معنا .. اتصالك أسهل

2015

YM Unified Networks Administration & Monitoring System

مواصفات نظام ادارة ومراقبة الشبكات الموحد:

BOQ of Unified Networks Administration and Monitoring System:

N	Item	License fee
1	Main Network Monitoring system	License fee for 1,000 Network Nodes with unlimited number of interfaces.
2	Network flow and traffic analyzer	License fee for 200 interfaces.
3	Network Configuration Manager	License fee for 300 Network Devices.
4	Log and Event Manager	License fee for 250 Nodes.
5	Switch Port Management and Users Tracking	License fee for 5,000 switch ports.
6	Network Topology Mapper	
7	Network Troubleshooting and Diagnostic Basic tools	
8	IT Remote support for helpdesk	License fee for 5 technicians.
9	Data Base Software with licenses	
10	External Training for 3 Persons	Annex-1
11	Installation & Engineering & Testing	
12	2-year support and maintenance	

A. Bidders Qualification:

Any bidder could consider himself as a qualified bidder has the right to participate at the bidding activity if he submits the required information and Evidence documents as following:

- A qualified bidder is *a Sole Agent of an authorized representative of a worldwide specialized company for network monitoring product* and of a good reputation in the Designing, Supplying, Implementing , Support and Maintenance of "Unified Networks Administration and Monitoring System" .
- He has an experience in this field for a period over 8 years.
- The manufacturer of the system must be a specialized in this area for a period of not less than 15 years.
- He had implemented at least 3 successfully Unified Networks Administration and Monitoring System Projects.
- Yemen Mobile company has the right to enquire about the correctness of submitted information and is asking for a referee names and addresses at the executed projects to be attached to the Evidence Documents.

B. Scope of the Supply, Installation & Commissioning:

- The Server that will be used for installing the system is available with OS and should NOT be included in the offer.
- The Vendor/Supplier shall be responsible for preparing the environment for the system that include all configuration, installation, commissioning, inspection, testing, and documentation at all monitored nodes and the centralized server. And must be approved by Yemen Mobile.
- This specifications are in general in nature and shall be read in conjunction with data sheets that will be provided.
- Any omission in this specification shall not relieve the Vendor/Supplier of his responsibility to deliver a completed "Unified Networks Administration and Monitoring System", which are of proven design, complete and conform to the quality assurance requirements specified and which will operate satisfactory.
- The Vendor/Supplier shall also supply any components/accessories that are not specifically mentioned, but are required to ensure satisfactory functions of the equipment, in accordance with this specifications and documents.

- Tools and equipment required for complete system installation, testing and operation, commissioning, start-up and operation also should be in vendor scope of supply.
- IP Surveillance System equipment's and installation must be supplied and installed in all applicable standards and from a good materials.
- Installation & Configuration should be performed according to applicable standards and **security** principles.
- The system proposal must include total pricing for planning, installation, configuration, documentation and user training for the complete system.
- Supplier shall submit documentation in accordance with the requirement of company requisition.
- The supplier shall submit for approval, all listed Planning/drawing/documents, strictly in accordance with the agreed schedule and program.

C. General Term Conditions:

- The proposed system must provide a complete and comprehensive solution.
- The system should be provided with the latest stable version of all products that offered by the system's company.
- The offer should include technical support and product updates at least for one year And license keys never expires.
- The full system should provide main and details features below (at Technical Specification part) with any categorization, order, and division. And what's matter is that the full proposed system should have these features.
- All the required systems should belong to the same network monitoring system company and work as a unit except the following parts:
    - Network Troubleshooting and Diagnostic Basic tools.
    - IT Remote support for helpdesk.
    - Database Software.
- The company should provide all function lists and technical specifications for all proposed systems.

D. Technical Specification:

The Unified System should support the following general specifications:

- The system should use a separate database.

- The database that integrated with system must be from database company (ex: oracle, MS SQL,…)
- The database license should be included in the offer.

