

Question & Answers
Response to Requests for Clarification
TURAN/SUP/ITB/007/2024

Question 1: According to Lot 6, item 59. "Post installation support will be provided as necessary." Since this article does not include the scope of support, it causes uncertainty. If the context of the support (update, configuration, etc.) and SLA (7x24 or 5x8 etc.) are written, it will be easier for us to determine the effort for the support.

Answer 1:

User Trainings: Providing training to the IT team at the Institution's location on the management and features of the new firewall device.

Regular Maintenance: Planning periodic updates and maintenance of the firewall device. Providing 24/7 support in case of malfunction. Preparing an intervention plan within 1 hour and implementing the said plan (except for hardware malfunctions).

Support and Backup: Health checks of the device at the Institution's location will be conducted by expert personnel once a month for 3 years, improvement and tightening steps will be taken and the report to be created will be shared with the Institution. A regular backup strategy will be established and implemented.

Question 2:

Lot 1: Server Capacity Expansion & Lot 2: Data Storage System Capacity Expansion

5. The added components will have a warranty period of 3 years, and 7 days/24 hours customer support. Malfunctions will be addressed within 4 hours. The warranty/customer support needs to be documented at the time of bidding proposals.

In order for this article to be applied to Lot 1 and Lot 2, the serial numbers of the server and storage devices belonging to the end user must be transmitted. The warranty status of existing server and storage devices is the same as the warranty status of the products with the desired specification to be added to it. If the warranty of the existing devices has expired, the warranty of the offered products is deemed to have expired. I would like you to know that no company can give a price quote if the serial numbers are not shared.

Answer 2:

Server (HPE DL380 Gen10 Plus)

Server Serial Number: CZ230309QH

Server Serial Number: CZ230309QG

Server Serial Number: CZ230309QF

Server (HPE DL580 Gen9)

Server Serial Number: CZJ620086S

Server Serial Number: CZJ620086M

Server Serial Number: CZJ620086P

Server Serial Number: CZJ620086X

Server Serial Number: CZJ620086R

Server Serial Number: CZJ620086V

Server (HPE Apollo 6500 Gen10 Plus)

Server Serial Number: CZ23090F9H

Storage Unit (HPE MSA 2060)

Controller SKU Serial Number: ACV247W49Z

Enclosure SKU Serial Number: ACV311W2MR

Question 3:

Lot 4: Ethernet Switch - Type 2 (2 units)

7. With each switch, the following transceivers and DACs will be provided in the proposal:
- 10 units of 25Gb SFP+/SFP28-SFP+/SFP28 3m DAC
 - 2 units of 40G QSFP+/QSFP28 LC BiDi MM transceivers
 - 1 unit of 100G QSFP+/QSFP28-QSFP+/QSFP28 1m DAC

OEM products shall not be accepted under any circumstances.

We are noticing that the highlighted clause above does not include a clause number.

Thus, we are assuming the following:

7. With each switch, the following transceivers and DACs will be provided in the proposal:
- 10 units of 25Gb SFP+/SFP28-SFP+/SFP28 3m DAC
 - 2 units of 40G QSFP+/QSFP28 LC BiDi MM transceivers
 - 1 unit of 100G QSFP+/QSFP28-QSFP+/QSFP28 1m DAC
 - OEM products shall not be accepted under any circumstances.

Accordingly, we will make sure that the brand of the units defined in a., b. and c. (sub sections of clause 7) will be the same with the brand of the switch (Lot 4: Ethernet Switch - Type 2 (2 units)) itself. Will this be sufficient to fulfill this clause?

Answer 3: Yes, it will be sufficient.

Question 4:

Lot 1: Server Capacity Expansion

- - 6. The supplier is expected to be an authorised HP dealer or reseller for the required HP branded products. This is required to ensure compatibility and functionality with the existing infrastructure.

Lot 3: Ethernet Switch - Type 1 (2 units)

- - The supplier is expected to be an authorised HP dealer or reseller for the required HP branded products. This is required to ensure compatibility and functionality with the existing infrastructure.

HP has been divided into 2 companies in 2015: HP Enterprise (HPE; datacenter equipment such as servers, storage, networking etc.) and HP Inc. (HP; end user products such as laptops, PCs, printers etc.). As Lot 1 and Lot 3 defines products in the enterprise (datacenter) domain, can we assume that “HP” in the clauses above actually means “HPE”?

