 1 containing Technical bid super-scribed as **"Work of Supply, Installation, Testing, Commissioning and Maintenance of NGFW in NCDC, Head Office"** should not contain any price information and should comprise of following along with supporting documents in the below mentioned order:
   i) Earnest Money Deposit of amount **₹1,50,000/-** by Demand Draft drawn in favor of **National Cooperative Development Corporation payable at New Delhi.**
   ii) Technical Bid in the prescribed format as per tender document, duly signed on each page by authorized person with rubber stamp of the firm.
   iii) Particulars of the Firm/ Company in **Annexure 'I' & Annexure 'II'.**
   iv) Compliance with Scope of work as per **Annexure 'III'.**
   v) Compliance of Technical Specifications as per **Annexure 'IV'.**
   vi) Documentary evidences confirming Registration with GST, PAN or any other statutory obligation required to be complied with by the Firm/Company.
   vii) The tender other than in the prescribed form shall not be accepted. Each page of the tender document is required to be signed by the person/ persons submitting the tender in token of his/ her/ their having acquainted himself/ herself /themselves with all the Terms & Conditions.
7. The envelope No.2_super-scribed as **"Financial Bid for the work of Supply, Installation, Testing, Commissioning and Maintenance of NGFW in NCDC, Head Office"** should contain only financial bid. It must give all the relevant price information, (both, in figures & words). The financial offer should not contradict the technical offer in any manner. The price schedule must be filled in completely without any error, cutting or alterations in rates (both in figures & words). The Financial bid of only those Tenderers who will qualify in Technical bid will be opened.
   The Technical Bid Envelope & the Financial Bid Envelope prepared as above are to be kept in a single sealed envelope super scribed with **"Tender for the Work of Supply, Installation, Testing, Commissioning and Maintenance of NGFW in NCDC, Head Office.**
   No Tender will be considered unless & until all the documents are properly signed & stamped and all corrections also signed by the bidder.

8. **Earnest Money Deposit:**
   EMD of ₹1,50,000/- (Rupees One lakh fifty Thousand Only) in the form of Demand Draft/ Banker's Cheque in favor of **"National Cooperative Development Corporation" and payable at New Delhi** has to be submitted along with tender documents, failing which the bid will be rejected. Earnest Money shall be forfeited in the event of any of the following situations:
   a) If the bidder withdraws or amends his tender or increases the rates after deadline for submission of the Tender but before the validity of the tender expires.
   b) On refusal to enter into contract after award.
   c) on failure to furnish the required performance security or
   d) If the work is not commenced on the date of starting the work after the work is awarded.
   e) Once the tender is submitted, no tenderer will be allowed to withdraw the tender. Even if, any tenderer withdraws the tender, E.M.D. of that tenderer will be forfeited in full.
   f) Any error on the part of the tenderer while quoting the rates will not be accepted as an excuse for refusal to execute the order for any or all items, if order is placed on the basis of the quoted rates. For refusal of the order, the E.M.D. of the tenderer will be forfeited in full.
   g) No interest is payable on the EMD under any circumstances and will be returned on completion of tendering process.
9. Bidder should submit certificate/ undertaking to the effect that firm is neither blacklisted by any government department nor any criminal case is registered against the firm. Firm/ Company declared by Central Governments / State Governments/ Public Sectors to be ineligible to participate on account of corrupt, fraudulent or any other unethical business practice shall not be eligible during the period for which such ineligibility is declared. Simultaneously the companies blacklisted by any such Government Department/established Institutions shall also be ineligible for the tender.
10. The firm/ company should have its office in Delhi/NCR region. Contact Details and Address of firm's/company's office to be provided in the tender. Physical verification may be done by NCDC before awarding the contract.
11. The bidder will have to submit a certificate from the manufacturer of NGFW that the spare parts for the supplied product will be available for after sales service for a period of at least 7 years.
12. **EVALUATION OF BIDS:-**
    An Evaluation Committee will evaluate the bids of all the bidders.
    a) To evaluate the Technical Bid, the committee constituted by the Corporation shall examine the documents furnished by the Firm/ Company in the Technical bid.
    b) The Financial Bids of those Bidders only who are technically qualified by the committee will be opened.
13. **CRITERIA OF DISQUALIFICATION**
    a) Failure of any Bidder(s) to provide all of the information / documents required in the bid proposal or any additional information / documents as sought by the Corporation including supporting documents.
    b) Non receipt of Bid proposal on or before due date and time.
    c) Misrepresentation in the Bid proposal
    d) Tender not accompanied with Earnest Money Deposit (EMD).
    e) Incomplete or conditional Bid
    f) Use of unfair means /misrepresentation
    g) Bid found in unsealed envelope, unsigned bids, bids signed by unauthorized person and any unconfirmed material alteration.
    h) Technical Bids containing any price information.
    i) Conditional tenders shall be summarily rejected.
14. NCDC shall have the right to contact and verify bidders' information, references and data submitted in the bid proposal without further reference to the bidder.

