

Answer to Queries raised On NCB No.: DEoC/NCB/2078/79/01, Clarification in Technical Specifications in Bid Document

On NCB No.: DEoC/NCB/2078/79/01

Supply, Delivery and installation of Server, Firewall, Storage Area Network-SAN Storage and Network Switch

To the Professional Service Companies:

This is to inform all prominent service companies on queries and clarification on On NCB No.: DEoC/NCB/2078/79/01 **Supply, Delivery and installation of Server, Firewall, Storage Area Network-SAN Storage and Network Switch.**

Thank you very much for your time and interest, we look forward for your participation in bid process.

Sincerely,

**Department of Cooperatives
New Baneswor, Kathmandu**



Description of Goods	Particulars	Requirements	Suggested Changes	Remarks	Response
Firewall	General Requirements	The proposed solution must be recognized as a Leader in the latest Gartner Magic Quadrant for Network Firewalls from last 3 consecutive years.	The proposed solution must be listed in the latest Gartner Magic Quadrant for Network Firewalls from last 3 consecutive years.	The specification closely matches with only 1 OEM from the Gartner leader list. Please change this clause as the RFP should involve equal and more participation from other solutions as well.	As per Specification,As security is paramount and we require gartner leader product to protect our infrastructure
	Firewall	The proposed system shall have at least 800Mbps of Threat protection throughput	The proposed system shall have at least 4.5 Gbps	The Threat Protection throughput does not seem justifiable with the firewall throughput. Please align the threat protection throughput with the Firewall throughput.	As per specification vendor could propose higher than 800 Mbps
Particulars					
Switch	Warranty, Security and Service Support	Switch should be listed as leader in Gartner Magic quadrant for Wired and Wireless Infrastructure for current year	Switch should be listed in Gartner Magic quadrant for Wired and Wireless Infrastructure for current year	Please change this for Gartner approved products and fair participation for different solutions as well.	As per specification for product standarization

S.N.	Description of Goods	Particulars	Requirements	Requesting to change to	Justification	Response
3	Firewall	General Requirements	The proposed solution must be recognized as a Leader in the latest Gartner Magic Quadrant for Network Firewalls from last 3 consecutive years.	The proposed solution must be listed in the latest Gartner Magic Quadrant for Network Firewalls from last 3 consecutive years.	Asking for only leader limits to only few OEMs and less number of participants. Other brands are also listed in Gartner which are proven	As per Specification, As security is paramount and we require gartner leader product to protect our infrastructure
					technologies. Request to change this clause for more number of participation.	
4	Switch	Warranty, Security and Service Support	Switch should be listed as leader in Gartner	Switch should be listed in Gartner Magic quadrant for Wired and Wireless	Products listed in Gartner are tested, verified and genuine. Limiting it to the leaders only will reduce the number of participants.	As per specification for product standarization
			Magic quadrant for Wired and Wireless Infrastructure for current year	Infrastructure for current year		

1.1.1 Servers						
Sl. No.	Description of Goods	Particulars	Requirements	Change Request	Remark	Response
1	Rack Server including Vmware vSphere Standard Kit with 3 Years Subscription	Bus Slots	Server should feature minimum eight PCI- Express 4.0 slots with at least two x16 PCIe slots	support 3x PCIe 4.0 x16 slots	Since the server is only of 1U Rack space, so the requirement of eight PCI is physically unjustifiable.	
		Power Supply	Minimum 800W dual hot plug redundant low halogen power supplies	dual hot plug redundant power supplies	Watt should not be specific , it should be as server requirement.	As to have the server performance for the requested DISK,CPU and Memory minimum power of 800W vendors should propose 800 W or higher for the same
		System Security	UEFI Secure Boot and Secure Start support, Tamper-free updates – components digitally signed and verified, Immutable , Silicon Root of Trust, Ability to rollback firmware, FIPS 140-2 validation, Secure erase of NAND/User data, Common Criteria certification, TPM (Trusted Platform Module) 1.2 option, Configurable for PCI DSS compliance, TPM (Trusted Platform Module) 2.0 option, Advanced Encryption Standard (AES)	Management and configuration support via UEFI and OS-based tools. Industry-standard Advanced Encryption Standard (AES) NI support for faster, stronger encryption. Power-on password,	Specific to particular vendor.	As per the published specs, as these are basic and mandaotry Server haardware security requirements.

