National Internet Exchange of India
9th Floor, Statesman House, Barakhamba Road,
New Delhi

TENDER NO. NIXI/2021/Cybersecurity Revamp

Name of Work	Cyber Security Revamp at NIXI Exchange POPs (Point of Presence)
Bid Submission Start Date	25th Feb 2021
Last Date for bid submission	24th March 2021 15:00Hrs

Request for Proposal for Cyber Security Revamp from System Integrators

New Delhi - 110001

INTRODUCTION

The National Internet Exchange of India (NIXI) is a non-profit Company incorporated under Section 25 of the India Companies Act, 1956 (now section 8 under Companies Act 2013) with an objective of facilitating improved internet services in the country. NIXI was registered on 19th June, 2003 and performs three operations -

National Internet Exchange of India (NIXI) was set up for peering of ISPs among themselves for the purpose of routing the domestic traffic within the country, instead of taking it all the way to US/Abroad, thereby resulting in better quality of service (reduced latency) and reduced bandwidth charges for ISPs by saving on International Bandwidth. NIXI is managed and operated on a Neutral basis, in line with the best practices for such initiatives globally. Website – www.nixi.in

.IN Registry is India's Country Code Top Level domain (ccTLD). The Govt. of India delegated/autorized the operations of .INRegistry to NIXI in 2005. The INRegistry operates and manages India's .IN ccTLD. Now .IN domain names are available to anyone on first-come-first-served basis. Website – www.registry.in

.IN Registry and Internationalized Domain Names (IDNs): Since 2005, NIXI also manages the .IN Registry (www.registry.in) including 15 IDN TLDs. At present, 137 Registrars have been accredited to offer .IN domain Name registration worldwide to customers. This has helped proliferation of web hosting in the country and promotion of Indian language content on the Internet.
IDN's in Hindi, Bodo, Dogri, Konkani, Maithili, Marathi, Nepali Sindhi, Bangali, Gujarati, Manipuri, Punjabi, Tamil, Telugu and Urdu languages were launched during the year 2014-15. The General availability of all the remaining Indian languages i.e. Assamese, Kannada, Oriya, Malayalam, Santali, Sanskrit, Sindhi, Kashmiri started from 15th July, 2020

Indian Registry for Internet Names and Numbers (IRINN) in India that provides allocation and registration services of IP addresses and AS numbers, and contributes to the society by providing Internet-related information as a non-profit, affiliation-based organisation, and performing research, education and enlightenment activities. IRNN is a division functioning under NIXI and provides allocation and registration services of Internet Protocol addresses (IPv4 & IPv6) and Autonomous System numbers to its Affiliates .It is a not-for-profit, Affiliates based entity, with the primary goal of allocation of Internet resources to its Affiliates. Website – www.irinn.in

1. SCOPE OF WORK

NIXI is looking to revamp their Internet Perimeter Security (New Generation Firewall along with On Premise Sand Box to be Installed, commissioned and tested for its proposed point of presence (POP)/ Internet exchange point (IX) at Noida/Mumbai/Kolkata & Chennai Locations. Bids (Technical & Financial) are invited from eligible vendors which are valid for a period of 180 days from the last date of submission. Following are the details of existing infrastructure and proposed Cyber Security solution.

NIXI Exchange –

NIXI primarily peers' ISPs and is connected on MPLS VPN. It also peers with Content Delivery Network (CDN) providers like Google, AWS, Akamai, Netflix and so on. NIXI currently has traffic of around 200+ Gbps. NIXI is the L2 & L3 exchange points for its peer ISPs and CDNs.
There are total 9 locations of NIXI, which are Noida, Mumbai, Chennai, Kolkata, Ahmedabad, Bengaluru, Hyderabad and Guwahati. Noida location is connected to MPLS VPN last mile on 1 Mbps link and rest 7 locations are connected on 512 Kbps link.

NIXI utilizes Multi Router Traffic Grapher (MTRG) for Traffic analysis for all the locations and hence the Traffic Analysis servers and other software tools are located in Noida DC location. The servers are protected by a Fortinet FG-100E firewall, which has a Threat Prevention throughput of only 250 Mbps.

NIXI Exchange envisages that there should be cyber security measures and controls which should provide security, control and visibility to maintain an effective cybersecurity posture. NIXI Exchange would like to adopt security system which should deliver advanced threat protection, multi-engine sandboxing architectures to unified policy creation which should make defending NIXI Exchange's network simpler and more effective. It should be "Security without Compromise".

NIXI Exchange would have Perimeter Security appliance and Advanced Threat Prevention appliance as per the network architecture below. The proposed Perimeter Security Appliance should be integrated with Security Management and Reporting software –

2- GENERAL CONDITIONS FOR BID

Following are the general terms & conditions are for this tender. The bidder/OEM should provide necessary documentary evidence of compliance as follows. Failure to do so for any of the Criteria mentioned below shall result in disqualification of the Bidder.