15. NCDC reserves the right to accept any or reject all the tenders without assigning any reason whatsoever.
16. After receiving the confirmed offer from NCDC, the Firm/ Company will give his acceptance and execute an agreement on stamp paper of requisite value on prescribed format as per tender document, within 07 days from the date of receiving the confirmed order. In case the Firm/ Company fails to execute the agreement within 10 days as above, the offer for the work is liable to be cancelled and the earnest money shall be forfeited. In such case, the Corporation is free to award the work to the next eligible firm/ company.
17. Any bid received by NCDC after the deadline for submission of bids prescribed will be rejected and/or returned unopened to the Bidder. NCDC shall not be responsible for any postal/transit delays.
18. It will not be permissible for the firm/agencies to which the work is outsourced to further outsource the work.
19. The Bidder shall bear all costs associated with the preparation and submission of its bid and NCDC will in no case be responsible or liable for these costs.
20. The successful bidder shall execute an indemnity bond as per annexure in favor of NCDC.
21. **PENALTY FOR NOT COMPLETING THE WORK IN TIME**
    In case the bidder fails to complete the work within the stipulated time, a penalty @ 0.5% of contract value per week may be imposed on the bidder. The penalty amount, if any, shall be recovered from any amount due for payment to the bidder. However, the penalty shall not exceed 10% of the contract value. Besides, imposing penalty as above, the balance work may be got done from any other agency at the risk and cost of the bidder, after giving a single notice.
22. **EXTENSION OF TIME FOR COMPLETION**
    If the bidder shall desire an extension of time for completion of the work on the ground of his having been unavoidably hindered in its execution or on any other grounds, he shall apply in writing to the Executive Director (GA), with full details within 2 days of the date of the hindrance on account of which he desires such extension as aforesaid. NCDC shall, if in its opinion (which shall be final) reasonable grounds for extension exists, grant such extension of time as may in its opinion be necessary or proper. No compensation shall be payable to the bidder for any extension of time.
23. **Timeline for implementation**
    The successful bidder has to install and commission at NCDC Head office as per the scope of the tender document within 50 days from the date of execution of agreement. All the aspects of safe delivery, installation, commissioning shall be the exclusive responsibility of the Service Provider.

    The successful bidder shall comply with all Local, State & Central Govt. Rules, Regulations, Ordinances and Codes & Law relating to the work or the conduct thereof.
24. **PAYMENT TERMS**

i. No advance payment would be made for the work.
ii. 50% of order value shall be paid after satisfactory delivery of the equipment at site and acknowledgment of physical receipt by the NCDC.
iii. Balance payment of the contract price shall be paid after successful installation and commissioning.

25. **PERFORMANCE SECURITY**
    The successful bidder shall furnish a refundable Performance Security of 10% of the order value in the form of Bank guarantee /Pledge of FDR/ DD in the favor of **"National Cooperative Development Corporation and payable at New Delhi"** valid for a period of 18 months within 10 days of award of contract. If successful bidder fails to comply obligations of contract in that case Performance Security will be forfeited. No interest shall be payable on the performance Security.

