غرفة تجارة وصناعة الشارقة
Sharjah Chamber of Commerce & Industry

Request for Proposal

DESIGN, SUPPLY, INSTALL, TEST AND COMMISSION OF TURNKEY WIRELESS ENHANCEMENT PROJECT

TABLE OF CONTENTS

1 INTRODUCTION

The main purpose of this RFP (Request for Proposal) is to choose a leading system integrator to provide a turnkey solution for the supply, design, installation and commissioning of Sharjah Expo Center Wireless, Security, that will provide fast, high-performance, reliable, highly available, manageable and secure Wi-Fi systems.

The Sharjah Expo Center internet access is provided by service provider's ADSL, MPLS, and ISDN Internet line.

Although this document presents much of what Expo Centre Sharjah requires, but it should not limit the project or implementation plan and it's the final description of requirements.

Site survey is also required.

2 STATEMENT OF REQUIREMENT

This Request for proposal outlines the requirements of Expo Centre Sharjah to procure the services of qualified system integrator to provide the following:

1. Minimum Hardware/Software/Licenses requirements as shown in technical requirements.
2. Optimized performance setup & configuration
3. Latest available technologies & best practices.
4. High scalability & upgradability
5. Extended warranty and support for up to 5 years.

3 SOLUTION REQUIREMENTS

3.1 Functional Requirements

1. The system integrator shall provide the required Wi-Fi solution and utilize or replace the existing solution of the listed hardware/software and Licenses.
2. The system integrator shall deliver, install, configure, and test the required solution.
3. The system integrator shall be responsible for the Network's , Access Management & Firewalling solution setup and configure within the SCCI HQ building and Expo Centre Sharjah.
4. The system integrator shall be responsible for Wi-Fi solution setup and configuration for Expo Centre Sharjah
5. The system integrator shall be responsible to provide the proper setup and configuration for External communication links (Internet, WAN) for Expo Centre Sharjah.
6. The system integrator shall test complete failover and failback scenarios.
7. The system integrator shall provide adequate knowledge transfer training for SCCI/Expo Centre staff for the provided solutions and technologies.

4 TECHNICAL REQUIREMENTS

System integrator must provide solid and sound enterprise Wi-Fi network architecture based on the following criteria:

