

ग्रामीण कार्य विभाग

बिहार ग्रामीण पथ विकास अभिकरण, पटना

पत्रांक:- मु0310-4 (मु0) विविध कार्य 23-148/18-4068 अक्र पटना/दिनांक:- 31-12-2024-

प्रेषक,

संजीव कुमार
प्रशासनिक पदाधिकारी,
ब्राडा, पटना।

सेवा में,

श्री जितेन्द्र कुमार सिंह,
कार्यपालक अभियंता-सह-नोडल
पदाधिकारी, E-Advertisement
ग्रामीण कार्य विभाग, पटना।


विषय : विभागीय सर्वर की Storage Capacity बढ़ाने के लिए NAS Storage and Firewall का आपूर्ति हेतु अति अल्पकालीन कोटेशन आमंत्रित करने की सूचना प्रकाशन के संबंध में।

महाशय,

उपर्युक्त विषय के संबंध में कहना है कि ग्रामीण कार्य विभाग में अधिष्ठापित सर्वर पर निरंतर बढ़ते डाटा के संग्रहण हेतु विभागीय सर्वर की Storage Capacity बढ़ाने के लिए NAS Storage and Firewall का आपूर्ति हेतु अति अल्पकालीन कोटेशन आमंत्रित करने हेतु विज्ञापन प्रकाशित किया जाना है। इसे राज्य के हिन्दी एवं अंग्रजी समाचार पत्रों एवं राष्ट्रीय स्तर के हिन्दी एवं अंग्रजी समाचार पत्रों में प्रकाशित करने की कृपा की जाये।

अनु0- यथोक्त।

विश्वासभाजन


(संजीव कुमार)

प्रशासनिक पदाधिकारी, ब्राडा



बिहार सरकार
ग्रामीण कार्य विभाग
बिहार ग्रामीण पथ विकास अभिकरण
हार्डिंग रोड (क्रांति मार्ग), बैरक नं०-03 (हज भवन के बगल में)

NAS Storage एवं Firewall के क्रय हेतु अति अल्पकालीन कोटेशन आमंत्रण सूचना

बिहार ग्रामीण पथ विकास अभिकरण, ग्रामीण कार्य विभाग, बिहार के नियंत्रणाधीन एक सोसाईटी है। जो ग्रामीण कार्य विभाग के कार्यान्वयन हेतु आवश्यक सहयोग उपलब्ध कराती है। ग्रामीण कार्य विभाग में अधिष्ठापित सर्वर पर निरंतर बढ़ते डाटा के संग्रहण हेतु विभागीय सर्वर की Storage Capacity बढ़ाने की आवश्यकता है। जिसके लिए निम्नलिखित विशिष्टियों के NAS Storage and Firewall का क्रय किया जाना है—

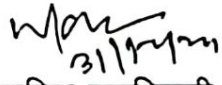
क्र०सं०	विवरण	रं०	प्रति इकाई दर	राशि	CGST	SGST	कुल राशि
1	NAS Stroge (Quantity-2Pcs) Configuration :- Capacit:-25TB Usable stroge, Procesor :- Intel R Xeun&Silve 4112 and above, Memory:-64GB Eternet:-1GB Ethernet Warranty:-3 Years, HD type:- Hot Plug Sata or Sas SFF (2.5") or LFF (3.5") Protocol Support:- SMB, NFS, ISCSI over Eathernet, FTP/S, HTTP/S	2					
2	Firewall Configuration:- NGFS Firewall with 16x1GRJ 45 Pports, 8x1G SFP Posts 2x2 10 G SFP+Ports Utm LICENSE, Web Filtering, AV, IPS, Anti Premium (24*7) Support for 3 Years.	1					