26. **PRICE COMPOSITION**

The price to be quoted in financial bid should be only in Indian rupees and inclusive of following:

a. Cost of the items with accessories, etc F.O.R. destination.
b. The price shall be inclusive of all taxes including duties, octroi, GST etc. as applicable.
c. Installation, commissioning and post deployment support for one year.
d. One-year onsite warranty covering all parts, service, and visits to the site.

27. **NO PRICE VARIATIONS**

The financial bid shall be on a fixed price basis. No upward revision in the price will be considered on account of subsequent increase in foreign exchange, customs duty, excise tax, minimum wages etc. However, if there is any reduction in government levies/taxes, during the execution of work, the same shall be passed on to the NCDC.

28. **WARRANTY & MAINTENANCE CLAUSE**

The product will stand for minimum 1 years' warranty against all manufacturing defects. During the warranty period, the bidder shall have to attend to all break-down calls within 24 hours free of cost upto expiry of warranty period of 1 year. In case, the bidder fails to fulfill its commitments during warranty period, the performance bank guarantee shall be revoked.

Bidder has also to provide post deployment support for 1 year after successful installation and testing. The charges towards the same shall be quoted by the bidder in the financial bid, if any.

The repair/ maintenance will be carried out by the bidder at the site of installation of the equipment's and satisfactory certificate will be obtained on the service report from the office.

29. **VALIDITY OF BID:**

The rates shall be valid for a period of four months from the date of submission of tender.

30. **FORCE MAJEURE CLAUSE:**

a) The Firm/Company shall be liable for any delay in execution or failure of their respective obligations under this agreement except for delay caused by occurrence of events beyond control of the Firm/Company, including but not limited to natural calamities, fire, explosions, floods, power shortages, acts of God, hostility, acts of public enemy, wars, riots, strikes, sabotage, order/action or regulations of government, local or other public authorities.
b) In case a Force Majeure situation arises, the Firm/Company shall immediately notify NCDC in writing of such conditions and the cause thereof within two calendar days and prove that the same is beyond his control and is likely to affect completion of the work.
c) Unless otherwise directed by NCDC in writing, the Firm/Company shall continue to perform its obligations under the contract as far as it is reasonably practical, and shall seek all reasonable means for performance not prevented by the Force Majeure event.

31. **ARBITRATION**

In the event of any dispute or disagreement over the interpretation of any of the terms herein above contained or claim of liability, the same will be referred to an arbitrator to be appointed by the Managing Director, NCDC, whose decision shall be final and binding upon both the parties. Such reference shall be deemed to be a submission to arbitration under the Arbitrations and Conciliations Act 1996. The venue of arbitration shall be New Delhi. Subject here to the court in New Delhi shall have exclusive jurisdiction to the exclusion of all other courts.

Signature of the Bidder/Firm
(Name & Address of the Bidder/Firm with seal)

SCOPE OF WORK

In a bid to strengthen IT security of the corporation, NCDC intends to introduce Next Generation Firewall having various security modules /components deployed in High Availability mode (replacing the existing Cyberoam 100iNG UTM) at its DC. The objective of the exercise is the following: -