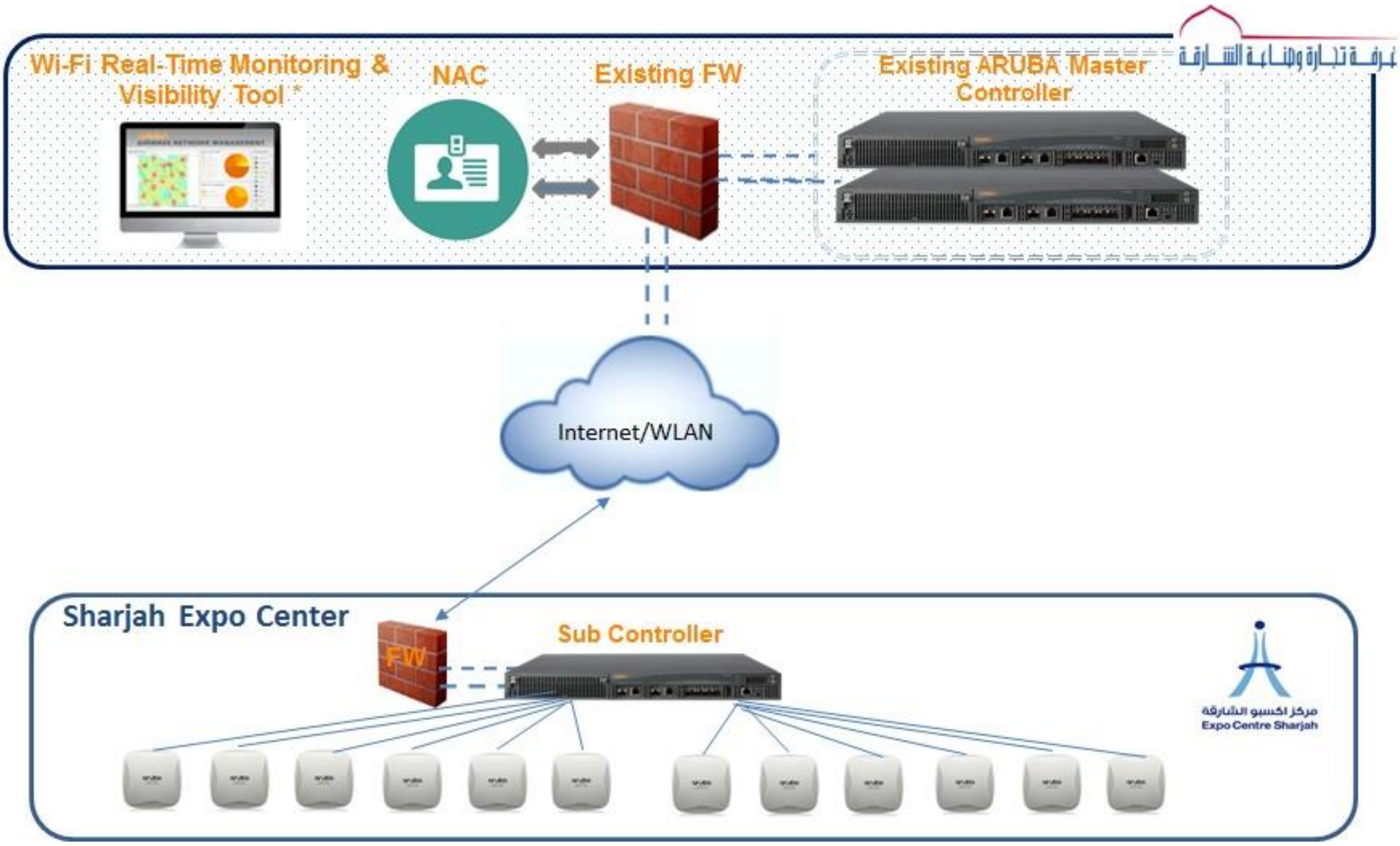
4.1 Network

Wireless solution based on AC technology that delivers high-performance which shall be built to meet needs of Wi-Fi service converged and comply with most efficient users security tools.

Access switches with PoE+ enabled for supporting networked devices such as IP phones, VoIP, video/IP cameras, CCTV, Digital Media Signage (DMS), wireless access points, and where it's required.

Ensure switch support for increasing large file access and transfers, Intranet access and other network intensive applications.

4.2 *General diagram*


Wi-Fi Real-Time Monitoring & Visibility Tool *
NAC
Existing FW
Existing ARUBA Master Controller
غـرفـة تجـارة وصنـاعـة الشـارقـة
Internet/WLAN
Sharjah Expo Center
FW
Sub Controller
مركز اكسبو الشارقة
Expo Centre Sharjah

4.3 Security

Network protection at the gateway level that block all malicious and blended threat attacks. Corporate network that prevents combination of malicious code, hacker, virus, Trojans and worm attacks by including the following Firewalling features for required firewall:

- Enforce security policies with granular control and visibility of users and devices for
- Thousands of discrete applications.
- Identify and stop threats with powerful intrusion prevention beyond port and protocol that examines the actual content of network traffic
- Perform high-performance SSL inspection using industry-mandated ciphers
- Proactively detect malicious unknown code using UTM & cloud-based sandbox service.
- Provide a real-time views into network activity with actionable application and risk dashboards and reports
- Deliver superior, multi-function performance by running on purpose-built appliances with ASICs.

4.4 Wireless Network Infrastructure revamp

The wireless network solution should be able to replace the existing wireless setup and also needs to support new wireless features and technologies.

Controller based centralized solution with AC type access points needs to be included to cater mobility services for the wireless end devices.

NG Firewall will provide all the security protection as mentioned in section 4.3.

5 SCOPE OF WORK

The following is the scope of work.

- The project is a Turnkey Project, should include design, supply, installation, configuration, testing, commissioning, integration, knowledge transfer, and maintaining the equipment's. If any additional item or accessory is required to complete the job and it is not included in the RFP, it will be considered under contractor responsibility and part of the deliverables.
- The proposal should include network (Layer 3) Access switches, security and firewall in the design, supply, installation, configuration, testing, commissioning and integration.
- The wireless LAN solution should be included to revamp the existing wireless infrastructure setup based on best practices.
- Any resulting impact on the existing systems, services, connections (LAN/WAN) is the responsibility of the Contractor.
- All international standards, norms and manufacturer recommendation have to be followed.
- Before commencing work, system integrator shall propose a complete and detailed project plan subject to review and approval of SCCI.
- The system integrator shall provide all labor, materials, tools and equipment required for work.
- All network equipment and appliance shall be a highly scalable and flexible modular architecture, hot swappable, centralized industry-standard manageability, high port/interface/module density, and high

routing/switching performance suitable for our current systems and future requirements.

- 99.99 percent reliable.
- Configuration must protect performance and productivity, avoid downtime and heighten network responsiveness.
- System integrator should provide proper labeling and documentation in English for all products installed both numeric and color coding.
- All items proposed are subjected to 5 years warranty on all parts and materials and on-site support as mentioned in section 5.2.1.
- The specified requirements are the minimum requirement and proposed specification may not be limited to that.
- Supplier shall respond paragraph by paragraph to all the following specifications and shall clearly indicate compliance or list exception to these specifications **(listed below).** The supplier shall include with the tender a complete material list of all equipment proposed and descriptive literature on each piece of equipment. Included in this proposal shall be rack-up drawings and block diagrams of the equipment supplied.
- The supplier should guarantee that the supplied design architecture is free from imperfections in design or construction that would create either operating difficulties or failure to meet specified performance quality.
- Suppliers must include in their proposals, a list of all client/company with whom the supplier has done business like that required by this tender. For each client/company, the supplier must include the name, title, address, and telephone number of a contact person along with a brief description of the project which was the basis for the business relationship. SCCI will determine which, if any, references to contact to assess the quality of work performed and personnel assigned to the project.