And as in the following table:

N	Requirement	Details
1	**Business Size**	Medium Businesses
2	**Deployment Model**	Premise / Client-Server
3	**Server Platform**	Windows
4	**Client Platforms**	Windows
5	**Maximum Manageable Nodes supported.**	At least 4,000 Nodes with unlimited number of interfaces.
6	**Licensing Details**	1,000 Nodes with unlimited number of interfaces.
7	**Multi-Vendor Support**	Yes, especially ("Cisco, Huawei, firewall juniper, F5" network's devices)
8	**Network Discovery**	Yes, (Automatic and Manual)
9	**Notifications**	Email, SMS, Run scripts
10	**IPv6 Support**	Yes
11	**Syslog**	Yes (and included at offer)
12	**SNMP Logging**	Yes (and included at offer)
13	**Route Monitoring**	Yes
14	**Reporting**	Built-in and customizable reporting
15	**User-Customizable Reporting Scenarios**	Yes
16	**User-Customizable UI/Dashboards**	Yes

And with the following details descriptions:

1) Network Monitoring system:

The System should has the following features:

- Monitors network device and interface availability and performance indicators, such as bandwidth utilization, packet loss, latency, errors, discards, CPU, and memory for SNMP and WMI-enabled devices.
- Get summary of network and application performance metrics. Quickly identify reductions or changes in application performance and determine if the change is caused by the application or the network.
- Schedule network scans from an easy-to-use, identifying new network devices and ensuring you are monitoring all of your critical equipment.
- Available to customize network maps and automatically view connections, layer-2 link utilization between devices and their real-time status.
- Multi-vendor device support.
- Monitoring, alerting, and reporting on the state of key device sensors including temperature, fan speed, and power supply.
- Deploy packet analysis sensors using a step-by-step wizard to monitor application and network performance.
- Configure alerts accurately by calculating dynamic baseline threshold data.
- Centralized and customizable network operations center (NOC).
- Get a central view for all of the notification messages about network’s performance.
- Monitor network route information and receive alerts when issues arise, and get a combined view of real-time network route information alongside device information.
- Alerts system should be by email, SMS, and web reports.

2) Network flow and traffic analyzer

The network flow and traffic analyzer should have the following features:

- Delivers an instant alert notification, including a list of “top talkers”, when an interface exceeds its bandwidth utilization threshold.
- Provides valuable insights into which applications are consuming the most network bandwidth and tracks application traffic arriving from designated ports, source IPs, destination IPs, and even protocols.

- Supports devices from Cisco, Juniper, Huawei, and other leading vendors
- Supports NetFlow traffic from VMware vSwitch
- Analyzes NetFlow v5, NetFlow v9, and Huawei NetStream data.
- Determines which flows are representative of the majority of bandwidth

3) Network Configuration Manager

The system should have the following features

- Identify and repair unauthorized and failed network configuration changes.
- Allows to receive real-time alerts when configurations change
- Allows to simultaneously change a community string, modify an access control list, or block a MAC address
- Easily executes advanced config changes
- Allows to archive your configuration, inventory, and policy data within a secure database.
- Allows to request approvals before making sensitive changes to devices.
- Protects against unauthorized network configuration changes
- Automatically scans your entire network and imports discovered devices into its database for fast and easy deployment.
- Generates a detailed network inventory of all managed devices, including serial numbers, port details, IP addresses, and more.

4) Log and Event Manager

The system should have the following features

- A log source could be a server (eg: Oracle server, Citrix server) or a device (eg: router, switch) or an application (eg: active directory, IIS, Apache)>
- Collects, consolidates, and analyzes logs and events from security and security-relevant applications and devices
- Analyzes activity to identify attacks in real time
- Collects and catalogs log and event data in real-time from anywhere data is generated within your IT infrastructure. Explore the supported data sources.
- Supports root cause analysis with built-in intelligence that applies to networks, applications, and security management
- Log & Event Manager's advanced ad-hoc IT search capability makes it easy to discover issues that tracks events instantly.

- Enables to immediately respond to security, operational, and policy-driven events using built in active responses that take actions such as quarantining infected machines, blocking IP addresses, killing processes, and adjusting Active Directory® settings.
- Makes it easy to generate and schedule compliance reports quickly using audit-proven templates and a console that lets customize reports for organization's specific compliance needs.
- It should be multivendor for all IT devices

5) Switch Port Management and Users Tracking:

The System should has the following features:

- It should provide a detailed switch port usage data, capacity analysis, and built-in reporting.
- It should map and monitor switch ports.
- It should track the location of a user on the network and retrieve connection information including switch name or access point, port or SSID, connection duration, as well as endpoint connection history.
- It should automatically discovers, maps, and monitors switches, ports, and network devices.
- It should enables searching on IP address, hostname or MAC address to track endpoints.