- The broad scope of work as detailed in this section refers to the hardware, software / licenses and services that is procured through this tender and used for implementing the Next Generation Firewall at the Data Centre, New Delhi. In other words, NCDC intends to procure 2 nos. of appliance based Next Generation Firewalls and get it installed by the successful bidder for securing its network perimeter, detecting and stopping malicious traffic as a preventive control solution. The appliances must be implemented in HA at NCDC, New Delhi.
- Provide complete visibility of Network, all applications including cloud & SaaS, all users and devices including all locations and encrypted traffic;
- Reduce attack surface area by enabling business apps, block 'bad' apps, Limit application functions, limit high risk websites and content and require MFA;
- Prevents all known threats – Malware, C&C, Malicious & Phishing Websites and Bad Domains;
- Detect and prevent new threats – unknown malware, zero-day exploits and custom attack behavior;
- The solution should support the protection of the mobile workforce by extending the Next-Generation Security Platform to all users, regardless of location. It secures traffic by applying the platform's capabilities to: understand application use; associate the traffic with users and devices; and enforce security policies with next-generation technologies. The solution should Inspect and control applications that are encrypted with SSL/TLS/SSH traffic. Stops threats within the encrypted traffic. The solution should be inbuilt or through external devices.
- Provision of all licenses/subscriptions like appliance, management Server, Operating System, Database (if required), up-gradation etc.
- Comprehensive onsite warranty of 3 years for all the hardware/software under the project. Device rules / device policy definition and enforcement on the boxes proposed in this tender. Enable to detect and block sophisticated attacks by enforcing security policies at various levels, prevent unauthorized access or malicious traffic within NCDC's system or in the network, ensure protection from zero day attacks and unknown threats.
- Enable NCDC to ensure that all the IT assets at New Delhi are secure from threats for today, tomorrow and in the future.
- The bidder shall be responsible for Supply, Installation, Configuration, Testing and Commissioning of the solution at NCDC's DC.
- The bidder shall also handle all matters relating to the configuration and operation of the system including but not limited to application, system interfaces, documentation, user manual and training for the successful implementation of the system.
- The bidder should be responsible for de-commissioning of existing Cyberoam 100iNG devices i.e, replacing the existing Cyberoam 100iNG with the new firewall in such a way that there is no impact on business continuity.
- The bidder would ensure installation of the proposed appliance which include migration of policies and configuration of the existing Cyberoam 100iNG device at NCDC.
- The bidder should ensure that the entire activity of supply, installation, commissioning & configuration whether done in a single pass or in phases must be completed within 50 days from the date of execution of agreement under all circumstance.

- The bidder is responsible for migration of existing rule base to the new devices, NATing, creation of rule base before go-live.
- Solutions which are not mature for over 1 year should not be quoted.
- Introduce the proposed firewalls in the network to act as perimeter level firewall.
- Install and configure management, reporting & logging tool to have a centralized and powerful management which should enable NCDC to deploy, view and control all firewall activity through a single pane.
- The proposed firewalls should be able to perform the Link Aggregation function for connectivity from two or more ISPs.
- Enable safe internet use while protecting against threats and malware. Scan for viruses and malware in allowed collaborative applications, protect environments with social media and internet applications.
- Virtual Private Network (VPN) technologies should be part of the solution to provide resilient and flexible site-to-site, client to site connectivity. Should have management tools to deploy, configure and operate the VPNs.
- Should have ability to manage security environment through intuitive graphical interface which should provide views, details and reports on security health through a comprehensive, centralized security dashboard.
- All the equipment (hardware, software) supplied as part of solution should be IPv6 ready from day one and should support all the protocols.
- Migration from existing Cyberoam 100iNG appliance to proposed NGFW, implementation, testing, commissioning, maintenance including post deployment support for a period of one year from the date of commissioning of two nos. of NGFW in NCDC

Time schedule: The bidder will have to provide install, configure and test NGFW and will be responsible for making system operational within 50 days from the date of execution of agreement.

The tenderers in their own interest before submitting their bids may survey the NCDC premises where the project has to be executed and satisfy themselves that they have the necessary Technical know-how and Man/Material support to complete the work within the stipulated time frame.