5.1 *Bid Scope*

The Bidder should provide a complete high level Design for the whole Network based on the provided requirements.

Bidding is limited to current project scope described below.

5.2 *Project Scope (Subject for Bidding)*

Project scope includes the design, implementation testing and migration services for the following Areas/Bids:

5.2.1 Bid (Wires & Wireless Network Infrastructure revamp)

1. NG Firewall
2. POE+ Access switches
3. Access points and controllers.
4. Centralized Network Access Management-NAC.
5. Centralized Network Real time Visibility Solution.
6. Connecting the New network to the WAN, Internet, PSTN routers

6 PROJECT SCHEDULE

Within 15 days of award of contract, a schedule must be submitted by the system integrator to SCCI IT System Support & Networking showing projected delivery and implementation plan of the Enterprise Network Upgrade. Provide all necessary information regarding the implementation.

A weekly and/or monthly update meeting (which ever SCCI decides) should be done to discuss the milestones/issues for the project until completion.

7 TECHNICAL SPECIFICATIONS

The following are the technical requirements for the WiFi solution enhancement. Existing wireless controller and access points and Firewall will be replaced or utilized according to our provision. Existing routers will remain and the proposed solution should be integrated seamlessly with it. In case these technical specifications may be incomplete, system integrator are welcome to give additional technical advice.

7.1 *Wireless Network Infrastructure*

Item Description	Qty
Wireless LAN solution for providing the SCCI-Expo Centre Sharjah with the ability to accommodate wireless network coverage at Expo Centre. The wireless LAN solution must be designed and deployed based on best industry practices. Each controller with 10G/1G interfaces. Maintenance and support for 5 years based on next day Hardware replacements by vendor or partner.	Solution
Access Points with internal antenna and mounting kit.	
All licenses should be included.	
Aps Mounting Scope should be included.	
Site visit will have to be carried out to check for the cabling requirements.	

7.1.1 General Features

- Solution must be a centralized WLAN architecture with “thin” AC type high density access points, centralized switch/controllers, and integrated network access management.
- Solution must be a self-contained, integrated, overlay, not requiring upgrades or enhancements to existing routers and switches.
- The same software, configurations and product functionality supported across all platforms in the product family proposed.

- Newly installed controllers should automatically synchronize in management layer with existing controller(s), without requiring a separate network management server.
- Solution must be Wi-Fi Certified for Data.
- Solution must be Wi-Fi Certified for Voice.
- All proposed devices are 802.11 standards-based.
- The solution must easily scale to accommodate future expansion requirements.
- Controller must be supported by NBD exchange option from product vendor.
- Controller must be support up to 256 Access Points.
- Controller must be able to support minimum 8,000 concurrent devices.
- NAC solution must be able to support up to 1000 Endpoints.
- Explain the upgrade procedure for new software.
- Life-Cycle announcements must be published.
- Solution must enable ease of troubleshooting via centralized management.

7.1.2 Authentication & Encryption

- Support for Universal Authentication.
- Must support MAC-based authentication.
- Must support 802.1X based authentication.
- Must support WPA2/AES link layer encryption.
- Must support WEP link layer encryption.
- Must support WPA/TKIP link layer encryption.
- Must support LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-GTC authentication.
- Support for Integrated RADIUS termination for increased security and cryptographic offload should be provided. Must support EAP-PEAP and EAP-TLS using EAP-MSCHAPv2 or EAP-GTC.

- Solution must offer full RADIUS support including interoperability with external servers.
- Web-Based Authentication (e.g. WebAuth/Captive Portal):
- Must support user name and password authentication, as well as support for token based authentication and social media account authentication.
- Facilitate process for non-IT staff to create temporary guest IDs and passwords to automatically expire/role provisioning.
- Must support airtime-based bandwidth contract for the guest SSID to preserve channel access for particular SSIDs.
- Must support packet-rate based bandwidth contracts for individual guest users for increased control of guest traffic usage.
- 802.1X based guest access using a local database must be supported on the switch/controller in order to authenticate users.
- Solution must provide support for walled garden functionality

7.1.3 Access Points (APs)

- APs must be plenum rated with applicable certifications.
- Auto-sensing 10/100/1000 on the network port for 802.11n/ac APs must be supported.
- Support 802.3af standard Power-over-Ethernet (PoE) and 802.3at.
- Ceiling and/or wall mounting options for APs must be supported.
- Access point must support out-of-the box, auto configuration across layer-2 and layer-3 networks without having to enter configuration information into the AP.
- APs must not hold “hard configured” internal network information or certificates for authentication to the centralized switches unless this information is stored in a trusted platform module (TPM) integrated into the AP.

