مـدينـة مـصـر

Madinet Masr

تأسســـــت ١٩٥٩

Madinet Masr New Building –
IT Infrastructure RFP

Document Content

INTRODUCTION

About the Project "HQ Active Network"

- The "HQ Active Network" project is a key initiative by MMHD aimed at deploying a comprehensive IT infrastructure for our new HQ.

  This project seeks to establish a robust, scalable, and secure network system to support our operational needs and enhance our organizational efficiency. The new network infrastructure will include advanced networking equipment, cabling, and associated systems designed to facilitate high-performance connectivity and support future technological advancements.

Purpose of Issuing this RFP

- This RFP is issued to solicit Proposals from qualified vendors for the provision and implementation of IT network systems required for the "HQ Active Network" project.

  The RFP details the scope of work, evaluation criteria, technical requirements, and submission requirements for interested vendors.

Project Scope:

1- Providing the IT infrastructure for the new building for Madinet Masr.
2- Project includes the following domains
A-Wired / Wireless network infrastructure B-
Collaboration
C- Security Solutions
3- All Licenses included in all domains must be for 3 years.

Scope Of Work:

1-Passive infrastructure:

Structured Cabling Installation

- Supply and install fiber optic Patches, Pigtails, patch cords cable and cable organizers as per the approved BOM, all material must be from the same vendor of network cabling
- Supply, installation, testing, commissioning, training and handing over of rack mounted Power distribution panels.
- Supply, installation, testing, commissioning, training and handing over of Power distribution units (PDUs) dedicated for in-rack power supply.
- Supply, installation, testing, commissioning, training and handing over of rack mounted uninterrupted power supply (UPS).
- Supply, installation, testing, commissioning, training and handing over cable organizers and cable management systems for power, data and fiber cables.

Termination and Installation of Passive Components

- Install and terminate all Fiber Cores at patch panels
- Install patch enclosures in designated data rooms and closets.

Labeling and Documentation

- Label all cables, patch panels, and outlets as per the agreed-upon labeling scheme.
- Prepare comprehensive documentation for the cabling system, including types, and terminations.

Testing and Certification

- Perform OTDR (Optical Time-Domain Reflectometer) testing for fiber optics.
- Provide certification reports for all installed cables and components.

Project Timeline

- Vendor should Provide a detailed timeline outlining key milestones such as site survey completion, design approval, installation phases, testing, and final handover.

Standards and Compliance

- Ensure all work complies with local building codes, health and safety regulations, and industry standards such as TIA/EIA, ISO/IEC, and BICSI.

2-Active Network

Project Overview

- Design, supply, install, test, train, and hand over a fully operational active network for the new HQ building that supports data, voice, video, and other IT services with high availability, scalability, and security.

1. Objectives

- Deploy an optimized and secure active network infrastructure.
- Ensure high availability, redundancy, and load balancing for all network level (perimeter Firewall, datacenter firewall, core Switches, Access switches, WLC, NAC,
- Provide comprehensive training to the IT team.
- Ensure proper documentation and handover of the network.

2. Deliverables

- Detailed network design and architecture documents.
- Network architecture and topology wiring diagram.
- Heat map for wireless access points according to the selected model.
- Compliance matrix / compliance statement with RFP items.
- Installation and configuration of active network devices (switches, routers, firewalls, etc.).
- Network testing and commissioning reports.
- Training sessions for IT staff.
- Comprehensive network documentation, including network diagrams, configurations, and manuals.

Scope of Work Details

1. **Site Survey and Network Design**

- Conduct a detailed site survey to assess requirements for network device placement, power, cooling, and cabling.
- Develop a detailed network design and architecture, including IP addressing schemes, VLANs, routing protocols, and security policies with alignment with IT Team.
- Design redundancy and failover strategies to ensure network reliability.
- Submit the network design for approval by relevant stakeholders.

2. **Supply of Active Network Components**

- Provide and deliver all active network equipment, including but not limited to:
    - Core and access switches.
    - Routers.
    - Firewalls and security appliances.
    - Wireless controllers and access points.
    - Voice over IP telephony system
    - Network management and monitoring systems.
    - Uninterruptible Power Supplies (UPS) for network devices.

3. **Installation of Active Network Devices**

- Install network devices as per the approved network design and layout.
- Mount and secure devices in racks and cabinets, ensuring proper cable management and airflow.
- Ensure all devices are powered correctly and that redundant power supplies are connected to separate circuits for high availability.