Signature of the Bidder/Firm
(Name & Address of the Bidder/Firm with seal)

ANNEXURE – IV

TECHNICAL SPECIFICATIONS

The proposed Next Generation Firewall Solution shall be able to:

I. Provide complete visibility of Network, all applications (including cloud & SaaS), all users and devices (including all locations) and encrypted traffic;
II. Reduce attack surface area by enabling business apps, block 'bad' apps, Limit application functions, limit high risk websites and content and require MFA;
III. Prevents all known threats – Malware, C&C, Malicious & Phishing Websites and Bad Domains;
IV. Detect and prevent new threats – unknown malware, zero-day exploits and custom attack behavior;
V. The solution should support the protection of the mobile workforce by extending the Next-Generation Security Platform to all users, regardless of location. It secures traffic by applying the platform's capabilities to: understand application use; associate the traffic with users and devices; and enforce security policies with next-generation technologies. The solution should Inspect and control applications that are encrypted with SSL/TLS/SSH traffic. Stops threats within the encrypted traffic. The solution should be inbuilt or through external devices.

Detailed Specification:

Type	**Next Generation Enterprise Firewall**
Model	Should be mentioned
3rd Party Test Certification	The proposed vendor must have a "Recommended" rating with min 99% Evasion proof capability and min 97.5% Security Effectiveness as per 2019 NSS Labs Next Generation Firewall Test Report.
	The proposed vendor must be in the Leader's quadrant of the Enterprise Firewalls Gartner Magic Quadrant for consecutive 5 years
Equipment Test Certification	NEBS Level 3, FCC Class A, CE Class A, VCCI Class A, cTUVus, CB
No of Units	Two Unit in HA for DC
Form factor	Modular or Fixed
Architecture	The NGFW architecture should have Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc.) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc.). Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats.
	Proposed NGFW appliances must have 16 GB RAM
	Proposed NGFW appliances must have a minimum 7 CPU Cores (Physical). Virtual core count will not be accepted
Storage	Minimum storage with 240 GB SSD
Power	200 W power supply (45 W)

Interface Requirement	Should have 8 x 1G Copper Interface support
	Should have 4 x1G SFP slots available from Day-1
	Should have Dedicated HA ports in addition to requested data ports
Performance Capacity	Next Gen Firewall application throughput – 1.5 Gbps
	Next Gen Threat prevention throughput – 750 Mbps
	Minimum IPsec VPN throughput – 1 Gbps
	Minimum Client to Site VPN tunnels (SSL, IPSec, and IKE with XAUTH) – 1000. Should have support of upto 2000 site to site IPSEC VPN from day-1.
	Minimum concurrent SSL decryption sessions – 12,500. This should be substantiated with documents from public website or testing/R&D report data. Declaration on letterhead will not be accepted.
	Minimum New sessions per second – 8,000 on HTTP traffic
	Concurrent Connections per second with Layer 7 inspection enabled – 1,25,000
High Availability	Active/Active, Active/Passive
Application Control Throughput	A Minimum NG Firewall application throughput in real world/production environment (by enabling and measured with application ID/AVC, user-ID/Agent-ID utilizing 64KB HTTP transactions and traffic mix such as HTTPS, SMTP and other protocols and logging enabled) - 1.5 Gbps. The bidder shall submit the performance test report from the Global Product Engineering department / Global Testing Department/ Global POC team of OEM to certify the mentioned performance.
Total Threat Protection Throughput	Minimum NG Threat prevention throughput in real world/production environment (by enabling and measured with Application-ID /AVC, User-ID/Agent-ID, NGIPS, Anti-Virus, Anti-Spyware, Anti-Bot, Zero-day attacks and all other security threat prevention features enabled with 64KB HTTP transactions and traffic mix such as HTTPS, SMTP and other protocols and logging enabled) - 750 Mbps. The bidder shall submit the performance test report from the Global Product Engineering department / Global Testing Department/ Global POC team of OEM to certify the mentioned performance.
Interface Operation Mode	The proposed firewall shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in: - Tap Mode - Transparent mode (IPS Mode) - Layer 2 - Layer 3 Should be able operate mix of multiple modes
Next Generation Firewall Features	The proposed firewall shall have network traffic classification which identifies applications across all ports irrespective of port/ protocol/ evasive tactic.
	The proposed firewall shall be able to handle (alert, block or allow) unknown/unidentified applications like unknown UDP & TCP
	The proposed firewall shall be able to create custom application signatures and categories using the inline packet capture feature of the