- Minimum of 16 BSSIDs must be supported per radio.
- Devices must be capable of multi-function services including: data access, intrusion detection, intrusion prevention, location tracking, and RF monitoring with no physical “touch” and no additional cost.
- Real-time, fully integrated spectrum analyzer capabilities on the Aps , that does not require dedicated sensors or separate operating system running on the AP radios must be supported.
- APs shall support real-time packet capture without disconnecting clients.
- APs must have both internal and external antenna options.
- Must be Wi-Fi alliance 802.11n/ac compliant.
- The proposed solution must support 802.11ac.
- Vendors must have a solution engineered to support all future wireless networking standards without requiring modular additions or new hardware.
- APs must have secure mounting options for indoor and outdoor applications

7.1.4 AP-to-Controller Communication

- Use of industry standards-based (IEEE or IETF) tunneling protocols including IPsec and GRE.
- Centralized Encryption/De-encryption must be supported to prevent wired eavesdropping on wireless user data and malicious attacks on Aps.
- Vendors must optionally support distributed Encryption/De-encryption without the need for specialized hardware which support mixed mode operations from a single switch/controller.
- Must improve enterprise wide mobility by securing legacy devices with integrated client VPN and site-to-site VPN.

7.1.5 AP Management

- System must perform automatic updates of firmware and software on all APs without user intervention.
- Must support a discovery protocol from APs to find and sync with switch/controller that works over routed and switched subnets and that does not require reconfiguration or features on routers or switches.
- All AP configuration and service delivery information must be centrally managed and maintained via the switch/controller/Network Access Management-NAC.
- Updates must be performed via a centralized switch/controller which provides an easy to use (template based) mechanism to support configuration of different groups of APs and does so without requiring a separate management interface.

7.1.6 RF Management

- Access points must have at least two radios operational via 802.3af (standard PoE).
- Access points must support dedicated dual-radio hardware and must not be a modular addition to an 11n device.
- The AP CPU must be purpose-built and cannot be older than 1 year prior to the release date of the AP device itself.
- The proposed solution must comply with 802.11ac standard-based transmit beam forming.
- Access points must be capable of serving .11n and .11ac clients on the same 5 Ghz radio and should not require separate radios to support both .11n and .11ac clients.
- RF management solution must be able to monitor roaming clients between access points for each mobile device and visually roaming patterns for every device on the network.
- Solution must have the ability to intelligently and dynamically load-balance devices without receiving a new association request from the device.

- The RF management solution must monitor client health metrics on the WLAN controller/management system on a per client basis.

- The solution must visually highlight mobile device health metrics and provide reports based on desired metrics to monitor network performance.

- Enable ease of deployment and ongoing management with automatic adjustment of individual AP power and channel setting to maximize performance around other APs, limit the effects of interference (both 802.11 and non-802.11), and detect and correct any RF coverage holes.

- Access points must have at least two radios operational via 802.3af (standard PoE).

- Access points must support dedicated dual-radio hardware and must not be a modular addition to an 11n/ac device.

- The AP CPU must be purpose-built and cannot be older than 1 year prior to the release date of the AP device itself.

- The proposed solution must comply with 802.11ac standard-based transmit beam forming.

- Access points must be capable of serving.11n and .11ac clients on the same 2.4 & 5 Ghz radio and should not require separate radios to support both .11n and .11ac clients.

- RF management solution must be able to monitor roaming clients between access points for each mobile device and visually roaming patterns for every device on the network.

- Solution must have the ability to intelligently and dynamically load-balance devices without receiving a new association request from the device.

- The RF management solution must monitor client health metrics on the WLAN controller/management system on a per client basis.

- The solution must visually highlight mobile device health metrics and provide reports based on desired metrics to monitor network performance.

- Solution must enable ease of deployment and ongoing management with automatic adjustment of individual AP power and channel setting to maximize performance around other APs, limit the effects of interference (both 802.11 and non-802.11), and detect and correct any RF coverage holes.

- Devices should support DFS certified radios that can enable 14 additional 5GHz channels thereby increasing total WLAN capacity.

- RF management solution should prevent data loss with adaptive RF management that provides the capability to pause channel scanning / adjust RF scanning intervals based on application and load presence.

- Solution must offer dynamic load balancing to automatically distribute clients to the least loaded 802.11 channel and AP. Load balancing must not require any client specific configurations or software.

- APs that are used for WLAN access should continue to perform RF scanning for the purposes of dynamic RF management and wireless intrusion detection and prevention. This scanning should not adversely affect data transmission for mission-critical applications.

