Outcome of Pre Bid Meeting for RFP of Wi-Fi Access

Selection of Supply, Installation, Commissioning and 3 years maintenance of Wi-Fi ACCESS in the building of Gujarat Mineral Development Corporation Limited Ahmedabad

e-TENDER NO. GMDC/RFP/IT/ Wi-Fi/15-16

Query No. 1.	Request to add the two more OEM "Check Point" and "Alcatel-Lucent"
Reply	We accepted the request and now clause number 12.2 shall be read as "**Product shall be any of OEMs Cisco, Juniper, Fortinet, Net gear, Sonic wall, HP, Check Point, Alcatel-Lucent**"
Query No. 2.	Suggested to add the clause that all equipments from same OEM for better integration and management.
Reply	We accepted the suggestion and added one more clause number 12.16 shall be read as **All equipments /devices / components must be provided by same OEM except passive devices / components and SMS gateway**
Query No. 3.	Are SMS gateway provide by bidder.
Reply	**Yes** it shall be provided by bidder.
Query No. 4.	Please provide broadly specification for active components.
Reply	Please find the specifications as Annexure "A". Please provide the duly filled form along with physical documents as Annexure "B".

Architecture

- The System should support seamless roaming within the campus for users with mobile devices such as laptops, smart phones and tablets.

- Wi-Fi network access should be available throughout the campus only inside the buildings as well as in Lobbies, Corridor locations to all the staff of the GMDC and guest based on well-defined access policy.

- It should be possible to configure and deploy access points (APs) remotely through a Wireless controller.

- System should support multiple VLANs to support users with different privileges.

- Bidder shall provide complete network diagram including detailed technical documentation and detailed Project Plan for all the locations mentioned.

- The Architecture of the system should support scalability to support future expansions such as increased user density.

- It should be possible to manage the Wi-Fi network from a central location Data Centre, though the wireless management system. The management system should support unified wired and wireless network management, and BYOD (Bring your own device) solution.

- Unified Management System shall includes

  - Facility to create two separates virtual LANs or any other techniques one for Guest and Second one for Employees.
  - Automatic Registration through one time password sent by SMS or through web browser for guest.
  - Time and Bandwidth Controls for guest.
  - Employee's devices access can be restricted by MAC Address and / or LDAP.
  - Guest can be connected in organization's WLAN with two factor authentications.
  - It should make common network functions manageable from a single console, such as security and integrity monitoring, handling exceptions, logging and reporting.
  - The console must also include elements that are unique to wireless management, such as connection reliability, spectrum management and monitoring, location and tracking functionality, and additional security concerns.

Security

- The system must correctly detect smart phones connecting to the corporate network and classify them as approved or unapproved (Registered / Non Registered).
- Controller should have rogue AP detection, classification, location and automatic containment.
- The system must be able to detect and automatically prevent smartphones and other Wi-Fi enabled devices tethering when connected to your corporate network.
- The system should detect and prevent outside client trying to connect to the organization's WLAN. (Except Employees or registered client)
- The entire Wi-Fi network should be fully secure and multiple authentication mechanisms should be implemented by the successful bidder.
- Every user should get access to only those services for which they are authorized.
- The successful bidder has to configure the system on Rule based Access Rights.
- Data communication between devices should take place in encrypted form to ensure end-to-end security of user information/ data along with implementation of Wireless Security Standards such as WPA and WPA2.
- The Bidder has to ensure compliance with all Regulatory and Legal guidelines issued by Department of Telecommunications from time to time. At no point GMDC or its agencies would be responsible for any non-compliance arising from non-adherence on the side of the successful bidder.

Specifications of Wireless Access Point

- Wi-Fi access must have wireless intrusion prevention (WIPS) in a single device both operating simultaneously.
- Access Point must support encryption/decryption.
- Access points must support to detect DoS (denial of services).
- Access Points proposed must include radios for 2.4 GHz and 5 GHz with 802.11ac wave1.
- Auto channel allocation to avoid interference between APs.
- Should support configuring the access point as network connected sensor to access any network location covered by the access point to get Spectrum analysis data.

- Must support 3X3 multiple-input multiple-output (MIMO) with THREE spatial streams.

Specifications of SMS Gateway

- The proposed wireless solution should seamlessly integrate with SMS Gateway solution over IP.
- Bidder shall be responsible for integrating SMS gateway (to be proposed) for automatically sending the required details/ information through SMS to the users as per the requirement e.g. during user registration, forgot password, password reset, Account Expiry, etc.

Specifications of Wireless Controller

- The solution should support minimum 500 AP & Sensor devices.
- Offers Control and Provisioning of Wireless Access Points compliant to ensure encryption between access points and controllers across remote WAN.
- Should support the ability to schedule AP power on/off for energy savings.
- Location context based policy management and administration.
- Built-in vendor agnostic performance monitoring and Wi-Fi Analytics without 3rd party licensed solutions.
- Must not require a separate controller for Wireless Intrusion Prevention Access Points.
- Preferably the system must provide forensic data categorized under major threat vectors.
- Preferably the system should locate wireless devices accurately on floor maps.
- The system must support to detect DoS (denial of services).
- The system must send notifications based on location and alarm type.
- The system must provide a report of device summary (for APs, and / or clients).
- Controller should have all traffic across the network to analyze information about applications usage, peak network usage times for all access points.
- Proposed controller should support N+N redundancy from day one. Must support state full failover for all the clients from primary to backup WLC to any client downtime and Client re-association is avoided.
- Must be able to set a maximum user bandwidth limit on a per SSID basis.