	firewall without any third-party tool or technical support.
	The proposed firewall shall be able to implement Zones, IP address, Port numbers, User-id, Application-id and threat protection profile under the same firewall rule or the policy configuration
	The firewall must support creation of policy based on wildcard addresses to match multiple objects for ease of deployment
	The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application based on the content.
	The proposed firewall shall be able to protect the user from the malicious content upload or download by application such as Facebook chat or file sharing by enforcing the total threat protection for known and unknown malicious content such as viruses, malwares or bad URLs.
	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy) and inbound connection. The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections
	The proposed firewall shall be able to identify port-based rules/policies so the admin / security team can convert them to application-based whitelist rules or add applications to existing rules without compromising application availability.
	The proposed firewall shall be able identifies rules configured with unused applications and prioritize which rules to migrate or clean up first
	The proposed firewall shall be able restrict application traffic to its default ports to prevent evasive applications from running on non-standard ports.
	Firewall must have inbuilt Automatic policy optimization to identify port-protocol based policies and convert the same into true application based policies. For
	example-Firewall is configured with Security policy to allow port 80/443 and multiple applications (Facebook/Rapidshare etc.) traffic going through the same policy, then the firewall should automatically identify those risky applications and help to add more application specific security policies which might be using the same ports (80/443). This will help us to tighten the application flow control and reduce the attack surface area.
	The firewall must have the capability to create DOS prevention policy to prevent against DOS attacks on per zone basis (outbound to inbound, inbound to inbound and inbound to outbound) and ability to create and define DOS policy based on attacks like UDP Flood, ICMP Flood, SYN Flood (Random Early Drop and SYN cookie), IP Address Sweeps, IP Address Spoofs, port scan, Ping of Death, Teardrop attacks, unknown protocol protection etc.
Threat Protection	Should support protocol decoder-based analysis statefully decodes the protocol and then intelligently applies signatures to detect network and application exploits
	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.
	Should block known network and application-layer vulnerability exploits

	The proposed firewall shall perform content based signature matching beyond the traditional hash based signatures
	The proposed firewall shall have on box Anti-Virus/Malware, Anti Spyware signatures and should have minimum signatures update window of every one hour
	All the protection signatures should be created by vendors based on their threat intelligence and should not use any 3rd party IPS or AV engines.
	Should perform stream-based Antivirus inspection and not store-and-forward traffic inspection to keep the maximum firewall performance Stream based Antivirus
	scanning should be used for scanning the contents of the files being transferred overthe wire for virus/malwares and should block the file transfer when a virus or malware signatures is triggered.
	Should be able to perform Anti-virus scans for SMB traffic
	Should support DNS sink holing for malicious DNS request from inside hosts to outside bad domains and should be able to integrate and query third party external threat intelligence databases to block or sinkhole bad IP address, Domain and URLs
	The Solution should support DNS security in line mode and not proxy mode.
	The solution should have a dynamic response to find infected machines and respond immediately. There should be provision for administrators to automate the process of sinkholing malicious domains to cut off Command and control and quickly identify infected users.
	Should be able to call 3rd party threat intelligence data on malicious IPs, URLs and Domains to the same firewall policy to block those malicious attributes and list should get updated dynamically with latest data
	Vendor should automatically push dynamic block list with the latest threat intelligence data base on malicious IPs, URLs and Domains to the firewall policy as an additional protection service
Advanced Persistent Threat (APT) Protection	This should be a cloud bases unknown malware analysis service with guaranteed protection signature delivery time not more than 10 minutes
	Advance unknown malware analysis engine should be capable of machine learning with static analysis and dynamic analysis engine with custom-built virtual hypervisor analysis environment
	Advance unknown malware analysis engine with real hardware, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware
	Solution should detonate evasive threats in a real hardware environment, entirely removing an adversary's ability to deploy anti-VM analysis techniques
	Solution should extract key features from the content and evaluate it against a model to determine its maliciousness.
	Cloud base unknown malware analysis service should be certified with SOC2 or any other Data privacy compliance certification for customer data privacy protection which is uploaded to unknown threat emulation and analysis