- Solution must support load balancing across bands and steering of dual-band capable clients from 2.4GHz to 5GHz in order to improve network performance without the use of client specific configurations or software.

- Traffic shaping capabilities must be supported to offer air-time fairness across different type of clients running different operating systems in order to prevent starvation of client throughput in particular in a dense wireless user population without the use of client specific configurations or software.

- RF management solution must have the capability to provide preferred access for “fast” clients over “slow” clients (11n/ac vs. 11a/b/g, and 11g vs. 11b) in order to improve overall network performance.

- Co-channel interference must be managed in order to prevent adverse effects of operating multiple APs in the same channel while in close proximity.

- Ability to mitigate adjacent channel interference among the APs operating on “neighboring” channels.

- System should support the above functions in real time and without the need to perform any network baselines or manually administered measurements and must be based on real RF information versus models in management systems.

- RF management solution must optimize user and bandwidth capacity.

- SLA/SLGs must be support through RF management solution features.
- Solution must support 40 MHz Channels and Channel Bonding.
- Solution must support 20 MHz Short Guard Interval.

7.2 Access switches

Item Description	Qty
Access Switches solution for providing the ability to accommodate all links to Access units.	8 switches 24G PoE+ 4SFP+

7.2.1 Key Features

- Basic Layer 3 switch series with VSF stacking, Static, Rip and Access OSPF Routing, ACLs, and robust QoS
- Consistent wired/wireless experience with NAC Policy Manager.
- Convenient built-in 1GbE or 10GbE uplinks and up to 370 W PoE+.
- Ready for innovative SDN applications with Open Flow support.
- Simple deployment with Zero Touch Provisioning and cloud-based Central support.

7.3 Edge Firewall

Item Description	Qty
Edge firewall solution for providing the SCCI-Expo Centre Sharjah with the ability to accommodate security filtering and control between the different network segments. The edge firewall solution will be designed and deployed to a fully redundant solution with next generation firewall and IPS features. Edge firewall with 2 X 10 GE and Minimum 8 X 1G interfaces. Maintenance and support for 5 years based on next day replacements by vendor or partner with UTM subscription.	Solution
8 x GE RJ45 Ports 2 x 10 GE SFP+ Slots	
Licenses should be included.	
Cables and accessories should be included.	

7.3.1 General Requirements:

- The Firewall must be Hardware based and should facilitate multi-application environment.
- The platform must use a security-hardened, purpose-built operating system.
- The platform should use hardware acceleration (ie ASIC) to optimize the packet, encryption/decryption and application level content processing.
- Appliance should be rack mountable. Should have provision for redundant power supply.
- Licensing: should be per device license for unlimited users for Firewall / VPN (IPSec & SSL) and other features. There should not have any user/IP/host based licenses - Please specify if the product does not follow the required licensing policy.
- Support for Virtualization.
- Should have support for Explicit Proxy (especially for the purpose of having session based policies for Citrix/Terminal Server users).

- Should support the following UTM security features: Antivirus, IPS, AntiSpam, Web Filtering, DLP, Application Control plus Wan Optimization and Web Cashing.
- UTM Technology should be BYOD compliant.

7.3.2 Interface and Connectivity Requirements:

- The platform must support GbE switched internal ports with dedicated WAN and DMZ ports.
- The platform must be capable of supporting a minimum of 2 x 10GbE, 8 x 10/100/1000 Interfaces .
- The platform should support the standards based Multi-Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.
- The platform should support VLAN tagging.
- (IEEE 802.1q) with about 4096 VLANs supported (in NAT/Route mode).

7.3.3 Performance Requirements:

- The Firewall must support at least 5 Million concurrent connections.
- The Firewall must support at least 270,000 (TCP) new sessions per second processing.
- The Firewall must support at least 10,000 policies (rules).
- The Firewall should support IPv4 & IPv6 Firewall throughputs of minimum 32 Gbps.
- The Firewall should support 3.2 Gbps NGFW Throughput.
- The Firewall should support 2.2 Gbps SSL-VPN Throughput.
- The Firewall should support 20 Gbps IPsec VPN Throughput .
- The Firewall should support at least 2 Gbps of SSL VPN Throughput.

- The Firewall should support a minimum of 1.7/3.1 Gbps of Antivirus Throughput (proxy-based/flow-based) .
- The Firewall should support at least 6 Gbps of IPS Throughput.

7.3.4 Network/Routing Requirements:

- Static routing must be supported.
- Multiple WAN links must be supported.
- Policy based Routing must be supported.
- Dynamic Routing (RIP, OSPF,BGP & IS-IS) must be supported for IPv4 .
- Should support RIPng, OSPFv3 and BGP4+
- Multicast routing must be supported.
- DHCP client/server must be supported.