1. The Bidder should be public or private limited company registered / incorporated under The Companies Act, 1956.
2. Bidder/OEM should have not blacklisted by any Government (Central/State) Department/Undertaking or PSU. A declaration of Non-Blacklisting will be submitted by bidder.
3. Bidder should have minimum average turnover of 12 Crores in last three financial years. (CA Certificate or Certified copy Balance Sheet or equivalent should be submitted for FY 2017-18, 2018-19, 2019-20)
4. Bidder should have executed at least one order of Cyber Security product and service for a value of at least INR Fifty lakhs in last five Financial Years.
5. The Bidder should be authorized by **Manufacturers / OEM** to supply, install, and support the products required by NIXI being proposed for this RFP. They should have expertise in Cyber Security and should have trained manpower for same. Certificate of this effect should be provided from OEM.
6. The product offered should be from an OEM product listed in the Magic Quadrant as per the 2019 Gartner Reports / NSS labs report. Document/certificate of same should be provided along with bid.
7. There should be complete compliance of product as mentioned in Annexure-1.
8. OEM of product should have TAC (Technical Assistance Centre) or Call Centre for all level of support in India.
9. Start-up/MSME exemption for turnover/ past performance/ experience will be

granted as per Government of India notifications. To claim same bidder has submit the copy of certificate from Department Industry Policy and trade promotion.

10. The equipment is planned to be utilised to Internet Exchange of NIXI at Noida, Mumbai & Chennai.

3- Technical Specification

Annexure 1: Technical Specification

1.0 Technical Specification for Firewalls (Type 1 & Type 2) :-

SL. No.	Specifications	Compliance (Y/N)
A.	**Security Features (General)**	
1	Integrated Security Appliance which have these features from day 1 - Firewall, VPN, IPS, Web filtering, Botnet Filtering, Gateway AV, Anti Spyware, Application Control and Geo-IP protection. The firewall should also support anti-Spam services or credential theft prevention services integrated as a license in the firewall (applicable to Firewall Type 2 only).	
2	The device should be IPv6 ready, and should support multi-core architecture and not proprietary ASIC based architecture.	
3	Appliance should support IPSec NAT traversal, OSPF, RIP V1 and V2 routing protocol and NAT without degrading the performance of the firewall.	
4	Should support authentication using XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, Internal user database, terminal Services, Citrix / kerberos, TACACS, SAML and MFA profiles	
5	Should have Layer 2 bridge or transparent mode, Wire mode, Sniffer mode /Tap mode	
6	Dual WAN/ISP Support : Should support automatic ISP failover as well as ISP laod balancing for outbound traffic	
7	Should be quad core or higher processor based solution for faster processing. The firewall should support multiple Security Processing Cores.	
8	Should provide complete protection by performing full decryption and inspection of TLS/SSL and SSH encrypted connections regardless of port or protocol.	
9	Should proactively detect and block mass market, zero-day threats and unknown malware by inspecting directly in memory or equivalent technology to stop memory based attacks.	
10	Product Support should be (24 x 7) with Advanced replacement	
11	Should have capability to look deep inside every packet (the header and data) searching for protocol non-compliance, threats, zerodays, intrusions, and even defined criteria. The firewall should support stream/flow based inspection only without compromising/missing any security features like AV, Windows File Sharing (CIFS), email filter, web filter, VOIP etc.	
12	Should detect and prevent hidden attacks that leverage cryptography, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control (C&C) communications and data exfiltration	
13	Should allow total control to customize which traffic is subjected to decryption and inspection based on specific organizational compliance and/or legal requirements.	

14	Vendor & OEM should support the appliance with all necessary upgrade for at least 5 years from the date of purchase installation along with 5 years security software subscription.	
15	Should scan for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware and does not become a launch platform for attacks in case an infected machine is brought inside.	
16	Should provide real-time monitoring and visualization provides a graphical representation of applications, users and bandwidth usage for granular insight into traffic across the network.	
17	Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes.	
18	The proposed solution should be scalable and offer fault tolerance to safeguard against hardware failures. The failover should be capable of taking over the traffic without any manual intervention and session loss.	
19	Should support deep packet SSL to decrypt HTTPS traffic for scanning(IPS, Gateway Antivirus, Content Filtering, Application control) transparently for future requirement and then re-encrypt and send to destination if no threat found.	
20	Should have TLS/SSL decryption and inspection engine that decrypts and inspects TLS/SSL encrypted traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden in encrypted traffic.	
21	Should have deep packet inspection of SSH to decrypt and inspect data traversing over SSH tunnel to prevent attacks that leverage SSH.	
22	Should have IPv6 and should support filtering and wire mode implementations.	
23	Should support REST APIs that allows the firewall to receive and leverage any and all proprietary, original equipment manufacturer and third-party intelligence feeds to combat advanced threats such as zero-day, malicious insider, compromised credentials, ransomware and advanced persistent threats.	
24	Should have Bi-directional raw TCP inspection. The appliance should be capable of scanning raw TCP streams on any port bi-directionally preventing attacks that they to sneak by outdated security systems that focus on securing a few well-known ports.	
25	Should have extensive protocol support to identify common protocols such as HTTP/S, FTP, SMTP, SMBv1/v2 and others, which do not send data in raw TCP, and decode payloads for malware inspection, even if they do not run on standard, well-known ports.	
26	Should have SD-WAN feature to choose lower-cost public Internet services while continuing to achieve a high level of application availability and predictable performance. Vendors not having SD-WAN fetures integrated in their firewall should provide additional device to provide this feature support from day 1. Necessary licenses, if required, need to be provisioned from day 1.	
27	Should have secure SD-WAN feature that enables distributed enterprise organizations to build, operate and manage secure, high-performance networks across remote sites for the purpose of sharing data, applications and services using using readily-available, low-cost public internet services. Vendors not having SD-WAN feature integrated in their firewall should provide additional device to provide this feature support from day 1.	