	Cloud base unknown malware analysis service should be able to perform dynamic threat analysis on such as EXEs, DLLs, ZIP files, PDF documents, Office Documents, Java®, Android APKs, Adobe Flash applets, Web pages that include high-risk embedded content like JavaScript, Adobe Flash files. MAC OS and DMG file types
	Solution must have the ability to automatically analyze advanced threats in real hardware systems.
	The proposed next generation security platform should be able to detect and prevent zero day threats infection through HTTP, HTTPS, FTP, SMB, SMTP, POP3, IMAP use by any of application used by the users (eg: Gmail, Facebook, MS outlook)
	Advance unknown malware analysis engine should be able to create automated high-fidelity signature for command and control connections and spyware to inspect command and control http payload to create one to many payload base signatures protection from multiple unknown spyware and command and control channels using single content based signature
	The protection signatures created for unknown malware emulation should be payload or content based signatures that could block multiple unknown malware that use different hash but the same malicious payload.
URL Filtering and Web Protection	Same Hardware platform should be scalable to provide URL filtering and web protection and should maintain same performance/throughputs mention in primary scope
	The proposed firewall shall have the database located locally on the device
	The proposed firewall shall have custom URL-categorization
	The proposed firewall shall customizable block pages
	The proposed firewall shall block and continue (i.e. allowing a user to access a web-site which potentially violates policy by presenting them a block page with a warning with a continue option allowing them to proceed for a certain time)
	The proposed firewall shall have logs populated with end user activity reports for site monitoring within the local firewall
	The proposed firewall shall have Drive-by-download control
	The proposed firewall shall have URL Filtering policies by AD user, group, machines and IP address/range
	Should have full-path categorization of URLs only to block re categories the malicious malware path not the full domain or website
	Should have zero-day malicious web site or URL blocking update less than 15 minutes for URL DB update for zero-day malware command and control, spyware and phishing websites access protection
	Should have URL or URL category base protection for user cooperate credential submission protection from phishing attack with malicious URL path
	The URL filtering service should be able to categorize a site by multiple categories and not just a single and custom category

	The NGFW should prevent this kind of credential theft attack (without the need of endpoint agents). Vendors should provide features with the ability to prevent the theft and abuse of stolen credentials, one of the most common methods cyber adversaries use to successfully compromise and maneuver within an organization to steal valuable assets. It should also complement additional malware and threat prevention and secure application enablement functionality, to extend customer organizations' ability to prevent cyber breaches. • Automatically identify and block phishing sites • Prevent users from submitting credentials to phishing sites Prevent the use of stolen credentials
SSL/SSH Decryption	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)
	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection
	The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections
	The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic
	SSL decryption must be supported on any port used for SSL i.e. SSL decryption must be supported on non-standard SSL port as well
Network Address Translation	The proposed firewall must be able to operate in routing/NAT mode
	The proposed firewall must be able to support Network Address Translation (NAT)
	The proposed firewall must be able to support Port Address Translation (PAT)
	The proposed firewall shall support Dual Stack IPv4 / IPv6 (NAT64, NPTv6)
	Should support Dynamic IP reservation, tunable dynamic IP and port over subscription
IPv6 Support	L2, L3, Tap and Transparent mode
	Should support on firewall policy with User and Applications
	Should support SSL decryption on IPv6
	Should support SLAAC Stateless Address Auto configuration
Routing and Multicast support	The proposed firewall must support the following routing protocols: - Static - RIP v2 - OSPFv2/v3 with graceful restart BGP v4 with graceful restart
	Policy-based forwarding
	PIM-SM, PIM-SSM, IGMP v1, v2, and v3
	Bidirectional Forwarding Detection (BFD)
Authentication	should support the following authentication protocols: - LDAP - Radius (vendor specific attributes) - Token-based solutions (i.e. Secure-ID) Kerberos

