SLOT 2

Request for Quotations

TENDER OPENING LINK FOR TENDERS CLOSING 08/03/2024
Friday, March 8 · 11:00am – 2:00pm
Time zone: UTC
Google Meet joining info
Video call link: https://meet.google.com/nqq-phpj-pgz

No	Tender	Description	Qty	Specs
1	RFQ 355-24	Supply and delivery of RUCKUS ZoneDirector ZD1200 controller for central management of RUCKUS access points	1	Specification attached
1	RFQ356-24	Provision of a Security Vulnerability Management Tool	1	Specification attached

Bidders with outstanding orders for any of the above items will not be considered for supply

TELONE RESERVES THE RIGHT TO INCREASE AND DECREASE QUANTITY

Please note that only bidders registered with **Procurement Regulatory Authority of Zimbabwe (PRAZ)** shall be considered.

(Please attach Proof of PRAZ registration in the specified category)

Closing date for ALL Tenders: On or before 1100hrs; Friday 08 March 2024

("Bids should be priced in US$ payable in ZW$ using the prevailing bank rate.")

Your Tender should state the price (Please state your **VAT** status), a firm delivery date Emailed to **procurement@telone.co.zw**

- **Bidders should also be compliant with the new regulations for FISCAL TAX INVOICE where necessary.**
- **Each tender should be in its own envelop, tenders should not be mixed on one quotation.**

Specifications RFQ 355-24

Technical Specifications

1	MODEL
1.0	**RUCKUS ZoneDirector ZD1200 controller**
2	GENERAL SPECIFICATIONS
2.1	**Managed wireless devices - Up to 4,000**
2.2	**Supported VLANs - Up to 256**
2.3	**Scalable, centralized management platform**
2.4	**Pay-as-you-grow licensing model**
2.5	**Simple and intuitive web-based interface**
2.6	**Advanced security features, including WPA3 and Layer 2/3/4 access control**
2.7	**Easy discovery from PC using UPnP**
2.8	**Two 1000 Mbps ports for full redundancy**
2.8	**Lifetime warranty coverage**
2.10	**Central control and configuration - Up to 150 Ruckus APs**
2.11	**Supported WLANs - Up to 256**
2.12	**Integrated DHCP server**
2.13	**Easy-to-use setup wizard**
2.14	**Ultra-intuitive GUI**
2.15	**1+1 redundancy with auto synchronization**
2.16	**Application recognition and controls**
2.17	**VLAN pooling**
2.18	**Smart Mesh Networking control and monitoring**
2.19	**Real-time client admission control**
2.20	**Load balancing**
2.21	**Customizable dashboard**
2.22	**Dynamic RF channel and power management**
2.23	**Quality of service with WLAN prioritization, band steering and airtime fairness**
2.24	**Integrated captive portal**
2.25	**Native ActiveDirectory/RADIUS/LDAP support**
2.26	**Local authentication database**
2.27	**Dynamic VLAN assignment**
2.28	**Guest networking**
2.29	**Dynamic generation of unique Pre-Shared Keys**
2.30	**Rogue AP detection and graphical map view**
2.31	**Hotspot authentication using WISPr**
2.32	**WISPr Smart Client Support**
2.33	**Performance monitoring and statistics**
2.34	**Limited lifetime warranty**

Specifications RFQ 356-24

Vulnerability Management System Technical Specifications

	DESCRIPTION	POSSIBLE SCORE	COMMENTS
1	GENERAL SPECIFICATIONS	15	
1.1	**Support Unlimited IPs**	**3**	
1.2	**On-premise Virtual Machine Deployment**	**3**	
1.3	**Product licensing and support for 1 year.**	**3**	
1.4	**Solution must be a leader or a challenger on the Gartner Magic Quadrant Report for Vulnerability management systems.**	**3**	
1.5	**Training and certifications for 4 administrators.**	**3**	
2	TECHNICAL SPECIFICATIONS		
2.1	Integration	**10**	
2.1.1	**The solution must be able to integration with multiple external identity repositories such as:** • **Microsoft Active Directory Lightweight Directory Access Protocol (LDAP)** • **Open Database Connectivity (ODBC) and SAML providers.**	**5**	
2.1.2	**The solution must support integration with thirdparty applications such as SIEMs, firewalls, patch management systems and endpoint security solutions.**	**5**	
2.2	Scanning Capabilities and Vulnerability Assessment	**40**	
2.2.1	**The solution should have the capability to scan, test and assess container images for vulnerabilities, malware, and adherence to policy compliance.**	**5**	
2.2.2	**The solution must integrate scan results into many third-party IT and security solutions**	**5**	
2.2.3	**The solution must be able to scan both internal and external web applications.**	**5**	
2.2.4	**The solution should be portable and flexible ability to scan systems anywhere and everywhere**	**5**	
2.2.5	**The solution should be able to quickly identify web application cyber hygiene Issues relating to**	**5**	
	SSL/TLS certificates and HTTP header misconfigurations.		
2.2.6	**The solution must Identify vulnerabilities in both your custom application code and the web components supporting it.**	**5**	
2.2.7	**The solution must safely scan environments without disruptions or delays.**	**5**	

2.2.8	**The solution must support fully qualified domain names (FQDN)**	**5**	
2.3	Asset Discovery	**15**	
2.3.1	**The solution should have the ability to automatically discover and categorize both known and unknown assets, including internal and internet-exposed assets.**	**5**	
2.3.2	**The solution should continuously identify unmanaged assets.**	**5**	
2.3.3	**The solution should not depend on IP addresses as the primary method for asset tracking.**	**5**	
2.4	Reporting And Dashboards	**20**	
2.4.1	**The solution must provide the ability to automate reporting by allowing scheduled reports.**	**5**	
2.4.2	**The solution must create reports based on customized views (e.g., specific vulnerability types, vulnerabilities by host/plugin, by team/ client)**	**5**	
2.4.3	**Reports should be available in PDF, CSV and HTML formats.**	**5**	
2.4.4	**Should allow customisable reports to suit different audiences.(Executive, Security)**	**5**	
	TOTAL SCORE	100	