4. **Configuration of Network Devices**

- Configure switches, routers, firewalls, wireless access points, Security systems and Collaboration systems based on the approved design and best practices.
- Set up VLANs, routing protocols (e.g., OSPF, BGP), and access control lists (ACLs) to ensure optimized traffic flow and security.
- Configure network security policies, including firewalls, VPNs, intrusion prevention systems (IPS), and network access control (NAC).
- Implement a Network Management System (NMS) for centralized monitoring, configuration, and troubleshooting of network devices
- **Ensure High Availability, Redundancy, and Load Balancing**
  Deploy redundant core switches, routers with failover capabilities to prevent single points of failure.
  Implement Layer 3 switches with redundancy with stacking or multi-chassis link aggregation for enhanced reliability to ensure seamless communication between core and access layers.
  Set up redundant WAN connections using diverse ISPs to ensure continuous connectivity and automatic failover in case of link failure.
  Utilize SD-WAN technology to dynamically manage and optimize WAN traffic.
  Deploy redundant firewalls in an active-active or active-passive configuration to protect the network perimeter and the data center without introducing a single point of failure.

5. Network Testing and Commissioning

- Perform end-to-end testing of the network, including connectivity tests, redundancy tests, failover tests, and performance tests.
- Document all test results and rectify any issues identified during testing.
- Prepare a detailed commissioning report, including test results, configurations, and network diagrams.

6. Integration with Systems

- Ensure seamless integration of the new network with existing IT systems, such as servers, storage, applications, and services.
- Migrate services, if necessary, with minimal disruption to ongoing operations.

7. Training for IT Staff

- Conduct training sessions for the IT team on the operation, monitoring, and management of the active network.
- Provide training on network management tools, including monitoring, troubleshooting, and reporting.
- Supply training materials, user manuals, and documentation.

8. Documentation and Handover

- Provide comprehensive documentation, including:
    - Network architecture and design diagrams.
    - Device configurations and IP addressing schemes.
    - Network security policies and configurations.
    - User manuals and training materials.
- Perform a final inspection and handover of the network to the client's IT team.
- Ensure that all documents are approved and signed by relevant stakeholders.

9. Project Timeline

- Vendor should Outline a detailed timeline with milestones for each phase: design approval, equipment delivery, installation, configuration, testing, training, and handover

Roles and Responsibilities

Vendor Roles and Responsibilities:

1. **Alignment with Project Manager:**
   - Collaborate with the company’s Project Manager to ensure alignment on project goals, timelines, and deliverables.
   - Participate in regular status meetings and provide updates on progress, risks, and issues.

2. **Configuration Approval:**
   - Work closely with the company's technical team to review and approve network configurations and designs.
   - Ensure that all configurations meet the project requirements and industry standards.
   - Provide documentation and rationale for any proposed changes or deviations from the initial plan.

3. **Implementation:**
   - Deploy network infrastructure components as per the approved configuration.
   - Ensure the installation adheres to the project’s specifications and quality standards.

4. **Testing and Validation:**
   - Perform testing to validate that the network infrastructure functions as intended.
   - Address any issues identified during testing and provide solutions for resolution.

5. **Training and Support:**
   - Offer training to the company’s IT staff on the new infrastructure, including best practices for management and troubleshooting.
   - Provide ongoing support during and after the implementation phase to resolve any issues that arise.

6. **Documentation:**
   - Deliver comprehensive documentation for all installed components, configurations, and changes.
   - Ensure that all documentation is clear, accurate, and easily accessible to the company’s IT team.

Company Roles and Responsibilities:

1. **Project Management:**
   - Oversee the overall project, including timelines, budgets, and resource allocation.
   - Act as the primary point of contact between the vendor and internal stakeholders.

2. **Configuration and Design Approval:**
   - Review and approve network designs and configurations proposed by the vendor.
   - Ensure that the designs align with the company’s requirements and security standards.

3. **Resource Provision:**
   - Provide necessary resources, including access to facilities, equipment, and personnel, to facilitate the vendor’s work.
   - Ensure that any internal dependencies are managed effectively to avoid project delays.

4. **Testing and Validation:**
    - Participate in testing and validation activities to confirm that the network infrastructure meets the company's needs.
    - Collaborate with the vendor to address any issues that arise during testing.