- Must allow adjacent APs to operate on different channels, in order to maximize available bandwidth and avoid interference.

Specifications of Firewall

- The appliance should support at least eight 10/100/1000 Gigabit ports.
- The appliance should support at least one dedicated management interfaces to configure/manage the firewall policies, perform image upgrades even in case of failure of the data interfaces. Data ports should not be used for management purpose.
- Firewall should support at least 750 concurrent users (Local and / or VPN).
- Proposed firewall should support N+N redundancy from day one. Must support state full failover of sessions in Active/Standby & Active/Active mode.
- Firewall should support multi VLANs.
- The appliance based security platform should be capable of providing firewall, IPS and VPN (IPSec and SSL) functionality simultaneously.
- Firewall should have full time Unified Threat Management (UTM) features such as AV, Anti Spam; DDoS; TCP / UDP/ SYN Flooding Application Control; Bandwidth Management etc.
- Firewall should support one time password through SMS and two factor authentications.

Annexure "B"

Technical Specifications

Sr. No.	Required Specifications	Yes / No	Remarks
Firewall			
1	The appliance should support at least eight 10/100/1000 Gigabit ports		
2	The appliance should support at least one dedicated management interfaces to configure/manage the firewall policies, perform image upgrades even in case of failure of the data interfaces. Data ports should not be used for management purpose		
3	Firewall should support at least 750 concurrent users (Local and / or VPN).		
4	Proposed firewall should support N+N redundancy from day one. Must support state full failover of sessions in Active/Standby & Active/Active mode.		
5	Firewall should support multi VLANs		
6	The appliance based security platform should be capable of providing firewall, IPS and VPN (IPSec and SSL) functionality simultaneously.		
7	Firewall should have full time Unified Threat Management (UTM) features such as AV, Anti Spam; DDoS; TCP / UDP/ SYN Flooding Application Control; Bandwidth Management etc.		
8	Firewall should support one time password through SMS and two factor authentications		
Wireless Controller			
1	The solution should support minimum 500 AP & Sensor devices		
2	Offers Control and Provisioning of Wireless Access Points compliant to ensure encryption between access points and controllers across remote WAN.		
3	Should support the ability to schedule AP power on/off for energy savings		
4	Location context based policy management and administration.		
5	Built-in vendor agnostic performance monitoring and Wi-Fi Analytics without 3rd party licensed solutions.		
6	Must not require a separate controller for Wireless Intrusion Prevention Access Points.		
7	Preferably the system must provide forensic data categorized under major threat vectors		
8	Preferably the system should locate wireless devices accurately on floor maps.		
9	The system must support to detect DoS (denial of services).		
10	The system must send notifications based on location and alarm type.		
11	The system must provide a report of device summary (for APs, and / or clients).		
12	Controller should have all traffic across the network to analyze information about applications usage, peak network usage times for all access points.		
13	Proposed controller should support N+N redundancy from day one. Must support state full failover for all the clients from primary to backup WLC to any client downtime and Client re-association is avoided.		
14	Must be able to set a maximum user bandwidth limit on a per SSID		

	basis.		
15	Must allow adjacent APs to operate on different channels, in order to maximize available bandwidth and avoid interference.		
Wireless Access Point			
1	Wi-Fi access must have wireless intrusion prevention (WIPS) in a single device both operating simultaneously.		
2	Access Point must support encryption/decryption.		
3	Access points must support to detect DoS (denial of services).		
4	Access Points proposed must include radios for 2.4 GHz and 5 GHz with 802.11ac wave1.		
5	Auto channel allocation to avoid interference between APs.		
6	Should support configuring the access point as network connected sensor to access any network location covered by the access point to get Spectrum analysis data.		
7	Must support 3X3 multiple-input multiple-output (MIMO) with THREE spatial streams		
Security			
1	The system must correctly detect smart phones connecting to the corporate network and classify them as approved or unapproved (Registered / Non Registered).		
2	Controller should have rogue AP detection, classification, location and automatic containment.		
3	The system must be able to detect and automatically prevent smartphones and other Wi-Fi enabled devices tethering when connected to your corporate network.		
4	The system should detect and prevent outside client trying to connect to the organization's WLAN. (Except Employees or registered client)		
5	The entire Wi-Fi network should be fully secure and multiple authentication mechanisms should be implemented by the successful bidder.		
6	Every user should get access to only those services for which they are authorized.		
7	The successful bidder has to configure the system on Rule based Access Rights.		
8	Data communication between devices should take place in encrypted form to ensure end-to-end security of user information/ data along with implementation of Wireless Security Standards such as WPA and WPA2.		
9	The Bidder has to ensure compliance with all Regulatory and Legal guidelines issued by Department of Telecommunications from time to time. At no point GMDC or its agencies would be responsible for any non-compliance arising from non-adherence on the side of the successful bidder.		
SMS Gateway			
1	The proposed wireless solution should seamlessly integrate with SMS Gateway solution over IP.		
2	Bidder shall be responsible for integrating SMS gateway (to be proposed) for automatically sending the required details/ information through SMS to the users as per the requirement e.g. during user registration, forgot password, password reset, Account Expiry, etc.		