6) Network Topology Mapper:

The System should has the following features:

- It should automatically discovers entire network and creates comprehensive, detailed network maps. also node details of map objects can be edited and connect network devices manually.
- It should automatically detects new devices and changes to network topology with scheduled network scanning.
- It should support exporting maps to common formats (ex: Microsoft Office Visio, PDF, and PNG formats).
- It should be able to performs multi-level discovery to produce an integrated OSI Layer 2 and Layer 3 network map that includes detailed device information.
- It should generates inventory and network reports.

7) Network Troubleshooting and Diagnostic Basic tools :

The offer should provide a collection of essential and basic tools for troubleshooting and diagnose networks problems like following:

- A multi-threaded TFTP server commonly used to upload and download executable images and configurations to network's devices.
- Syslog Server that can sends and receives syslog messages and decode the messages for logging purposes.
- Port Scanner that used for testing open TCP ports across IP addresses, port ranges, or a selection of specific machines and ports.
- Ping Sweep that used for scanning a range of IP addresses to display which addresses are in use and to perform reverse DNS lookups.
- SNMP Sweep that used for querying an IP address range to locate used and unused IP addresses; obtain data about each system in the range.
- DNS Analyzer that visually displays the hierarchy of DNS resource records, including name server, CName, and pointer.
- Network Sonar that produces a detailed network inventory in just minutes and generate reports using built-in templates.
- MAC Address Discovery that used to scan subnets and construct a table relating IP addresses to MAC address, DNS, and manufacturer address.
- DHCP Scope Monitor that polls DHCP servers to extract IP scopes and highlight scopes low on dynamically assigned IP addresses.
- Bandwidth Gauges that display bandwidth statistics in real time for data being received and transmitted for any remote network device.
- CPU Gauges that monitor CPU load on network devices and workstation computers via SNMP.

8) IT Remote support for helpdesk.

The System should has the following features:

- It should be able to view windows clients' desktops for troubleshooting them or making specific configurations.
- It should support quickly establish a remote connection to your clients' desktop and make the necessary changes.

- It should enable working as if we are in front of that computer and can also have multiple simultaneous connections to work collaboratively.

E. Warranty

- Guarantee Systems under these specifications.
- The supplier shall be responsible for providing a local support & maintenance and contacting with the system's company if needed.
- Two year technical support and maintenance for all systems.
- The supplier company should have a system and network specialists and the company will guarantee appropriate support to solve problems with systems or contacting the system's company in appropriate time.
- The supplier company should guarantee providing a regular maintenance to make sure that all systems work in appropriate way during the support and maintenance period.

Annex-1
Training Course

General Outlines:

1. NETWORK PERFORMANCE MONITOR
   a. System Architecture
   b. System Installation & configuration
   c. System Management & administration
   d. Alert definition
   e. Threshold definition
   f. Report definition & analysis
2. Network flow and traffic analyser
   a. System Architecture
   b. System Installation & configuration
   c. System Management & administration
   d. Traffic analysis.
   e. Report definition & analysis
3. Network Configuration Manager
   a. System Architecture
   b. System Installation & configuration
   c. System Management & administration
   d. Work with network equipment & VLANs.
4. Log and Event Manager
   a. System Architecture
   b. System Installation & configuration
   c. System Management & administration
   d. Work with logs & Events from network devices
   e. Work with logs & Events from windows, Linux , Unix , oracle & Citrix servers.
   f. Report definition & analysis
   g. Log analysis
5. Switch Port Management and Users Tracking
   a. System Architecture
   b. System Installation & configuration
   c. System Management & administration
6. Network Topology Mapper
   a. System Architecture
   b. System Installation & configuration
   c. System Management & administration
7. Network Troubleshooting and Diagnostic Basic tools
   a. System Architecture
   b. System Installation & configuration
   c. System Management & administration
8. IT Remote support for helpdesk
   a. System Architecture
   b. System Installation & configuration
   c. System Management & administration