Answer 4: Yes, we should assume “HP” in the clauses above includes HPE.

Question 5:

We are currently in the process of preparing our proposal for the [ITB/007/2024] involving the procurement of firewall (FW) hardware as outlined in the provided specifications. However, it has come to our attention that the detailed scope of services and support required for the FW beyond the hardware procurement, is not explicitly defined in the tender documents.

To ensure that we accurately assess the necessary effort, human resources, project planning, and associated costs, we kindly request clarification on the following:

1.

Scope of Services: Could you please provide a detailed description of the specific services and technical support that are expected to be delivered during the FW procurement process?

2.

Expected Deliverables: Are there any particular milestones, documentation, or performance criteria that should be met as part of this service?

3.

Post-Delivery Support: What are the expectations regarding post-delivery support, including any required service levels or response times, SLAs?

Clarification on these points will enable us to provide a more precise and comprehensive proposal that aligns with your expectations.

Answer 5: Answers to Question 1 and Question 6 answer this.

Question 6: For the installation of Firewalls can you please clarify the work that needs to be done to enable us to calculate the correct time consumption. Specifically, we need information on the way the firewalls should be coupled together and whether you need the following to be part of the installation:

- a. IPSEC Connections
- b. DMZ / DNAT setup
- c. Core og WAN switch installed and ready for use?
- d. SSLVPN setup

Answer 6:

Since the device in question is of critical importance for the Institution and a security device, the company that will perform the installation and transition will be a company approved by the Institution. However, expect the following steps to be followed for the installation and transition operation.

Preparation and Planning for Transition

- **Review of Network Topology and Security Policy:** A detailed analysis of the current firewall configuration, rules, network topology, and all configurations such as NAT, VPN, IPSEC, SSL VPN will be made.
- **Assessment of the Capacity and Features of the New Device**
- **Transition Plan and Timeline:** Determining when the transition will take place, which steps will be taken in what order, possible downtime, and the measures to be implemented during these periods.
- **Recall Plan:** Creating a recall plan to revert to the old device if a problem is encountered during the transition; Preparing a plan to restore the system with no or minimal downtime

Backing Up Current Configuration

- **Backup:** Backing up all configuration files on the current firewall device. This will include rules, policies, VPN settings, NAT rules and any other configurations.
- **Documentation:** Preparing a complete documentation of the current configuration and sharing with the Institution the document which will be used as reference when creating the same configuration on the new device.

Installing the New Firewall Device

- **Physical Installation:** Installing the new firewall device and establishing network connections
- **First Configuration:** Configuring the new device to be functional by setting basic network settings (IP addresses, management interface, access rights, etc.)
- **Updates and Licenses:** Updating the software of the new firewall device and activating all necessary licenses.

Moving Existing Configuration to New Device

- **Transfer of Rules and Policies:** Planning to transfer security rules, NAT settings, VPN tunnels and other policies from the existing device to the new device manually or with automatic migration tools
- **Customization:** Assessing the additional features and security measures offered by the new device and adding them to the configuration. Also, optimizing the configuration using features that are not available on the old device but are available on the new device.

Testing and Validation

- **Functional Tests:** Testing all critical functions of the new firewall device. Control of basic operations such as internet access, VPN connections, security rules and application filtering
- **Security Tests:** Performing penetration tests to ensure the security policies are working as expected
- **Performance Tests:** Testing network performance and device performance under load.

Conducting an assessment to identify improvements or possible performance problems by comparing with the current device

Conducting the Transition

- **Planned Transition:** Routing traffic from the existing firewall to the new firewall at the previously planned transition time. Scheduling work to ensure it is performed with little to no interruption.
- **Tracking and Monitoring:** After the transition, regular monitoring of the new firewall device and planning and implementing actions that will regularly improve network traffic, security events and performance.

Question 7: In item 13 on the Firewalls, the requirement is for 4 SFP+ modules. Is that per firewall or in total?

Answer 7: It is the total requirement. 4 SFP+ modules are required, 2 for each firewall device.

Question 8: It is kindly requested to extend the deadline.

Answer 8: The deadline was extended until 7 October 2024, 23:50 GMT+3