इच्छुक आपूर्तिकर्ता फर्म/संस्थान उक्त सामग्रियों की आपूर्ति करने हेतु वांछित कागजातों के साथ अपर मुख्य कार्यपालक पदाधिकारी-सह-सचिव, ब्राडा के पद नाम से दिनांक-09.01.2025 को अपराहन 03:00 बजे तक निम्नांकित शर्तों के साथ मुहरबंद लिफाफे में कोटेशन आमंत्रित की जाती है। प्राप्त कोटेशन दिनांक-09.01.2025 को अपराहन 03:30 बजे खोला जायेगा।

कोटेशन की शर्तें निम्नवत हैं :-

- कोटेशनदाता को कोटेशन के साथ PAN Card, GST प्रमाण पत्र एवं संस्था के निबंधन से संबंधित प्रमाण पत्र की स्व-अभिप्रमाणित छाया प्रति संलग्न करना आवश्यक होगा।
- कोटेशनदाता को कोटेशन के साथ विगत 03 वर्षों का आयकर रिटर्न से संबंधित प्रपत्र एवं विगत 03 वर्षों का Turn Over से संबंधित प्रमाण पत्र संलग्न करना आवश्यक होगा।
- सर्वर एवं फायर वॉल की विशिष्टियों एवं संख्या विभाग द्वारा निर्धारित की गयी है। जिसके अनुरूप सामग्रियों की आपूर्ति करना आवश्यक शर्त है।

4. कोटेशनदाता को BID Security के रूप में ₹25,000/- (पच्चीस हजार) मात्र का किसी राष्ट्रीयकृत बैंक से निर्गत FDR/DD जो ACEO&CUM&SECRETARY, BRRDA के नाम से प्रतिज्ञप्त हो समर्पित करना होगा।
- 5 NAS Storage and Fire Wall की विस्तृत तकनीकी विशिष्टियां विभागीय वेबसाईट www.rwdbihar.gov.in के Notice Board पर अपलोड कर दिया गया है। निविदादाता उक्त वस्तुओं का कोटेशन उपरोक्त प्रारूप में उद्धृत करेंगे।
6. उक्त निर्धारित प्रारूप के अतिरिक्त किसी अन्य प्रारूप में उद्धृत दर स्वीकार्य नहीं होगा।
7. सफल निविदादाता को क्रय आदेश निर्गत होने के 07 दिनों के अन्दर क्रय आदेश के अनुरूप सामग्रियों की आपूर्ति करना अनिवार्य होगा।
8. सामग्रियों की आपूर्ति प्राप्त होने के पश्चात् निर्धारित विशिष्टियों एवं गुणवत्ता की जाँच विभाग द्वारा की जायेगी। निर्धारित विशिष्टियों एवं गुणवत्ता के अनुरूप सामग्री पाये जाने पर आपूर्तिकर्ता से प्राप्त विपत्र का भुगतान किया जाएगा।
9. यदि सामग्रियों की जाँच में सामग्रियों की विशिष्टियों एवं गुणवत्ता निर्धारित मानक के अनुरूप नहीं पाई जाएगी तब इस स्थिति में विभाग द्वारा सामग्री वापस करते हुए BID Security के रूप में समर्पित FDR को जप्त कर लिया जाएगा।
10. आपूर्तिकर्ता के विपत्र से TDS&GST की कटौती के पश्चात् भुगतान किया जाएगा।
11. सामग्रियों के परिवहन पर होने वाले व्यय का वहन आपूर्तिकर्ता द्वारा किया जाएगा।
12. कोटेशनदाता को किसी भी अन्य विभाग एवं संस्था द्वारा Black List नहीं किया गया हो इस आशय का शपथ पत्र देना अनिवार्य होगा।
13. बिना कारण बताये किसी भी स्तर पर निविदा को रद्द करने एवं शर्तों में संशोधन करने का अधिकार विभाग के पास सुरक्षित रहेगा।