28	Should control applications, or individual application features, that are identified by the security engine against a continuously expanding database of over thousands of application signatures, to increase network security and enhance network productivity. Should control custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications, in order to gain further control over the network.	
29	The firewall should support traffic management option to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy.	
30	Should identify and block command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points. Appliance should protect against DOS & DDOS attacks .	
31	Should have anti-evasion technology by using extensive stream normalization, decoding and other techniques ensure that threats do not enter the network undetected by utilizing evasion techniques in Layers 2-7	
32	Should not buffer traffic before scanning for IPS and must support inbound and outbound IPS scanning. It should scan the entire traffic and not few specific kilo-byte of the session.	
33	Should be integrated solution with appliance-based firewall on a single chassis with multicore processor.	
34	The device should be featured with Gateway Antivirus and DPI SSl Scanning	
35	The OEM should have regular update of its attack signature database and the same should be configurable to update the signatures automatically without manual intervention. The new attack signatures and new major software releases should be available in OEM website for free download.	
36	Should not buffer traffic before scanning for virus. Should have capacity to scan unlimited file size without buffering them.	
37	Firewall must support inbound and outbound Antimalware/Antispyware scanning. Should identify and block command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points.	
38	Should enforce acceptable use policies and block access to HTTP/HTTPS websites containing information or images that are objectionable or unproductive with Content Filtering Service and Content Filtering Client.	
39	Should block content using the predefined categories or any combination of categories. Filtering can be scheduled by time of day, such as during school or business hours, and applied to individual users or groups.	
40	URL database should have at least 15 million sites and 64 + categories.	
41	There should be a proposed sand boxing solution which should be appliance - based and employ sandboxing engine for effective scanning and integrated with the proposed firewalls. The appliance-based Sandbox should support Reputation & Global Threat Lookup and should support 6000 files per day. The Sandbox appliance should also support max file size of 100 MB and should support REST API interface that can be used to submit files for analysis and query results by threat intelligence teams via their own scripts, web-portal integrations, and other security products. Single Sandboxing appliance to be quoted which should cater the type 1 & type 2 firewalls.	

42	The appliance Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. The technology should discover packed malware code that has been compressed to avoid detection, the technology should allow the malware to reveal itself by unpacking its compressed code in memory in a secure sandbox environment. It should see what code sequences are found within and compares it to what it has already seen.	
43	The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Portsmash etc or similar kind of advanced memory based attacks.	
44	The firewall should have single pass, low latency inspection system that performing stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol.	
45	Should have ability to prevent potentially malicious files from entering the network. Should have support for files sent to the proposed on-premise sandbox for analysis to be held at the gateway until a verdict is determined.	
46	Should have continuously updated database of tens of millions of threat signatures residing in the sandbox servers and referenced to augment the capabilities of the onboard signature database, providing deep packet inspection with extensive coverage of threats. Should support min 20K DPI signatures or tens thousands of IPS signatures and 3400+ Application Signatures from day 1.	
47	Appliances should have dedicated management Ethernet interface	
48	Appliance should be 1U and rack mountable. Vendor not having 1RU configuration may quote higher RU to meet the requirement.	
49	Should support REST APIs for management. Solution should support IPSEC & SSL VPN and Layer 2 Tunneling protocol (L2TP) over IPSEC	
B.	**Licensing and Certification**	
1	The devices should not have license restriction on number of users. The license should the following subscriptions from day 1 - Firewall, Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control, URL/Content Filtering and Advance Threat Prevention/Protection including advance sandboxing.	
2	The OEM should be having "recommended rating" by NSS Labs for consecutive three years in the last six years. OEM should have scored minimum 97% in Exploit Block rate in the last NSS Lab for NGFW report (2019)	
3	The OEM should have NetSec Open certification in FY2020 for Network Security / NGFW product performance testing and should have overall Block rating of 98% and above	
4	The OEM should have Common Criteria/NDPP and ICSA Enterprise Firewall certification.	
5	The device should be IPv6 Ready and USGv6 certified	
C.	**High Availability**	
1	Proposed Solution should support Hardware redundancy.	
2	Proposed solution should support Active/Passive with State Sync and Active/Active Clustering. Firewall should be configured with Active-Passive configuration from day 1.	
3	Proposed should failover incase of a primary hardware failure without session loss and manual intervention.	