			and Triple Data Encryption Standard (3DES) on browser, Bezel Locking Kit option, Support for Commercial National Security Algorithms (CNSA), Chassis Intrusion detection option, Secure Recovery – recover critical firmware to known good state on detection of compromised firmware	administrator's password, Trusted Platform Module (TPM), supporting TPM 2.0 lockable front security bezel.		
		Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise- wide data encryption deployment.	<i>Specification seems to be specific to vendor , please help to generalize it.</i>		As per specification. As Encryprion is required in order to store data on the servers.
		Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature			As per specification. These feature is required as per to maintain the secueity of the server.It will make sure only signed firmware is loaded In server and no tamperig has been done.

			<p>should be immutable</p> <p>2. Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware</p>			
		Server Security	<p>Server should have storage space earmarked to be used as a repository for firmware, drivers and software components. Server should support agentless management using the out-of-band remote management port and should support multiple server management via single console using group virtual media and Encrypted Virtual Media. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support. System should have inbuilt features like one-button secure erase</p>			<p>As per specification. These feature is required as per to maintain the security of the server. It will make sure only signed firmware is loaded in server and no tampering has been done. As remote support is required for preventive and proactive support for the system to mitigate unwanted downtime and data corruption</p>

			designed to decommission/ repurpose servers and workload performance advisor designed for server tuning recommendations to improve server performance.			
		Server Management	<p>The remote management engine should have minimum 4 G Memory and 32Mb Flash</p> <p>Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources user is authorized to view.</p> <p>The Systems Management software should provide Role-based access control</p> <p>Zero Touch Provisioning (ZTP) using SSDP with remote access</p> <p>Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.</p>			As per specification,For remote management and device health checkup from the central platform for all the server hardware in data center,

2	SAN Storage	Raid Support	<p>1. Offered Storage Subsystem shall support RAID 0, 1, 5, 6, 10, DP+.</p> <p>Raid intermix should be supported within the array.</p> <p>2. All Raid Sets shall support thin provisioning.</p> <p>3. Disc groups should support different capacity discs in a RAID Pool</p> <p>4. Should support distributed spare capacity without the use of traditional spare drives technology.</p> <p>5. Should support erasure coding to ensure high performance, availability, and very fast rebuild times.</p>	Storage should support Equivalent RAID configuration with DP , Erase coding and thin provisioning		As per specification,As based on various data type various raid level security is required.
		Vendor Recognition	Vendor should be recognised as Leader in latest Gartners Magic Quadrant for Primary Storage for the current year. Manufacturer Authorization Letter should be provided by the bidder if the bidder is not the manufacturer of the SAN Storage .	Vendor should be listed in Gartner Magic Quadrant for Primary Storage for the current year.	Components listed in gartner are themselves tested, verified and genuine products.	As per specification for product standarization
3	Firewall	General Requirements	The proposed solution must be recognized as a Leader in the latest Gartner Magic Quadrant for	The proposed solution must be listed in the latest Gartner	There are only Fortinet, Checkpoint	As per Specification,As security is paramount and we require gartner leader product to protect our infrastructure

			Network Firewalls from last 3 consecutive years.	Magic Quadrant for Network Firewalls from last 3 consecutive years.	and Palo Alto in the gartner leader from last 3 consecutive years. Moreover the specification aligns with one of the OEM in this list. Therefore, components if are listed in Gartner, they are themselves tested, verified and genuine product.	
		Firewall	The proposed system shall have atleast 800Mbps of Threat protection throughput	The proposed system shall have atleast 5 Gbps	With the firewall having 10 Gbps throughput, the asked Threat protection throughput	As per specification vendor could propose higher than 800 Mbps

					is very low. Since every subscription asked will increase the threat protection throguput it should be at least 50% of the Firewall throughput.	
--	--	--	--	--	---	--