7.3.5 Firewall Features Requirement:

- It should be possible to operate the firewall in “bridge mode” or "transparent mode” apart from the standard NAT mode.
- The Firewall must provide NAT functionality, including PAT.
- Should support “Policy-based NAT”.
- The Firewall should provide advanced NAT capabilities, supporting NAT Traversal for services like SIP/H.323 /SCCP.
- Firewall should support Voice based protocols like H.323, SIP, SCCP, MGCP etc and RTP Pinholing.
- The Firewall should support User-Group based Authentication (Identity based Firewalling) & Scheduling.
- The Firewall should support Device-Based firewalling (based on OS).
- Vulnerability management should be supported.
- IPv6 support for both NAT and Bridge / Transparent Mode.

7.3.6 Authentication Requirements:

- Support for authentication at the firewall policy level (Local and Remote).
- Support for external authentication servers integration for User and Administrator Authentication.
- RADIUS,
- LDAP
- TACACS+
- Support for Native Windows Active Directory or Novell eDirectory Integration.
- Support for clientless Active Directory Integration.
- Support authentication based on LDAP Groups.
- Support Two-Factor Authentication Using Tokens for both users and Administrators.
- Support PKI / Digital Certificate based two-factor Authentication for both Users and Firewall Administrators.

7.3.7 Administration/ Management Requirements:

- The device must support Web UI (HTTP/HTTPS) and CLI (Telnet / SSH) based Management.
- Should have configurable option to define remote access to the Firewall on any interface and restrict the same to a specific IP/Subnet (ie Trusted Hosts for Management).
- There must be a means of connecting directly to the firewall through a console connection (RJ45 or DB9).
- The device should have SNMPv2c and SNMPv3 support (for sending alerts to NMS in case of threats and system failures).
- Provision to generate automatic notification of events via mails / syslog.
- Provision to send alerts to multiple email recipients.

- Support for role based administration of firewall.
- Should have provision to customize the dashboard (eg: by selecting suitable Widgets).
- The Firewall must provide a means for exporting the firewall rules set and configuration to a text file via Web or TFTP.
- Support for Image upgrade via FTP, TFTP and WebUI.
- Support system software rollback to the previous version after upgrade.

7.3.8 Network IPS:

- Should have integrated Network Intrusion Prevention System (NIPS) and should be ICSA Labs certified.
- Should have a built-in Signature and Anomaly based IPS engine on the same unit.
- Able to prevent denial of service attacks.
- Should be able to exclude certain hosts from scanning of particular signatures.
- Supports CVE-cross referencing of threats where applicable.
- Provide the facility to configure Profile based sensors (Client/Server) for ease of deployment.
- Supports granular tuning with option to configure Overrides for individual signatures.
- Supports automatic Attack database updates directly over the internet. (ie no dependency on any intermediate device).
- Supports attack recognition inside IPv6 encapsulated packets.
- Supports user-defined signatures (ie Custom Signatures) with Regular Expressions.
- Supports several prevention techniques including Drop-Packet, TCP-Reset (Client, Server & both) etc. List all prevention options.

- Offer a variety of built-in responses including dashboard alerts, syslog / email notifications, SNMP traps and Packet Capture log. List all response options, excluding prevention responses.
- Support to Identify and control wide range of applications, mention the number of applications recognized and can be controlled.
- Support QoS policies based on applications.

7.3.9 Gateway Antivirus

- The appliance should facilitate embedded Antivirus support which is ICSA Labs certified.
- Should include Antispyware and Worm Prevention.
- Should have option to schedule automatic updates of the new virus pattern.
- Gateway AV should be supported for real-time detection of viruses and malicious code for HTTP,HTTPS, FTP, SMTP, SMTPS, POP3 and IMAP, NNTP and IM.
- Should have configurable policy options to select what traffic to scan for viruses.
- Solution should offer multiple options to take action in case of virus detection.
- Should have support for “Flow-Based Antivirus Scanning Mode” for high throughput requirements.
- The solution should be capable scanning Encrypted VPN tunnel traffic originating from the unit for virus.
- Should have an ability of Antivirus scanning for IPv6 traffic.

7.3.10 Web Content Filtering

- The appliance should facilitate embedded Web Content Filtering feature.
- Web content filtering solution should work independently without the need to integrate with External proxy server.
- Should have facility to block URL' based on categories. Should support HTTP and HTTPS based traffic.
- Solution should be able to create different access level based on user identity by integrating with LDAP, Radius or Local System users.
- Should have configurable parameters to block/allow unrated sites. Should have option to locally rate sites.
- Solution should support fail-open and fail-close features.
- Solution Messages (Block, Error and Warning messages) should be customizable to show any message that meets with internal policies.
- Should have configurable policy options to define the URL exempt list.

7.3.11 Logging/Monitoring

- The platform should support local event logging.
- Logging to remote Syslog/WELF should be supported.
- Graphical Real-Time, Historical Monitoring and One-Click Monitoring should be supported.
- SNMP should be Supported.
- Email Notification of Viruses and Attacks should be supported.
- VPN tunnel monitoring should be supported.

