

GOVERNMENT OF INDIA
(Ministry of Home Affairs)
DIRECTORATE GENERAL
CENTRAL RESERVE POLICE FORCE
EAST BLOCK-7, SEC-1, R.K. PURAM, NEW DELHI-110066
(Tele/Fax No-011-26107493, Email-Id: comncell@crpf.gov.in)

No. B.V-7-C/2023-24-C (QRs)

Dated, the Febraury'2024


23

Subject:- REQUEST FOR COMMENTS OF
STAKEHOLDERS/OEM/FIRMS ON QRs (QUALITY
REQUIREMENT) & TDs of "Networking Management System &
Networking Auditing Tools".

3. The QRs/TDs of "Networking Management System & Networking Auditing Tools" is attached as **Appendix 'A'**. The OEMs/Vendors are requested to forward information of the product, which they can offer and also forward correct specifications of their system against each parameter. Only complied or not complied remarks will not be accepted. The firms are also requested to furnish the following details:-
- Whether you are OEM/Vendor?
 - If vendor details of OEM.
 - Authorization certificate from OEM.
4. The required information/details may please be forwarded at the following addresses by 9TH March'2024.

Communication Directorate ,CRPF
East Block-7, Sec-1, R.K. Puram, New Delhi-110066
Email: comncell@crpf.gov.in

3. An early response is requested.


{Sunil Kumar Singh, DC(Comn)}
For DIG (Equipment)
Directorate General, C R P F

Draft QRs/TDs of Network Monitoring System

S.No	Parameters	Specifications	Trial Directives
a. Network Performance Monitoring, Fault & Availability Management			
1	It should provide integrated fault reporting, performance Monitoring, Configuration & compliance Management together in one tool		BOOs will check and confirm
2	Monitoring across heterogeneous user network with multi-OEM devices monitoring and management supported	Tabular and Graphical trend analysis	BOOs will check for subset network
3	Trend analysis of stored historical records		BOOs will check and confirm
4	Identify, analyze network latency issue	Causing internet or application lag	BOOs will check and confirm
5	Monitoring of Network metrics	Packet loss (TTL may be customized), Errors, Discards, Interface traffic volume, Interface packets count, Response time etc.	BOOs will check and confirm
6	Overall hardware monitoring capability	Including temperature; Fan Status; Power Status; Power Consumption of standalone and IT infrastructure etc. Depending upon inputs provided by respective device	BOOs will check and confirm
7	To be pre - integrated, centralized and consolidated platform to manage network devices		BOOs will check and confirm
8	Supported protocol to communicate the devices	SNMP, ICMP, NetFlow, HTTP, Ping, SMTP, POP3, WMI, JMX, SOAP, REST API, PDC, SSH, Telnet, or any other protocol defined by user	OEM to certify
b. Network Configuration & Change Management			
1	Identification of configuration changes / policy violations/ inventory changes across multi-vendor network tools.		BOOs will check and confirm

S.No	Parameters	Specifications	Trial Directives
2	Device configuration capture and validation	<ul style="list-style-type: none"> The proposed solution be able to perform real-time or scheduled capture of device configurations. Upload and thereby detect inconsistent “running” and “start-up” configurations and alert the administrators. Tool supports automated Change Plans including but not limited to: Conditions to validate, Pre-Change Validation, Change Script (similar to legacy Command Script), Post-Change Validation, Rollback Script. 	BOOs will check and confirm
3	Feature of “load & merge” configuration changes to multiple network devices		OEM to certify and BOOs will check and confirm
4	Automate Network Operations and Orchestration	Able to restart selected Switches or Routers	OEM to certify and BOOs will check and confirm
5	Configuration Backup	<ul style="list-style-type: none"> Capable to perform device configuration backup, maintain history by tracking changes, and compare versions from a centralized web GUI. Capable to perform scheduled backup of configuration from network devices and backup files are to be centrally stored and organized by device and version. Capable to generate alerts for failed configuration backup. Capable to generate configuration backup reports. 	OEM to certify and BOOs will check and confirm
6	The solution must support rollback to a previous configuration and should maintain at least three previous versions and/or configurations		BOOs will check and confirm
7	Ability to perform a textual configuration search using regular expression pattern matching		BOOs will check and confirm

S.No	Parameters	Specifications	Trial Directives
8	Tool should allow remote access to internal network devices via remote management system without using VPN or agent	<ul style="list-style-type: none"> • Tool should record session for further audit with single sign-on • Capable to do white listing of devices and two-factor authentication 	BOOs will check and confirm
9	Tool should have IP Address Management (IPAM) facility (to be checked for end points)	Complete IP Discovery, IP Management, Historical Tracking and Grouping and sub-grouping.	OEM will certify and BOOs will check and confirm
c. Network Traffic Analysis			
1	Capture, track & analyze traffic	Flowing over the network via different industry standard traffic capturing methodologies viz. NetFlow, jflow, sFlow, IPFIX etc.	OEM will certify and BOOs will check and confirm
2	To provide key performance monitoring capabilities by giving detailed insight into the application traffic flowing over the network.		BOOs will check and confirm
3	Able to monitor network traffic utilization, packet size distribution, protocol distribution, application distribution, top talkers etc. for network traffic.		BOO will check and confirm
4	To collect and report the real-time network flow.	Data from devices across the network and provide reports on traffic based on standard TCP/IP packet metrics such as Flow Rate, Utilization, Byte Count, Flow Count, TOS fields etc.	BOO will check and confirm
5	Route tracing and link quality monitoring		BOO will check and confirm
6	Traffic and bandwidth usage monitoring		BOO will check and confirm
7	Capable to support NBAR (Network based Application Recognition) or similar protocols. Capable to provide QoS (Quality of Service) based Monitoring and reporting.		BOOs will check and confirm