प्रशासनिक पदाधिकारी,
बिहार ग्रामीण पथ विकास
अभिकरण, पटना

Features	Qualifying Minimum Requirements
No. of Storage Units	1
Rack mount	NAS Controller Should be rack mounted with a form factor of not more than 2U
Processor	One 8 Core Intel 1.8GHz Intel Xeon Bronze 3408U
Memory	4 x 16GB Single Rank x8 DDR5-4800 Registered Smart Memory Kit, scalable to 192GB DDR5 RAM
Hard Drives	<ol style="list-style-type: none"> 1. Shall be supplied with minimum of 6 x 6TB SAS 7.2K LFF LP 512e HDDs in Raid 5. 2. Offered NAS Storage shall have separate dedicated dual 480GB M.2 or more NVMe SSD drives for Operating system in Raid 1+0. 3. Offered boot drive shall not consume any Disk bay slots.
Storage expandability	<ol style="list-style-type: none"> 1. Offered NAS controller shall support at-least 16 internal LFF Slots and shall be offered with at-least 12 LFF Slots. 2. Offered storage shall also have capability to attach additional drive enclosures. NAS shall support at-least 300TB using SAS / SAS -NL drives by providing associated hardware whenever required.
Network Connectivity	Minimum 4 x 1Gbps ethernet Base -T ports shall be provided in the NAS appliance
Protocols support	ISCSI, FTP, FTPS, CIFS/SMB 3.0, 3.02, 3.1.1, HTTP, HTTPS, NFS 4.1, WebDev etc.
Fault Tolerance for internal drives	Offered NAS shall support Raid 0, Raid 1, and Raid 5 for internal drives. Offered Raid controller shall have minimum of x16 Lanes and 8GB cache.
Fault Tolerance for external drives	Offered NAS shall support Raid 0, Raid 1, and Raid 5 for additional disk enclosures.
Network Client Types Support	Should support Windows 11, Windows 2019/2022, , HP-UX, AIX, SOLARIS, Linux etc.
Operating System	Microsoft Windows Storage IOT 2022 storage standard edition.
De-duplication	<p>Offered NAS shall have block based De-duplication which can be enabled for for all required volumes. De-duplication engine shall have:</p> <ol style="list-style-type: none"> 1. Flexibility to decide the multiple schedules when de-duplication process can be run. 2. Flexibility to limit the time period of de-duplication process so that production operations remains intact. 3. Flexibility to bypass the recent files under the de-duplication process so that production operations remains intact. 4. License for De-duplication shall be provided. 5. Shall support more than 64TB of file system for de-duplication.
File screening and quota management	<ol style="list-style-type: none"> 1. Offered NAS shall have support for file screening so that administrator can ensures that users shall not be able to store unwanted files on offered NAS device. 2. Offered NAS shall have Quota management for both Volume and Directory. 3. Software for both File screening as well as Quata management shall be provided.
File Management	<ol style="list-style-type: none"> 1. Shall have flexibility to expire or move files to different folder / Location / Volumes / drives on the basis of polices like day of creation / modification / access of on the basis of file pattern like extension. 2. Shall also be able to expire or move files to different folder / Location / Volumes / Drives on the basis of content classification within files.
SAN storage (iSCSI based)	Integrated iSCSI for block access over LAN.
Snapshots	Point in time copies of your data to guard against data corruption.
Encryption and compression	Shall have support for 256 bit encryption and Compression. License for both of same shall be offered.
Cloud Integration	<p>Offered NAS shall be able to integrate with Microsoft Azure - running with valid subscription with following features:</p> <ol style="list-style-type: none"> 1. Azure File Sync 2. Azure backup
Replication	Offered NAS shall also be supported with leading NAS replication softwares in the industry and shall also have 100TB license for replication through DFS-R
Web Based Management	Shall have web based interface to manage and monitor system health, capacity, performance, hardware events, quotas, snapshots, authentication and network services
Capacity Insights	Capacity planning with a granular historical utilization dashboard with growth rate and usage trends
FAN and Power Supply	Dual redundant Power supply and at-least 6 number of redundant FANs
Warranty and Support	NAS appliance should be provided with 3 Years 24 x 7 support