8 Network Access Control

NAC solution must be a scalable, easy-to-use visitor management Solution that delivers secure automated guest access workflows for visitors, Exhibitors , partners, shoppers and fans on wireless and wired networks using any type of mobile device. Self-registration and sponsor involved options ensure credentials and pre-authorized access privileges are enforced for short-term and long-term guests, without putting a heavy burden on IT, receptionists and staff.

Once registered, credentials can be delivered via SMS text, email, users accounts can be set to expire automatically after a specified number of hours or days. Solution have capability to provide security and automation to support hundreds or thousands of guests, while also reducing the threats that come with unauthorized guest access and possible risks.

8.1 *Main Solution Requirements*

- Self-registration – customizable guest portal provides easy-to-use login Process that also deters unwanted users from requesting access.

- Customizable branding – logos, visual imagery and optional advertisements Provide an opportunity to extend SCCI and Exhibition messaging, and promote mobile Apps and offers.

- Automated credential delivery – registration process can deliver SMS text, email or Printed credentials depending on security requirements.

- Mobile device awareness – captive portal is automatically sized for smart phones, Tablets and laptops.

- Secure guest access –login and traffic encryption option for public Networks.

- Social logins – enables retailers and public venues to gather Valuable demographics about guests that opt-in to guest Wi-Fi using Facebook, Twitter credentials.

9 Network Real time Visibility Solution

Solutions must provide visibility and controls to optimize how devices and apps perform on the network. Through a centralized and intuitive user interface, And Provides real-time monitoring, proactive alerts, historical reporting, and fast, efficient troubleshooting. Dedicated dashboard views quickly help to view potential RF coverage issues, unified communications and collaboration (UCC) Traffic, application performance and network services health.

10 PASSIVE COMPONENTS

CONTRACTOR/system integrator shall include in their proposal passive components as needed to support the Enterprise Network Upgrade Designed Solution and all service provider connectivity.

Passive components include Fiber patch cords, cable managers, etc. and miscellaneous materials like PVC conduit, and trunking etc.

11 SCALABILITY

The proposed network system must maintain its quality performance or service under an increased system load by adding resources (usually hardware, modules, etc).

For the active components (management appliance, switch, router, IPS/IDP, firewall) it must function well as it scales up or down. The system/components must provide a provision to scale up 10 to 20 percent for port/interface density.

12 INSTALLATION AND CONFIGURATION

All settings and procedure must be properly documented and result must be delivered to SCCI IT department in both soft and hard copy.

Physical installation of proposed network and security, including interconnection/system integration and pre –handover testing.

13 SYSTEM ACCEPTANCE TEST

After completion of installation and commissioning, a **Final System Acceptance Test** will be conducted. The system integrator will provide a network (active and passive) and security system acceptance test procedure document and be evaluated by the IT department for additional test requirement. The acceptance test shall cover but not limited to the compliance to the requirements expressed in the tender specification. The overall system acceptance test will be the internal network and the external network (Internet, Remote Access and VPN client/clientless). For partial compliance, system integrator must comply at a later date that is acceptable to SCCI.

14 TRAINING

There should be a transfer of technical skills in form of actual and classroom training environment: System integrator must provide an official manufacturer technical training for 4 people for all installed network and security solution.

15 TECHNICAL SUPPORT

System integrator must explicitly undertake, or provide maintenance (corrective and preventive), spare parts and support for the hardware and software acquired under this Information to tender for a **Warranty Period of 5 years** from the relevant date of successful installation commissioning, acceptance and certificate delivery .

15.1 Warranty period

System integrator must have a 24x7 On-Site warranty service, these will include but not limited to:

- Phone-In problem diagnosis
    - Detailed response for more complex inquiries (telephone/hardcopy).
    - Remote software diagnosis service.
    - Corrective action for rectifying software bugs and performance.
    - Escalation procedures for problems, which cannot be solved in an early manner.
- Service Technical Engineer Dispatch.
- 24x7 On-site service.
- Up-and-run support (initial installation and setup of the system).
- Reconfiguration of active components as the needs arises.
- Operating System Support (whatever system is loaded on the machine).
- Software Support (software loaded at time of purchase).
- Software Upgrade.

15.2 Warranty terms and duration

System integrator shall describe the terms and duration of whatever warranty is offered (per equipment/item) on the proposed network equipment.

15.3 Support response time

System integrator must commit to a response time of 3 hours (from the time the fault had been reported by SCCI either by phone/email or whatever means SCCI chooses) during the period of support cover. In cases where remedial action (i.e. engineer on site) is required, system integrator must commence such remedial action within 4 hours (from the time the fault had been reported by SCCI either by phone/email or whatever means SCCI chooses) .