D.	**Firewall Type 1 - Hardware, Interface & Performance requirement**	
1	The product should have minimum of 4 x 1GbE interfaces and 12 x 10Gig interfaces	
2	Should have built-in storage of atleast 1 TB, 1 console Port and 1 USB interface	
3	Appliance should have redundant hot swappable fans	
4	Appliance should have built in dual, redundant, hot swappable power supplies	
5	Threat prevention throughput of 9 Gbps or higher which should include Firewall, Gateway Anti-Virus, AntiSpyware, Intrusion Prevention and Application Intelligence and Control, URL/Content Filtering and URL & Reputation service from Advance Threat Prevention/Protection/sandboxing services.	
6	The Firewall should have atleast 10 Gbps of IPS throughput or higher.	
7	VPN throughput at least 10 Gbps or higher.	
8	The Firewall shoyld have TLS/SSL decryption and inspection throughput (with IPS enabled) of 2 Gbps	
9	The Firewall should support at least 125,000 new sessions/connections per second.	
10	The Firewall should support at least 12 million maximum connections and 100K maximum DPI SSL sessions/connections.	
11	Should support at least 12,000 IPSec Site-to-Site VPN tunnels and 5000 or more no of IPSec Client Remote access VPN	
12	Should support at least 3000 SSL VPN users	
E.	**Firewall Type 2 - Hardware, Interface & Performance requirement**	
1	The product should have minimum of 10 x 1GbE interfaces, 4 x 1G SFP, 4 x 10Gig interfaces	
2	Should have built-in storage of atleast 1 TB, 1 console Port and 1 USB interface	
3	Appliance should have dual hot swappable fans	
4	Appliance should have built in dual, redundant power supplies	
5	Threat prevention throughput of 3 Gbps or higher which should include Firewall, Gateway Anti-Virus, AntiSpyware, Intrusion Prevention and Application Intelligence and Control, URL/Content Filtering and URL & Reputation service from Advance Threat Prevention/Protection/sandboxing services.	
6	The Firewall should have atleast 6 Gbps of IPS throughput or higher.	
7	VPN throughput at least 3.5 Gbps or higher.	
8	The Firewall shoyld have TLS/SSL decryption and inspection throughput (with IPS enabled) of 800 Mbps	
9	The Firewall should support at least 40,000 new sessions/connections per second.	
10	The Firewall should support at least 4 million maximum connections and 35K maximum DPI SSL sessions/connections.	
11	Should support at least 6,000 IPSec Site-to-Site VPN tunnels and 3000 or more no of IPSec Client Remote access VPN	
12	Should support at least 1500 SSL VPN users	
F.	**Logging and reporting**	
1	Should have reporting facility to generate reports on virus dedected over different protocols, top sources for viruses, destination for viruses, top viruses etc.	

2	Logging and reporting solution should be supported.	
3	The solution should generate the reports for the firewall, gateway level AV, IPS web filtering requested.	
4	The solution shall have readymade templets to generate reports like complete reports or attack reports, bandwidth report etc.	
5	The solution should help to analyze/understand attacks over various protocols like HTTP , FTP , SMTP etc.	
6	The solution should help to analyze/understand the live application usage in the network.	
7	Should have options to generate reports in terms of which are the frequent attacks as well as top sources and destination for attacks.	
8	Should have options to generate reports in different formats	
9	The solution should have configurable options to schedule the report generation.	
10	The solution should be running its own syslog server or integrated server to collect the logs. If separate server and/or appliance is required for the logging & reporting, the BOM & cost should be included in the proposed solution.	
11	The solution should provide Change Order Management and Work Flow which assures the correctness and compliance of policy changes by enforcing a process for configuring, comparing, validating, reviewing and approving policies prior to deployment.	
12	The should support Offline management thereby enabling scheduling of configurations and firmware updates on managed appliances to minimize service disruptions.	
13	The solution should establish a unified security governance, compliance and risk management security program	
14	The solution should support sophisticated VPN deployment and configuration - should simplify the enablement of VPN connectivity and consolidate thousands of security policies.	
15	The solution should support active-device monitoring and alerting - should provide real-time alerts with integrated monitoring capabilities, and should facilitate troubleshooting efforts, thus allowing administrators to take preventative action and deliver immediate remediation.	
16	The solution should support Application Visualization and Intelligence - should show historic and real-time reports of what applications are being used, and by which users. Reports should be completely customizable using intuitive filtering and drill-down capabilities.	
17	Centralized logging - should offer a central location for consolidating security events and logs for thousands of appliances providing a single point to conduct network forensics.	
18	Real-time and historic next generation syslog reporting - should streamline the time-consuming summarization process, allowing for near real-time reporting on incoming syslog messages. Also, should provide the ability to drill down into data and customize reports extensively.	
19	The Security Management Solution should be appliance based or virtual appliance based. If vendor is proposing virtual appliance- based solution then the hardware pre-requisites should be as below – • 16 CPU/vCPU, 32 GB RAM and 500 GB HDD	
20	The Firewalls (Type 1 & Type 2) should be from the same OEM. The Firewalls and Security Management Software should be from the same OEM. The Firewalls (Type 1 & Type 2) & Sandbox appliance should be from the same OEM	

4- Instruction for Bid submission

1. Bids will be submitted in hard copies at NIXI office Delhi. There is no electronic or digital submission is allowed.
2. The bid should be submitted in two parts. Part-1 is Technical Bid and Part-2 will be Financial/Commercial bid.
3. Technical will contain all the documents/compliance asked in General Term of conditions along with Technical Compliance as per Annexure 1. Technical Bid will also have unpriced BOM as per Annexure-2. Please do not put Financial Bid/Commercial bid in Technical bid this would lead to summary rejection of the bid.
4. Financial/Commercial bid will contain schedule of prices as per the Financial/Commercial Bid format.
5. Both Technical and Financial/Commercial bid should be kept in separate envelope and this envelops should be kept in on large envelope. All the envelopes should be properly sealed.
6. Each page of the tender bid should be signed and sealed by authorized signatory.
7. No bid will be accepted post the last date and time mentioned in the tender document. However, NIXI reserves the right to extend the date and time of bid submission.

Schedule table

Name of Work	Cyber Security Revamp at NIXI Exchange POPs (Point of Presence)
Bid Submission Start Date	25th Feb 2021
Last Date for bid submission	17th March 2021

5- Assistance to bidders

Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the following email id abhishek.gautam@nixi.in and soumen@nixi.in

6- Bid Evaluation Criteria

a. Tender committee will first evaluate the Technical bid and technical BOM. They can seek any clarification/documents/confirmation, should they need the same for further clarity.
b. Financial/Commercial bids of those Bidders whose Pre-Qualification &Technical bids are found suitable by the committee, will be opened.
c. Contract will be awarded to L1 bidder which will arrived at as per Financial/Commercial Bid format inclusive of taxes.

