CARC
هيئة تنظيم الطيران المدني
CIVIL AVIATION REGULATORY COMMISSION

REQUEST FOR PROPOSAL (RFP)

نظام شبكة لاسلكية لجميع مديريات الهيئة والملاحة
WIFI and NAC solution

9/2023

Wireless Controller (Qty 1) located in Amman HQ

#	Specifications
1	The vendor should be placed as leader in the Gartner Magic Quadrant reports for Wired and Wireless LAN.
2	The Controller shall be hardware-based, rack-mountable
3	The Controller should support up to 64 Access Points in a single Controller.
4	The equipment shall conform to the industry standard specifications issued by IEEE 802.11a/802.11b/802.11g, 802.11n, 802.11ac and 802.11ax.
5	The Access Points shall be tunneled to the controller, which all the traffic should pass by the controller for better visibility and traffic control.
6	The Controllers shall support high availability with Active-Passive failover with client synchronization between the two controllers, in case one Controller is down the HA controller will have the users table without disconnection for connected active users. **(Future Requirement)**
7	The controller shall support the applications control, fingerprinting and visibility. Which allow IT to see applications by user, including top web-based applications like Facebook, Youtube and Box. The following describes the required features: 1. Applications visibility and Control 2. URL awareness 3. Limit bandwidth for applications. 4. Limit bandwidth for users or group of users. 5. Limit access based on time, date and location.
8	The controller should have min. 4 ports 1G UTP and Fiber, and one RJ-45 console port
9	The controller shall support Bonjour, mDNS, UPnP and DLNA device discovery protocols.
10	The controller shall be able to detect any rouge AP, classify rouge from interfering APs, locate any rouge AP on the map, and contain it automatically when needed (manual containment option is not accepted)
11	The vendor shall propose advanced enterprise Intrusion Prevention System (IPS) integrated with the controller or an external IPS with redundancy.
12	Controller should support the following authentication methods: 1. MAC address and by standard 802.11 authentication mechanisms. 2. Captive Portal and guest management 3. Network Admission control(NAC)
13	The system must support internal routing, bridging and spanning tree capabilities across its ports within the centralized controller in order to enable ease of deployment and scalability
14	An internal DHCP server for ease of deployment and scalability must be available and must be able to redistribute dynamically learned information such as DNS, WINS, and local DNS suffix entries in the DHCP response
15	The system must support L2 and L3 seamless roaming capabilities across APs
16	Automatically recognize the type (eg. Apple iOS) and model (eg. iPhone, iPad) of the mobile device connecting to the network
17	RADIUS support, ability to utilize RADIUS attributes to assign users or devices to specific roles/VLANs

18	The controller shall be manageable using CLI, Telnet/SSH, HTTP based GUI and SNMPv2/v3 and console.
19	Controller shall support integrated and External AAA server and Database for user authentication
20	Must support WPA and WPA2 authentication, also preferred WPA3 and Enhanced Open to be supported now or only with Software upgrade later
21	Manages authentication, encryption, VPN connections, IPv4 and IPv6 Layer 3 service
22	**RF Management**
	Intelligently and dynamically load-balance devices without receiving a new association request from the device
	Load balance across bands and steering of dual-band capable clients from 2.4GHz to 5GHz
	Traffic shaping capabilities to offer airtime fairness across different type of clients
	Allow for automatic and manual RF adjustment
	RF filters on access points for cellular coexistence
	Dynamic Frequency Selection DFS
	IEEE Beam forming standard
	Automatic transmit power and channel management control with auto coverage hole correction via Adaptive Radio Management or ClearAir or any equivalent features of the controller and supported by Access point.
	Self-healing on the detection of RF interference or loss of RF coverage
23	**Security**
	Capability to ensure privacy protection by preventing firewall and spoofing attacks, and enforcing TCP handshake
	Support for Access Control Lists (ACLs)
	Access policies should provide for automatic capture of data and syslog of access rule triggers for audit and analysis.
	Rules for access rights based on any combination of time, location, user identity, device identity, and extended attributes from the authentication database.
	The firewall must be able to take action including allowing the traffic, denying the traffic, rejecting the traffic, routing the traffic, destination or source NAT the traffic, modify the QoS level of the traffic, and blacklist (remove from the network) the client for policy matches
	Blacklisting of wireless user devices after failed authentication attempts or rule violations
	Controller shall support L2 Client Isolation so User cannot access each other's devices. Isolation should have option to apply on AP or SSID's
24	**Shall support Intrusion Detection / Prevention,**
25	**Shall support Quality of Services:** Provide application, user, and policy based QoS.
26	**Support:**
	Official Support and Warranty from the mother company for Five years minimum