15.4 List of support

System integrator shall describe what type of help and support can be made available to SCCI-Expo Centre Sharjah during the warranty and operation period. In particular, system integrator must list the following support.

15.5 Defected materials responsibility

System integrator shall be responsible for any defects that may develop under normal usage arising from faulty materials, design or workmanship in the items supplied. The system integrator shall rectify such defects at his own cost when called upon to do so by SCCI.

16 PROJECT MANAGEMENT REQUIREMENTS

All system integrator teams are required to familiarize themselves with the policies and processes for project management in SCCI. This is possible by making contact with the SCCI PMO where the appropriate material will be made available.

16.1 Project Plans

1. For the purposes of responding to this RFP the supplier must provide a high level project plan. The plan must be comprehensive enough in scope and detail to convey the system integrator ability to manage this project as specified in this RFP.
2. The system integrator shall submit a master schedule, based on a work breakdown structure for defining and controlling the project.
3. The system integrator must stress work quality and how quality is ensured in all aspects of the project.
4. The system integrator must indicate in his plan how the status and visibility of project progress will be monitored.
5. As part of the overall project the system integrator shall perform at least the following:
   a. Maintain a summarized program schedule of key high-level activities in a suitable graphical form.
   b. Update the master schedule to reflect activity completion and schedule changes.
   c. Maintain detailed schedules for major activities such as site preparation, hardware installation, testing and training.
   d. Project will be monitored and reported within the established Microsoft (Enterprise Project Management) EPM system at SCCI.

e. Risks should be monitored, and mitigation plans should be devised to ensure the project is not affected.

16.2 Project Organization plan

1. The system integrator shall provide an organization plan that includes the organization for the management and execution of the project.
2. The system integrator shall define the interfaces between SCCI and the organization, highlighting the escalation path.
3. SCCI requires a Project Manager be assigned to oversee the operation of the entire project.
4. The Project Manager must be available on-site at the SCCI-Expo Centre Sharjah or at the appropriate government agency in Sharjah.

17. DOCUMENTATION

System integrator must provide the following documentation and manuals in Hard, soft copy or email (PDF and word format) form.

- Design documents.
- Configuration documents.
- Operation documents.

System integrator shall state whether on-line access to such materials is available via the equipment manufacturer's website.

After completion of the implementation, the system integrator must submit a detailed documentation that will cover, in minimum, the following:

- As-built drawing/diagram of SCCI-Expo Sharjah Centre network upgrade system.
- Implementation and configuration details per module and/or system.
- Step by Step implementation procedures.
- Wire distribution of equipment and connectivity.
- Test result for equipment connectivity and POST.
- Network and security test result.

- First level troubleshooting procedures.
- Serial and part number of modules and equipment.
- Warranty certificate from OEM – specifying that all items supplied are new and free from all defects.

18. CONFIDENTIALITY

All information supplied by SCCI and contained in this RFP must be treated as strictly confidential by the Bidder. Bidders must not communicate any information contained in the RFP to any other party or make use of such information for any purpose other than for the preparation of a Tender proposal.

Vendor SLA must be added

Bidders shall not, without the prior written consent of SCCI, make any reference to SCCI in any advertising, promotional or published material.

19 GENERAL CONDITIONS ON ALL SYSTEMS

Quotation:

Must include full specifications and brochures of all items, and must include clear delivery period. Prices should reflect Competitive Prices and/or Special discounts on all items.

In case some items become obsolete or end of sale during the tendering process, the bidder must propose the latest and newest models for SCCI.

Quality:

All equipment, their peripherals and items must be known brand name, make and quality. The original manufacturer must certify internal components if made in other brands.

Readiness:

All equipment must be complete with all needed software, hardware, cables and connectors to form a complete working unit within the system. Additional items should be clearly specified in the offer otherwise it's the supplier's own responsibility to provide any additions. A site visit will be arranged if required. It's the suppliers responsibility to inspect and assess readiness and compatibility of supplied equipment with existing systems and infrastructure.

Delivery & Installation:

All systems should be supplied, installed and made functional within the given delivery period. Final delivery and acceptance will be certified by SCCI only after the complete delivery is concluded in compliance with the above terms.

Commissioning the awarded items includes, delivery to SCCI store, unpacking and installing in the designated location, connecting it to the network and make ready for the user to start its utilization.

In terms of equipment supply, a detailed time and workforce plan should be provided when/if requested (template below) for the project execution and one engineer will be requested to monitor & support for at least one week after the complete delivery to observe and solve any arising problems related to the new equipment.

A project manager (PM) should be assigned and named to SCCI to coordinate and to ensure proper implementation of the project and he should be given adequate authority and responsibility to do this.

Reservations:

SCCI reserves the right to accept other proposals not necessarily in line with the above proposal for embracing newer technology and keeping the interest of SCCI at the foremost.

Contact Information:

For any further Questions or site visit, please contact SCCI PURCHASE DEPT.