Firewall Specification	
General Requirements	<p>Network security appliance should support "Stateful" policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc.</p> <p>The proposed vendor must have a track record of continuous improvement in threat detection (IPS) and must have successfully completed NSS Labs' NGFW Methodology with a minimum exploit blocking rate of 99% . The Firewall product/ product family should have 99 % SECURITY EFFECTIVENESS certified by Cyber Rating Org for enterprise firewall</p>
Hardware & Interface requirements	<p>Appliance shall be ICSA certified for Firewall, IPS & Gateway Antivirus functionalities</p> <p>14 x 1GE RJ45 inbuilt interfaces, 8 x 1GE SFP slots, 4x 10G SFP+ slots populated with single mode transceiver. All the interface/slots should be available from day one</p> <p>The Appliance should have 1x USB & 1x Console Ports</p> <p>The Firewall should have redundant power supply from day one</p> <p>The Firewall should have min 400 GB or better local storage from day one.</p>
Performance and Availability	<p>The Firewall should support of 2,500,000 concurrent sessions, and 100,000 new sessions per second from day one.</p> <p>Minimum IPS throughput of 5000 Mbps for real world traffic or enterprise mix traffic</p> <p>Minimum Threat Prevention Throughput (measured with Application Control and IPS and Anti-Malware enabled) of 2500 Mbps for real world traffic or enterprise mix traffic</p> <p>IPSec VPN throughput: minimum 20 Gbps</p> <p>Simultaneous VPN tunnels: 1000</p> <p>Proposed solution must support minimum 3Gbps or better SSL Inspection throughput</p>
Routing Protocols	<p>Static Routing</p> <p>Policy Based Routing</p> <p>The Firewall should support dynamic routing protocol like RIP, OSPF, BGP, ISIS</p>
Firewall Features	<p>Firewall should provide application inspection for LDAP, SIP, H.323, SNMP, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, IMAP, NFS etc</p> <p>IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP</p> <p>Allows secure deployment of next-generation IPv6 networks, as well as hybrid environments that require simultaneous, dual stack support of IPv4 and IPv6</p> <p>The firewall should support transparent (Layer 2) firewall or routed (Layer 3) firewall Operation</p> <p>The Firewall should support multiple ISP link load balancing</p> <p>Firewall should support link aggregation functionality to group multiple ports as single port.</p> <p>Firewall should support static NAT, policy based NAT and PAT</p> <p>Firewall should support IPSec data encryption</p> <p>It should support the IPSec VPN for both site-site and remote access VPN</p> <p>Firewall should support IPSec NAT traversal</p> <p>Support for standard access lists and extended access lists to provide supervision and control</p> <p>Control SNMP access through the use of SNMP and MD5 authentication</p> <p>Firewall system should support virtual tunnel interfaces to provision route-based IPSec VPN</p> <p>The Firewall should have integrated solution for SSL VPN</p> <p>Should support LDAP, RADIUS, Windows AD, PKI based Authentication & should have integrated 2-Factor Authentication server support & this two factor authentication can be used for VPN users for accessing internal network from outside and for Local users accessing internet from inside the network and for administrative access to the appliance or all of them</p> <p>The solution should have basic server load balancing functionality as an inbuilt feature</p> <p>The appliance should support configuration of virtual firewall/virtual context with full functionality for at least 8 nos. from day one.</p> <p>Licensing should be a per device and not user or IP based (should support unlimited users)</p>
Integrated IPS Features Set	<p>IPS should have DDoS and DoS anomaly detection and protection mechanism with threshold configuration.</p> <p>Support SYN detection and protection for both targets and IPS devices.</p> <p>The device shall allow administrators to create Custom IPS signatures</p> <p>Should have a built-in Signature and Anomaly based IPS engine on the same unit</p> <p>Signature based detection using real time updated database & should have minimum 10000+ IPS signature database from day one</p> <p>Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)</p> <p>Signature updates do not require reboot of the unit.</p> <p>Configurable IPS filters to selectively implement signatures based on severity, target (client/server) and operating systems</p> <p>IPS Actions: Default, monitor, block, reset, or quarantine</p> <p>Should support packet capture option</p> <p>IP(s) exemption from specified IPS signatures</p>
Anti-Virus & Anti Bot	<p>Firewall should support antimalware capabilities, including antivirus, botnet traffic filter and antispysware</p> <p>Solution should be able to detect and prevent unique communication patterns used by BOTs i.e., information about botnet family</p> <p>Solution should be able to block traffic between infected host and remote operator and not to legitimate destination</p> <p>Should have antivirus protection for protocols like HTTP, HTTPS, IMAPS, POP3S, SMTPS protocols etc.</p> <p>Solution should have an option of packet capture for further analysis of the incident</p> <p>Solution should uncover threats hidden in SSL links and communications</p> <p>The AV should scan files that are passing on CIFS protocol</p> <p>The proposed system shall provide ability to allow, block attachments or downloads according to file extensions and/or file types</p> <p>NGFW should have cloud sandbox functionality to protect organization from Adance Persistence Threats. In case any</p>