Wireless Access Point (Qty 45): HQ, QA, KH-aqaba

#	Specification
1	The vendor should be placed as leader in the last five Gartner Magic Quadrant reports for Wired and Wireless LAN.
2	Indoor Dual Radio and Dual Band Access Point
3	Should support 802.11ax with MU-MIMO
4	Should support 802.11ax with 2x2 MIMO with 2 spatial streams, 802.11 DFS (Dynamic frequency selection),
5	Auto-sensing 10/100/1000 on the network port for Access Point
6	Should support Controller-based mode which offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding
7	Minimum of 16 SSIDs and BSSIDs available on each radio per access point
8	Capable of multi-function services including data access, intrusion detection, intrusion prevention, location tracking, and RF monitoring with no physical "touch" with license upgrade.
9	Internal Omnidirectional Antenna capabilities
10	Integrated Bluetooth BLE 5 and 802.15.4 radio (for Zigbee support) to simplify deploying and managing IoT-based location services, asset tracking services, security solutions and IoT sensors
11	Real time packet capture on the APs , without disconnecting clients , Built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices
12	The AP supports direct DC power and Power over Ethernet
13	Support 802.3af standard Power-over-Ethernet (PoE) with full capacity operation at full power of the radios
14	Ceiling mounting kits to be provided with the AP's, (suspended ceiling rail, flat 24mm)
15	Official Support and Warranty from the mother company for five years minimum

Network Access Control (Qty 1)

#	Specification
1	**Virtual Appliance or Equivalent**
	Virtual appliances are supported on VMware vSphere Hypervisor (ESXi), CARC has VMware ESXi ver 7.0
	Single platform approach that combines AAA, NAC, BYOD and Guest Access by incorporating identity, health, physical/device information, and conditional elements into one set of policies.
	Must have ability to scale to up to (10,000) concurrent sessions per Virtual appliance.
	Solution must be Agnostic to existing wired, wireless and VPN network in place today.
	Platform provides role- and device-based network access control for employees, contractors and guests across any wired, wireless and VPN infrastructure.
	Platform must be deployable in an out-of-band model and support for clustering with N+1 redundancy model. **(Future Requirement)**
2	**Functionality**
	Web-based, interface that includes several productivity tools such as a configuration wizard and preconfigured policy templates.
	Support any type of networking equipment (wired, wireless, VPN) and a variety of authentication methods (802.1X, MAC auth, Web auth).
	Must incorporate a complete set of tools for reporting, analysis, and troubleshooting. Data from access transactions can be organized by customizable data elements and used to generate graphs, tables, and reports. Must correlate and organize user, authentication, and device information together.
	All external facing interfaces are programmable, which means APIs are available to extend the system to support different authentication protocols, identity stores, health evaluation engines and port and vulnerability scanning engines.
	NAC health checking should support agent and agentless methods and be available as a permanent or dissolvable health agent for Windows, Linux, and Macintosh endpoint platforms. In addition to authenticating the user, the solution must gather granular information about the endpoint device, perform advanced health checks on Windows platforms (services, processes, peer-to-peer apps, registry keys, USB device usage, Windows Hot fixes, patch management agents), and perform standard health checks on Linux and Mac platforms (Anti-virus, Anti-spyware, Firewall).
	The solution Must be an easy-to-deploy virtual appliance platform that utilizes identity-based policies to secure network access and includes an integrated set of capabilities bundled under one policy platform: • Full AAA server – RADIUS and TACACS+ • Device Profiling • Built-in guest management and device/user onboarding • Web based management interface with Dashboard • Reporting and analysis with custom data filters • Data repository for user, device, transaction information • Rich policies using identity, device, health, or conditional elements • Deployment and implementation tools.