7- Bid Validity

I. All the bids (Technical and Financial) must be valid for a period of 180 days from the last date of submission of the tender for execution of Contract.

II. In exceptional circumstances, prior to expiry of the original time limit, the NIXI may request the bidders to extend the period of validity for a specified additional period beyond the original validity of 180 days. The request and the bidders' responses shall be made in writing/Email. The bidders, not agreeing for such extensions will be allowed to withdraw their bids.

8- Modification / Substitution/ Withdrawal of bids

I. No Bid shall be modified, substituted, or withdrawn by the Bidder after the bids due date.

II. Any alteration/ modification in the bid or additional information supplied subsequent to the bid's due Date, unless the same has been expressly sought for by the Authority, shall be disregarded.

9- Rejection of the Bid:

The bid submitted shall become invalid if: -

I. The bidder is found ineligible.

II. The bidder does not provide all the documents as stipulated in the bid document.

10- Special Terms and Conditions

1 The NIXI reserves the right of accepting or rejecting any quotations without assigning any reason thereof.

2 Bidder will enter into the contract with NIXI as per format mentioned in Annexure 2.

11- Delivery, Installation/ Acceptance and Commissioning of Equipment:

The vendor should agree to deliver the equipment and install and commission all the equipment at the specific location identified by NIXI at the respective POP locations. NIXI shall reject the component/equipment supplied if it does not comply with the specifications or does not function properly after installation. The contractor shall replace the non-functioning or defective equipment or its spares immediately and ensure proper functioning of all equipment.

12- Warranty/ AMC & Maintenance Clause

I. Warranty shall include free maintenance of the whole equipment supplied including free replacement of parts and all software updates and upgrades.

II. The on-site comprehensive warranty will start from the date of successful installation of equipment by NIXI. All items shall be covered with five-year on-site comprehensive warranty (as per scope of work).

III. The vendor shall assure to maintain the inventory of spare parts for maintenance of the equipment supplied for a period of 5 years.

IV. All ongoing software upgrades for all major and minor releases should be provided during the warranty period without any additional payment by NIXI.

V. The vendor shall ensure that that there is a back-to-back agreement with OEM to meet above hardware and software warranty terms.

VI. During the period of support, the vendor shall:

a) Support the entire hardware/software of equipment.
b) Diagnose the hardware/software faults and rectify the hardware/software faults detected.
c) Repair and replace the faulty parts or part thereof.
d) Upkeep the software periodically including implementation of patches, if required.
e) Contractor shall carry out support activities as per requirement of NIXI.

VII. Bidder would enter into the Annual Maintenance contract post the expiry of warranty period, if NIXI wishes so. Bidder will have to upgrade the hardware with equivalent or better model, if same has been declared end of life by OEM and no longer being supported during the five-year original contract period.

13. Dispute Resolution (Arbitration)

- The Purchaser and the Bidder shall make every effort to resolve amicably by direct informal negotiations, any disagreement or disputes, arising between them under or in connection with the Contract.

- In case of dispute between the purchaser and bidder, the dispute may be resolved through arbitration process as per the Arbitration & Reconciliation Act 1996 with its seat at New Delhi.

14- Permits, Taxes, and other duties

The vendor shall obtain necessary road permits or documentation pay all necessary taxes and duties in delivering the equipment at respective locations. NIXI is not responsible for the same.

15-Payment Schedule:

S. No.	Details	Payment payable (% of contract value)	Remarks
1	Delivery of Equipment	90	Payable upon delivery
2	Satisfactory completion of installation and running duly certified by NIXI team	10	Payable upon successful installation.

The vendor shall charge all applicable taxes as per the prevailing tax laws in India. All the payment to the contractor shall be subject to tax deductions under the prevailing tax laws of India.

TECHNICAL BOQ Format -

Schedule of Requirement (Technical Bill of Material for Each Location)

Sl. No.	New Generation Firewall description	Total Qty	Make & Model
1	**Firewall Type 1** in HA with Security Management & Reporting along with 5 years Subscription & Support. Additional Advance On-prem Sandbox appliance (only in Noida location) with 5 years support and subscription as per specification mentioned in Technical Specification Annexure.	2	
2	Mumbai (2 locations) & Chennai Locations – **Firewall Type 2** in HA with 5 years Subscription & Support as per specification mentioned in Technical Specification Annexure.	6	

Annexure-1 FINANCIAL Bid Format
Schedule of Requirement (Bill of Material for Each Location)

Sl. No.	New Generation Firewall description	Total Qty	Total Price (in INR) w/o Tax	Final Price (in INR) with Tax
NIXI EXCHANGE BOQ:				
1	Noida Location – **Firewall Type 1** in HA with Security Management & Reporting along with 5 years Subscription & Support. Additional Advance On-prem Sandbox appliance (only in Noida location) with 5 years support and subscription as per specification mentioned in Technical Specification Annexure.	2		
2	Mumbai (2 locations) & Chennai Locations – **Firewall Type 2** in HA with 5 years Subscription & Support as per specification mentioned in Technical Specification Annexure.	6		
	SUB TOTAL FOR NIXI:			

Note: All Prices should be inclusive of implementation and deployment. Any third-party product or services needed to make the solution operational should be provided at NO-COST by the bidder.