	The proposed firewall's SSL VPN shall support the following authentication protocols
	- LDAP - Radius - Token-based solutions (i.e. Secure-ID) - Kerberos - SAML Any combination of the above
Monitoring, Management and Reporting	Should support on device and centralized management with a dedicated control plane with complete feature parity on firewall administration. In case the NGFW doesn't have a separate control plane, The dedicated Management appliance must be provided.
	Should have separate real time logging based on all Traffic, Threats, User IDs, URL filtering, Data filtering, Content filtering, unknown malware analysis, Authentication, Tunneled Traffic and correlated log view based on other logging activities
	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis
	Should allow the report to be exported into other formats such as PDF, HTML, CSV, XML etc.
	Should have built in report templates based on Applications, Users, Threats, Traffic and URLs
	Should be able to create a report based on SaaS application usage
	Should be able to create reports base user activity
	Should be able to create custom report based on custom query base any logging attributes
	The NGFW must be able to identify unused security policies. NGFW must provide detailed information regarding first hit counts, last hit counts and total hit counts on individual security policy. So We can optimize configuration.
	OEM / Bidder must push IOC (Bad IP Address + URL + Domain Name) using automated & dynamic block list proactively to all NGFW without need to login to NGFW & commit config changes. This is to reduce the implementation time + effort thus reducing the overall risk and improving overall security posture. Such automated security policy updates must be completed in less than 5 minutes.
	In order to ensure NGFW is deployed as per industry best practices + OEM best practices + avoid misconfiguration + avoid Human error, We Would like to review the NGFW config on a quarterly basis. Bidder / OEM to provide online, GUI based, easy to use tools for best practice assessment. Bidder / OEM to provide comprehensive report highlighting config gaps against best practices & provide steps to rectify them. We should also have access to this tool to do Best Practice assessment by themselves whenever required by generating automated reports

	The proposed solution with Malware & Bot Prevention engines should be supplied with the readily available support for the ingestion & Sharing of threat intelligence feeds in a common threat language called as STIX (Structured Threat Information expression) & TAXII (Trusted Automated exchange of Indicator Information).
Authorization	Original Manufacturer Authorization Certificate to be submitted along with the bid
Support & Warranty	3 Years OEM Premium support bundle with 24x7x365 days TAC support, RMA, software updates and subscription update support. The NGFW should be proposed with 3 years subscription licenses for NGFW, NGIPS, Anti-Virus, URL Filtering, Anti Spyware, Anti Botnet and Anti APT.

Date:

Place:

I/We have read and understood all the technical specifications as mentioned above in the Annexure 'IV'. It is to confirm that all the equipments to be supplied are as per the specifications indicated in the tender document.

Signature of the Bidder/Firm
(Name & Address of the Bidder/Firm with seal)

ANNEXURE - V

NGFW's MANUFACTURER'S AUTHORIZATION FORM (MAF)

To

The Executive Director, (Gen. Administration)
National Cooperative Development Corporation
4 Siri Institutional Area,
Hauz Khas, New Delhi 110016.

Dear Sir,

Reg : NCDC's Tender Ref No : dated

We, M/s. _____ who are established and reputed manufacturers of _____(Brand, Model of NGFW) having registered office at _____ do hereby authorize M/s. _____ (Name and address of bidder) to offer their quotation and conclude the contract with you against the above invitation for the bid, as one of our authorized vendor for the sale and service of our products.

Authorized Signatory

Signature:

Name:

Designation:

Name & Address of the company:

Seal of the Company

* To be submitted on OEM's letter head duly signed by the Authorized signatory of Company.

वित्तीय बोली

FINANCIAL BID