	Should support multiple methods for device identification and profiling such as: • Integrated, network based, device profiler utilizing collection via SNMP, DHCP, HTTP, AD, ActiveSync
	Policy model should support incorporation of several contextual elements including identity, endpoint health, device, authentication method & types, and conditions such as location, time, day, etc.
	Support the following enforcement methods: • VLAN steering via RADIUS IETF attributes and VSAs • VLAN steering and port bouncing via SNMP • Access control lists – both statically defined filter-ID based enforcement, as well as dynamically downloaded ACLs. • Roles or any other vendor-specific RADIUS attribute supported by the network device.
	Profiling capabilities included in base licensing to offer full visibility of the devices present on the network.
3	**Reliability / Performance**
	Virtual Appliances have ability to be clustered in any combination via local and remote network connections providing unlimited scale, redundancy, and access load balancing.
	Failure of master node should not impact the ability for backup appliances to continue servicing authentication traffic.
	Must support several deployment modes including centralized, distributed, or mixed.
	Core product should have been available in the market for at least 4 years.
4	**BYOD**
	Self-service workflow built on an industry leading platform. Supports popular smart devices as well as traditional computing platforms.
	Unique portal pages based on devices type – iOS, Android.
	provides high level of visibility into what devices are on the network and associated with what users.
	Automated onboarding of devices to enable secure access via self-serve portal allowing for the configuration of 802.1x supplicants, device enrolment and provisioning.
5	**Guest Access**
	Solution must be capable of providing sponsored and self-provisioned Guest Access.
	Must be able to provide custom branding and right size skins to auto adjust to smaller screen size types (tablets, smart phones etc.).
	Ability to send automated SMS or email credentials to the Guest User.
	Ability to set Account Details including Time Frame, Bandwidth Contract etc. Once account timeframe expires the User Account becomes inactive automatically.
	Ability to perform caching of MAC address post guest authentication to avoid the need for guest to re-authenticate during the period of their visit (3G like user experience after first authentication via captive portal).
	Auto-login for self-registration workflow – no need for the guest to retrieve account credentials from email or SMS for initial login.
	Anonymous login support with per device policy still applied.
	Sponsored approval workflow for guest self-registration where open SSID registration can be protected by requiring internal staff to approve the creation of guest account.
	Prevent employees from accessing the guest network on the corporate laptop.
6	**Required Licenses for min. 500 end-points**
7	Min. Three years Official Support from the mother company (vendor)

شروط عامة وخاصة:

١- على المتعهد تقديم خطة عمل واقتراح أفضل الحلول لتشغيل النظام ورسم توضيحي يوضح آلية الربط للنظام.

٢- على المتعهد ابراز خبراته في هذا المجال وعرض المشاريع المشابه التي تم تنفيذها في المؤسسات والدوائر الحكومية

٣- العدد قابل للزيادة لذا يتوجب على المتعهد تقديم سعر افرادي لجميع بنود النظام ولجميع الخيارات والمقترحات والمعروضة.

٤- على المتعهد تقديم تفاصيل برمجيات إدارة النظام من حيث رخص البرنامج التي يدعمها النظام وأي تفاصيل أخرى.

٥- على المتعهد تقديم الكتالوجات لجميع بنود المشروع

٦- فترة الصيانة المجانية لا تقل عن ٣ سنوات

٧- يشمل المشروع التركيب والتشغيل علما بأن الكوابل الشبكية جاهزة ل ١٨ نقطة في المباني الرئيسية للهيئة. **لأي أعمال تمديدات إضافية يجب تسعير هذا البند بشكل مستقل.**

٨- أجهزة AP's موزعة على ثلاث مواقع: مطار عمان-ماركا، مطار الملكة علياء، مطار الملك حسين-العقبة

٩- يتم استلام النظام بعد الانتهاء من التركيب والتشغيل والتدريب وتجربة عمل النظام ككل.

١٠- فترة التوريد مهمة جدا في تقييم العروض / يفضل توريد فوري

١١- تدريب محلي في الموقع مفصل لنظام WIFI ونظام NAC لموظفي القسم