S.No	Parameters	Specifications	Trial Directives
d. Network Mapping Tools			
1	Graphical representation of network nodes and the links between them	Network nodes may include routers, switches, firewalls, and other devices. Network mapping can be used to produce an overview of a network or just a portion, typically showing the current status and other key pieces of information for all devices connected to the network.	BOOs will check and confirm
2	Mapping logical and physical network in one tool	<ul style="list-style-type: none"> • Monitoring SDN environment directly from primary monitoring tool. • Displays a map of physical and logical relationships between entities which is Auto-generated or created from scratch. 	BOOs will check and confirm
3	Visual display of traffic pathways	As traffic travel between nodes from source computer to their destination	BOOs will check and confirm
4	Network path analysis	To have a deep visibility into critical network paths. It allows to visually understand traffic at each node, isolate data latency, perform root cause analysis to eliminate problems.	BOOs will check and confirm
5	Logical grouping of network nodes	<ul style="list-style-type: none"> • Connected routers/interfaces together - aggregate views of routers according to services such as email, location, department, or manufacturer to roll up service-level status across organization. • Templates based device classification and monitoring • Business Views for custom grouping of devices • Automatically/Manual grouping of devices into element type, location and severity etc. 	BOOs will check and confirm
6	Map relationships between virtual Port Channels (vPCs/LACP/MLAG or equivalent), and monitor and backup every virtual device context of switches		BOO will check and confirm

S.No	Parameters	Specifications	Trial Directives
7	Automatic Layer 2/ Layer 3 Network Maps	Allow creation of custom maps using available network devices so that the L2/L3 network connections between all selected devices are automatically created.	BOO will check and confirm
8	Utility to draw links on the network maps		
9	Should provide network outages and other error conditions on visual topological map		
10	Tool should have a capability to create a manual network diagram	Diagram should be representing live devices	
11	Tool should support panel view functionality	Panel view should show device model, interface with status	
e. Network Reporting Analysis			
1	Able to collect and collate information regarding relationship between IT elements and business service, clearly showing how infrastructure impacts business service levels		BOOs will check and confirm
2	Web-based interactive reporting for business users, Rich graphical report designer for power users, Parameterized reports with charting.		BOOs will check and confirm
3	Centralized Reporting & Dashboard	<ul style="list-style-type: none"> • The Dashboard and reporting engine provides centralized view as the face of all the elements in the IT (network, server, application and database) • Reporting in graphical as well as tabular format • Output in popular formats: HTML, Excel, CSV, PDF etc. 	BOOs will check and confirm

S.No	Parameters	Specifications	Trial Directives
4	Report configuration	<ul style="list-style-type: none"> • To easily create, view, and edit reporting schedules as needed for specific departments or recipients • whether it will automatically be emailed, printed, or saved by user profile • for building additional reports • customizable reporting • Integrated report editor • Utilization of out-of-the-box reporting templates • Report Scheduling 	BOOs will check and confirm
5	Report exporting	Reporting data capable to export to HTML, PDF, XLS, CSV etc. file formats.	BOOs will check and confirm
6	Network Link utilization, Bandwidth utilization and down time report		BOOs will check and confirm
7	Reporting capabilities	All performance threshold breaches for a specified period of time, all performance threshold breaches for a specified group of devices, WAN link availability, WAN performance statistics - bandwidth consumption, round-trip-latency, packet loss, jitter etc.	BOOs will check and confirm
f. Alerting			
1	Device/link fault or network performance degradation alert		BOOs will check and confirm
2	Alert notification via E-mail, SMS and syslog		BOOs will check and confirm
3	Alert prioritization. Network alert software should focus on critical alerts that have high network impact.		BOOs will check and confirm
4	Suppression of non-critical alerts as per need		BOOs will check and confirm
5	Flagging certain conditions with custom actions such as sending an email, text, audio alerts, or executing an external program		BOOs will check and confirm
6	Nested trigger conditions as per defined parent/child dependencies		BOOs will check and confirm