Annexure -2 CONTRACT FORMAT

THIS AGREEMENT made the day of 2021.

BETWEEN

National Internet Exchange of India (NIXI) (hereinafter referred to as “the Purchaser”) which expression shall unless repugnant to the context or meaning thereof mean and be deemed to include its authorized agents, representatives, and permitted assigns of the First Part.

AND

The Party (hereinafter referred to as “the Bidder”) which expression shall unless repugnant to the context or meaning thereof mean and be deemed to include their successors and permitted assigns having its registered office at of the Second Part.

WHEREAS

The Purchaser had invited Tenders vide their Tender (hereinafter referred to as ‘Tender Document’) for “Cyber Security Revamp AT NIXI Exchange POPs”
The Bidder had submitted its proposal dated (hereinafter referred to as the ‘Tender’) for the provision of such services in accordance with its proposal as set out in its Tender and in accordance with the terms and conditions of the Tender and this Contract.
The Purchaser has agreed to appoint the Bidder for the provision of such product & services and the Bidder has agreed to provide Product and services as are represented in the Tender, including the terms of this Contract, the Schedules attached hereto and in accordance with the terms of the Tender, and in terms of the discussions, negotiations and clarifications in relation to the implementation of the scope of work.
In consideration of the foregoing and the mutual covenants and promises contained herein and other good and valuable consideration the receipt and adequacy of which is hereby acknowledged, the parties intending to be bound legally.

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the General Conditions of Contract referred to.

The following documents shall be deemed to form and be read and construed as part of this Agreement viz:

the Scope of Work/Purchase order
the General Conditions of Contract mentioned in tender document.

In consideration of the payments to be made by the Purchaser to the Bidder as hereinafter mentioned, the Bidder hereby covenants with the Purchaser to provide the Product & Services and to remedy defects therein in conformity in all respects with the provisions of the Contract.

The Purchaser hereby covenants to pay the Bidder in consideration of the provision of the Product /Services and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Purchase order.

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with their respective laws the day and year first above written

Signed, Sealed and Delivered by the said
(For the Purchaser in the presence of: (WITNESS)

Signed, Sealed and Delivered by the said
(For the Bidder) in the presence of: (WITNESS)

Annexure 3 - Performance Bank Guarantee for Contract

Ref: Date

Bank Guarantee NO.

To

National Internet Exchange of India (NIXI)
9th Floor, Statesman House,
Barakhamba Road,
New Delhi

1. Against contract vide Advance Acceptance of the Tender No. ------- dated covering (hereinafter called the said "Contract") entered into between the National Internet Exchange of India (NIXI) (hereinafter called "the Purchaser") and ---------- (hereinafter called the "Bidder") this is to certify that at the request of the Bidder we---- Bank Ltd., are holding in trust in favour of the Purchaser, the amount of ----------(write the sum here in words) to indemnify and keep indemnified the Purchaser against any loss or damage that may be caused to or suffered by the Purchaser by reason of any breach by the Bidder of any of the terms and conditions of the said contract and/or in the performance thereof. We agree that the decision of the Purchaser, whether any breach of any of the terms and conditions of the said contract and/or in the performance thereof has been committed by the Bidder and the amount of loss or damage that has been caused or suffered by the Purchaser shall be final and binding on us and the amount of the said loss or damage shall be paid by us forthwith on demand and without demur to the Purchaser.

2. We Bank Ltd, further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for satisfactory performance and fulfillment in all respects of the said contract by the Bidder i.e. till hereinafter called the said date and that if any claim accrues or arises against us Bank Ltd, by virtue of this guarantee before the said date, the same shall be enforceable against us Bank Ltd, notwithstanding the fact that the same is enforced within six months after the said date, provided that notice of any such claim has been given to us Bank Ltd, by the Purchaser before the said date. Payment under this letter of guarantee shall be made promptly upon our receipt of notice to that effect from the Purchaser.

3. It is fully understood that this guarantee is effective from the date of the said contract and that We Bank Ltd, undertake not to revoke this guarantee during its currency without the consent in writing of the Purchaser.

4. We undertake to pay to the Purchaser any money so demanded notwithstanding any dispute or disputes raised by the Bidder in any suit or proceeding pending before any court or Tribunal relating thereto our liability under this present bond being absolute and unequivocal.

   The payment so made by us under this bond shall be a valid discharge of our liability for payment there under and the Bidder shall have no claim against us for making such payment.

5. We Bank Ltd, further agree that the Purchaser shall have the fullest liberty, without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said contract or to extend time of performance by the Tendered from time to time or to postpone for any time of from time to time any of the powers exercisable by the Purchaser against the said Bidder and to forebear or enforce any of the terms and conditions relating to the said contract and we, Bank Ltd., shall not be released from our liability under this guarantee by reason of any such variation or extension being granted to the said Bidder or for any forbearance by the Purchaser to the said Bidder or for any forbearance and or omission on the part of the Purchaser or any other matter or thing whatsoever, which under the law relating to sureties, would, but for this provision have the effect of so releasing us from our liability under this guarantee.