	additional license is required, bidder has to include it in proposal from day one.
	NGFW should have functionality of Content Disarm and Reconstruction (CDR) to remove all active content from attachment in real-time before passing it to user.
	The proposed system should be able to block or allow oversized file based on configurable thresholds for each protocol types and per firewall policy.
Other Support	Should support features like Web-Filtering, Application-Control & Gateway level DLP.
	The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should support over 250 million webpages in 72+ categories and 68+ languages without external solution, devices or hardware modules.
	Should support detection over 3,000+ applications in multiple Categories: Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, social media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)
	The product must support Layer-7 based UTM/Firewall virtualization, and all UTM features should be supported in each virtual firewall like Threat Prevention, IPS, Web filter, Application Control, content filtering etc.
	The solution should have the flexibility to write security policies based on IP Address & Username & Endpoint Operating System
	QoS features like traffic prioritization, differentiated services, Should support for QoS features for defining the QoS policies.
	It should support the VOIP traffic filtering
	Appliance should have identity awareness capabilities
	The firewall must support Active-Active as well as Active-Passive redundancy.
	Solution must support VRRP clustering protocol.
	The NGFW shall support interface link monitoring failover
	The NGFW shall support external device ping probe failover
	The NGFW must have provision of fail-over in case of high memory utilisation on primary appliance.
	The NGFW should have SDN connector for Kubernetes, VMware ESXi and NSX, OpenStack, Cisco ACI, Nuage Networks and Nutanix Prism and AWS, MS Azure, GCP, OCI, AliCloud and IBM Cloud
	The NGFW should have capability to apply NAC profiles for onboarding clients into the default VLAN, NAC policies match clients based on device properties, user groups, or ZTNA tags, and then assign the clients to specific VLANs.
	The NGFW should be ZTNA ready from day one, all required license needs to be considered accordingly.
	The Proposed solution should be capable of extending firewall policy to access layer in future with native integration.
	The NGFW should have built-in 2FA server and at least two tokens for administrator login from day one.
Management Functionality	The firewall should have embedded web-based management functionality to configure without any additional software/hardware. The NGFW should support central management as well if required.
	Support accessible through variety of methods, including console port, Telnet, and SSHv2
	Support for both SNMPv2 and SNMPv2c, providing in-depth visibility into the status of appliances.
	Should have capability to import configuration and software files for rapid provisioning and deployment using Trivial File Transfer Protocol (TFTP), HTTP, HTTPS
	Solution must have different administrative profiles to choose to login in read-only or read-write mode
Warranty & Support	The solution must provide 3-year support for hardware and all required license for above-mentioned functionality