S.No	Parameters	Specifications	Trial Directives
7	Identification and suppression of alerts for duplicated events		BOOs will check and confirm
8	Pre-defined alerts for typical network problems		BOOs will check and confirm
9	Configuring alerts/notifications to provide the detailed information including interface and node name, the date and time when the alert occurred, the alert severity etc.		BOOs will check and confirm
10	All alerts to be recorded in a database for easy, efficient and future retrieval		BOOs will check and confirm
g. Wireless Device Monitoring (OPTIONAL AS PER USER REQUIREMENTS)			
1	Monitor faults and manage key performance metrics across wireless network		BOOs will check and confirm
2	Creation of a library for custom Wi-Fi heat maps within the Network Performance Monitor dashboard		OEM will certify and BOOs will check and confirm
3	Wireless access point discovery	<ul style="list-style-type: none"> The Wi-Fi network analyzer automatically recognizes and begins polling your wireless APs and controllers as soon as they are added. Gain information about access points like name, type, SSID, and connected clients. View similar details about each client, as well as MAC address, signal strength, time connected, data rate, bytes received/transmitted etc. 	BOOs will check and confirm
h. Discovery of network devices			
1	Automatically discover network paths and nodes through ICMP, SNMP and WMI protocols		BOOs will check and confirm
2	The tool supports for SNMP traps		BOOs will check and confirm

S.No	Parameters	Specifications	Trial Directives
3	Scheduled discovery and CSV bulk discovery		BOOs will check and confirm
4	Network discovery rule engine		BOOs will check and confirm
5	Filters in discovery		BOOs will check and confirm
6	Layer 2 discovery		BOOs will check and confirm
7	VLAN discovery		BOOs will check and confirm
8	IP Printer availability		BOOs will check and confirm
9	Support for adding custom device types		BOOs will check and confirm
10	TCP Based Status Polling (for Non ICMP Environment)		BOOs will check and confirm
11	The solution should have the capability to accurately discover and classify assets connected in the network and auto comparing the total count with the previously discovered assets scan to report newly discovered assets.		BOOs will check and confirm
i. Server Monitoring (OPTIONAL AS PER USER REQUIREMENTS)			
1	The solution should support Monitoring of VMs from major vendors/OEM like VMware, Microsoft etc.		OEM will certify and BOOs will check and confirm
2	The solution should Monitor effective utilization of critical resources like CPU, Memory, Network and storage		OEM will certify and BOOs will check and confirm
3	Supports monitoring of hardware health such as temperature, voltage, power, fan speed, status of processors etc.		OEM will certify and BOOs will check and confirm
4	Take charge of your virtual machine monitoring on the go with instant notifications via SMS or email on performance hiccups, faults and downtime		OEM will certify and BOOs will check and confirm
5	Capable to support Virtual Machine, Hypervisor and Cluster monitoring		OEM will certify and BOOs will check and confirm

S.No	Parameters	Specifications	Trial Directives
6	Capable to monitor availability and performance of web server, email server and database server etc.		OEM will certify and BOOs will check and confirm
7	Tool should support OS and other applications services and processes monitoring	HTTP service, HTTPS service, FTP server statistics, POP/SMTP services, ICMP services etc.	OEM will certify Monitoring of available services will be assessed by BOOs. BOOs will check and confirm
j. Network Vulnerability Auditing Tool (OPTIONAL AS PER USER REQUIREMENTS)			
1	The solution should continuously check for vulnerabilities on network device operating system and report it to administrator via email or GUI dashboard	<ul style="list-style-type: none"> Regular check for updates of the vulnerability by the OEM Identify device vulnerabilities and provide provision for upgrade framework with remediation suggestion 	OEM will certify and BOOs will check and confirm
2	Admin should be able to configure policies to detect for vulnerabilities and report it to under specific compliances.		BOOs will check and confirm
k. Miscellaneous			
1	The system should be capable to store the raw data or polled data, and also have the facility to automate the backup process or allow to take manual backup, in case required	On the proposed appliance	BOOs will check and confirm
2	Storage of known errors/issues that allows IT operations to document known issues in order to speed up the resolution process		OEM will certify and BOOs will check and confirm
3	Baseline & running Configuration and compliance management		BOOs will check and confirm
4	The system should be accessible via a Web based GUI console/portal from intranet as well as from internet. It should also be accessible through portable (Android/iOS and others) devices.		BOOs will check and confirm

S.No	Parameters	Specifications	Trial Directives
5	It should have a secured single sign-on and unified console for all functions of components offered for seamless cross-functional navigation	Manage device access and authorization through a centralized control model that is integrated with standard workflow and approval processes	BOOs will check and confirm
6	ACL (access control list) based access		BOOs will check and confirm
7	The proposed solution must support deployment on latest version of Windows or Linux Operating Systems		BOOs will check and confirm
8	The proposed solution should have the capability to support the deployment on either on-premises data centre platform or the cloud platform.		BOOs will check and confirm
9	Backup logs (storage duration)	12 months (storage as provided by buyer)	OEM will certify and BOOs will check and confirm
10	The Solution should provide mechanism to integrate with SIEM, SOAR, PAM, IT Ticketing systems, NACs etc.		OEM will certify and BOOs will check and confirm
11	Solution should support remote device management		BOOs will check and confirm
12	All modules must be integrated seamlessly		BOOs will check and confirm