6. This guarantee will not be discharged due to the change in the constitution of the Bank or the Bidder.

Date

Place Signature

Witness Printed name

(Bank's common seal)

Clarifications/ Querries raised by bidders

Sr.No.	Technical Specifications (NIXI)	Change Request (Palo Alto)	Change Request(Sonic wall)	Change Request (Check point)	
1	Integrated Security Appliance which have these features from day 1 - Firewall, VPN, IPS, Web filtering, Botnet Filtering, Gateway AV, Anti Spyware, Application Control and Geo-IP protection. The firewall should also support anti-Spam services integrated as a license in the firewall (applicable to Firewall Type 2 only).	Integrated Security Appliance which have these features from day 1 - Firewall, VPN, IPS, Web filtering, Botnet Filtering, Gateway AV, Anti Spyware, Application Control and Geo-IP protection. The firewall should also support credential theft prevention services integrated as a license in the firewall.		Not able to provide license Anti spam service from day1	
4	Should support authentication using XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, Internal user database, terminal Services, Citrix	"Should support authentication using XAUTH/RADIUS, Active Directory, SSO, LDAP,kerberos, TACACS, SAML and MFA profiles			
7	Should be quad core or higher processor based solution for faster processing. The firewall should support the following Security Processing Cores as per the type of firewalls – a) Type 1 – 30 Security Processing Cores b) Type 2 – 10 Security Processing Cores	Should be physical core based solution for faster processing. The firewall should support the following physical Processing Cores as per the type of firewalls – a) Type 1 – 48 Physical Security Processing Cores b) Type 2 – 12 Physical Security Processing Cores			
9	Should proactively detect and block mass	Solution shouldd have provision for			

	market, zero-day threats and unknown malware by inspecting directly in memory	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			
18	Should have support to enable guest users to use their credentials from social networking services such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication. The Firewall should support atleast 40 Wireless Access Points from day 1. Necessary licenses, need to be provisioned from day 1.	The device or any of its family should not have any feature of wireless within its hardware or software. The NGFW should have native protection against credential theft attacks(without the need of endpoint agents) with ability to prevent the theft and abuse of stolen credentials.			
19	Should have H.323 gatekeeper and SIP proxy support to block spam calls by requiring that all incoming calls are authorized and authenticated by H.323 gatekeeper or SIP proxy.	Delete			
20	Should support mobile device authentication such as (biometric authentication) fingerprint recognition that cannot be easily duplicated or shared to	Delete			

	securely authenticate the user identity for network access.				
44	There should be a proposed sand boxing solution which should be appliance - based and employ sandboxing engine for effective scanning and integrated with the proposed firewalls. The appliance-based Sandbox should support Reputation & Global Threat Lookup Throughput (12K Files per hour), Real- World File Mix Throughput (2500 Files per hour) and Dynamic Analysis Throughput (300 Files per Hour). The Sandbox appliance should also support max file size of 100 MB and should support REST API interface that can be used to submit files for analysis and query results by threat intelligence teams via their own scripts, web-portal integrations, and other security products. Single Sandboxing appliance to be quoted which should cater the type 1 & type 2 firewalls.	There should be a proposed sand boxing solution which should be appliance - based and employ sandboxing engine for effective scanning and integrated with the proposed firewalls. The appliance-based Sandbox should support Reputation & Global Threat Lookup. This solution should be option for hybrid malware analysis service with guaranteed protection signature delivery time not more than 5 minutes. This should be mentioned on the public datasheets or reference. Single Sandboxing appliance to be quoted which should cater the type 1 & type 2 firewalls.	There should not be any delivery time line of 5 minutes for guaranteed protection signature delivery		
46	The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Portsmash etc.	Delete			

48	Should have ability to prevent potentially malicious files from entering the network. Should have support for files sent to the proposed on-premise sandbox for analysis to be held at the gateway until a verdict is determined.	Advance unknown malware analysis engine with real hardware, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware. The device shouls support upto 28 VMs and atleast 2TB RAID1 and 2 extra bays for future scalability.Cloud base unknown malware analysis service should be supported and certified with SOC2 or any other Data privacy compliance certification for customer data privacy protection which is uploaded to unknown threat emulation and analysis. The proposed device should also be FCC Class A, CE Class A, VCCI Class A, CB and Common Criteria Certified.			
49	Should have continuously updated database of tens of millions of threat signatures residing in the sandbox servers and referenced to augment the capabilities of the onboard signature database, providing	Should have continuously updated database of ten thousand of IPS signatures and 3400+ Application Signatures from day 1.			

	deep packet inspection with extensive coverage of threats. Should support min 20K DPI signatures, 70 millions Cloud AV signatures and 3500+ Application Signatures from day 1.				
B 2	The OEM should be having "recommended rating" by NSS Labs for consecutive three years in the last six years. OEM should have scored minimum 97% in Exploit Block rate in the last NSS Lab for NGFW report (2019)	The proposed vendor must have "Recommended" rating with min100% Evasion proof capability and min 97% Security Effectiveness as per 2019 NSS Labs Next Generation Firewall comparative Test Report.			
B 3	The OEM should have NetSec Open certification in FY2020 for Network Security / NGFW product performance testing and should have overall Block rating of 98% and above.	The proposed vendor must be in the Leader's quadrant of the Enterprise Firewalls Gartner Magic Quadrant for consecutive 5 years	Proposed vendor should not be in leaders quadrant of Gartner		
B 5	The device should be IPv6 Ready (Both phase 1 and Phase2)	The device should be IPv6 Ready and USGv6 certified			
D 1	The product should have minimum of 16 x 1GbE interfaces, 2 x 10Gig Copper and 10 x 10Gig SFP+ interfaces	The product should have minimum of 4 x 1/10GbE interfaces, 16 x 10Gig SFP+, 4X 40Gig interfaces			
D 2	Should have built-in storage of atleast 1 TB, 1 console Port and 1 USB interface	Should have built-in storage of atleast 2 TB HDD and 200 GB Memory in RAID 1, 64GB RAM, 1			

		console Port, 1 OOB and 1 USB interface			
D 3	Appliance should have triple removable fans	Appliance should have redundant hot swappable fan trays			
D 5	Threat prevention throughput of 9 Gbps or higher which should include Firewall, Gateway Anti-Virus, AntiSpyware, Intrusion Prevention and Application Intelligence and Control, URL/Content Filtering and URL & Reputation service from Advance Threat Prevention/Protection/sandboxing services.	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 Malware and logging security threat prevention features enabled – 10 GBPS real world/production environment/Application Mix . 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.			
D 8	The Firewall shoyld have TLS/SSL decryption and inspection throughput	Delete			

	(with IPS enabled) of 2.2 Gbps				
D 10	The Firewall should support at least 12 million maximum connections and 300K maximum DPI SSL sessions/connections.	The Firewall should support at least 4 million maximum connections			
D 11	Should support at least 12,000 IPSec Site-to-Site VPN tunnels and 6000 or more no of IPSec Client Remote access VPNShould support at least 12,000 IPSec Site-to-Site VPN tunnels and 6000 or more no of IPSec Client Remote access VPN	Should support at least 10,000 IPSec Site-to-Site VPN tunnels			
E1	The product should have minimum of 20 x 1GbE interfaces, 4 x 1G SFP, 2 x 10Gig Copper and 2 x 10Gig SFP+ interfaces	The product should have minimum of 12 x 1GbE interfaces, 4 x 1G SFP and 4 x 10Gig SFP+ interfaces			
E2	Should have built-in storage of atleast 1 TB, 1 console Port and 1 USB interface	Should have built-in storage of atleast 200 GB, 32 GB 1 console Port, 1 OOB and 1 USB interface			
E3	Appliance should have dual removable fans	Appliance should have hot swappable fan tray			
E5	Threat prevention throughput of 3 Gbps or higher which should include Firewall, Gateway Anti-Virus, AntiSpyware, Intrusion Prevention and Application Intelligence and Control, URL/Content Filtering and URL & Reputation service from Advance	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-			

	Threat Prevention/Protection/sandboxing services.	Spyware, Anti Malware and logging security threat prevention features enabled – 2.5 GBPS real world/production environment/Application Mix . 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.			
E6	The Firewall should have atleast 6 Gbps of IPS throughput or higher.	The Firewall should have atleast 2.5 Gbps of IPS throughput or higher.			
E7	VPN throughput at least 3.5 Gbps or higher.	VPN throughput at least 2.5 Gbps or higher.			
E8	The Firewall shoyld have TLS/SSL decryption and inspection throughput (with IPS enabled) of 800 Mbps	Delete			
E10	The Firewall should support at least 4 million maximum connections and 35K maximum DPI SSL sessions/connections.	The Firewall should support at least 1 million maximum connections			
E11	Should support at least 6,000 IPSec Site-to-Site	Should support at least 2,000 IPSec			

	VPN tunnels and 6000 or more no of IPSec Client Remote access VPN	Site-to-Site VPN tunnels			
E12	Should support at least 1500 SSL VPN users	Should support at least 1000 SSL VPN users			
F20	The Firewalls (Type 1 & Type 2) should be from the same OEM. The Firewalls and Security Management Software should be from the same OEM. The Firewalls (Type 1 & Type 2) & Sandbox appliance should be from the same OEM	The Firewalls (Type 1 & Type 2) should be from the same OEM. The Firewalls and Security Management Software should be from the same OEM. The Firewalls (Type 1 & Type 2) appliance should be from the same OEM			
	DNS Security	DNS security is very important to handle attacks hidden in DNS.	Not able to provide DNS security as this is separate service provided by ISP/CSP and specialized OEMs of DNS security		
		The Solution shoukd support DNS security in line mode and not proxy mode and proposed from day1.			
		Solution should maintain a database containing a list of known botnet command and control (C&C) addresses which should be			

		updated dynamically.			
		DNS Security should have predictive analytics to disrupt attacks that use DNS for Data theft and Command and Control.			
		DNS security should block known Bad domains and predict with advanced machine learning technology and should have global threat intelligence of atleast 10 million malicious domains.			
		It should prevent against new malicious domains and enforce consistent protections for millions of emerging domains.			
		The solution should integrate and corelate to provide effective prevention against New C2 domains, file download source domains, and domains in malicious email links. Ingegrate.with URL Filtering to continuously			

		crawl newfound or uncategorized sites for threat indicators. Should have OEM human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honeypots. Should take inoputs from atleast 25 third-party sources of threat intelligence.			
		Should have simple policy formation for dynamic action to block domain generation algorithms or sinkhole DNS queries.			
		Solution should prevent against DNS tunneling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel inspection			
		The solution should have capabilities to neutralize DNS tunneling and it should automatically stop with the combination of policy on the next-generation			

		firewall and blocking the parent domain for all customers.			
		The solution should have dynamic response to find infected machines and respond immidiately. There should be provision for administrator to automate the process of sinkholing malicious domains to cut off Command and controk and quickly identify infected users.			