5. **Documentation Review:**
    - Review and validate the documentation provided by the vendor to ensure completeness and accuracy.
    - Maintain records of all network infrastructure components and configurations for future reference.

6. **Ongoing Management:**
    - Take responsibility for the ongoing management and of the network infrastructure post-implementation.
    - Address any issues or requirements that arise after the vendor's support period ends.

11. Standards and Compliance

- Ensure compliance with industry standards such as ISO/IEC 27001 (Information Security), ITIL (IT Service Management), and local regulatory requirements.

Financial offer

a. Payment Terms: payments will be in EGP. (30% downpayment,30% after delivery, 20% after installation, 20% after 6 months from handing over the project.
b. Delivery Duration within 2 - 3 months
c. Installation duration should be completed within 1 month
e. Warranty details :3 years for hardware
f. Licenses :3 years
g. After-sales support and service contract.

Vendor Specifications

1- Third party report:

A vendor must be among the Leaders in Gartner reports for wired and wireless networking at least three times for years 2020, 2021, 2022, 2023 and 2024.

2- Solution Integration:

Solution domains (SDN, WLC, NAC) MUST be from a single vendor.

3- The Vendor Preferred to have variety of the following IT solutions among their portfolios

- Collaboration solutions like Video conferencing endpoints, IP telephony, call managers
- SD-WAN routers that can act as voice gateways
- Enterprise switching models that are capable to host path performance monitoring solution.
- Data Center networking solutions including modular and fixed switches
- Hyper converged solutions
- Security solutions including NGFW, DNS layer security, on premises mail security solution, cloud-based security solution, NAC (Network access control solution)
- Application performance monitoring solution
- SDN (Software defined Networking) solutions for WAN (Wide area networks), LAN/access and Data Center.

4- The Vendor must have wide range of partners in Egypt with strong support organization for after sales operations

5- The Vendor must well industry recognized technical certifications in the following tracks

- Enterprise networking.
- Collaboration.
- Security.
- Data Center networking.

Project Timeline

Phase	Milestone	Duratio n	Start Date	End Date	Description
Project Planning	Project Kick-off	1 weeks	Week 1		Formal start of the project; align on goals, resources, and expectations.
	Design Approval	1weeks	Week 1		Finalize and approve network architecture and design.
Procurement	Vendor Selection and Procurement	1 weeks	Week 2		Select vendors and order necessary hardware and software components.
	Hardware Delivery	8 weeks	Week 3	Week 10	Delivery of all network equipment including switches, routers, firewalls, and other components.
Installation	Infrastructure Setup (Cabling, Racks)	1 weeks	Week 11		Install and test physical infrastructure including cabling, racks, and power supplies.
	Network Equipment Installation	1weeks	Week 11		Install switches, routers, firewalls, and other active network components.
Configuration	Network Configuration	1 weeks	Week 12		Configure devices with security policies, VLANs, routing protocols, etc.
	Security Configuration	1 weeks	Week 13		Implement security settings, including firewalls, IDS/IPS, and VPNs.
Testing	Network Testing and Optimization	1 weeks	Week 13		Test network performance, security, and redundancy.
Migration	Data Center Migration	1 weeks	Week 14		Migrate data center services to the new HQ network.
Training	Staff Training	1 weeks	Week 15		Train IT staff on new network operations and management.
Go-Live Preparation	Final Review and Go-Live Approval	1 week	Week 16		Review final configuration, sign-off, and prepare for go-live.
Go-Live	Network Go-Live	1 week	Week 16		Launch the active network; monitor closely for initial stability.
Post-Implementation	Post Go-Live Support	2 weeks	Week 17	Week 18	Provide support to address any immediate issues and fine-tune performance.
Project Closure	Project Close-Out	1 weeks	Week 19		Finalize documentation, complete any pending tasks, and formally close the project.

Key Points:

- **Total Duration**: 4 Months
- **Critical Milestones**: Project Kick-off, Design Approval, Network Go-Live, Project Close-Out.
- **Focus Areas**: Emphasis on Network, security, WLC, VOIP configuration, thorough testing, and comprehensive training to ensure a smooth transition.
- **Vendor Timeline**: vendor timelines should align with the provided project timeline to avoid delays.

Network Infrastructure Domain

1 - Networking infrastructure domain must be based on SDN (software defined networking) solution

Component	Quantity	Function
1- SDN Centralized Controller	1	• provide centralized management and assurance for both wired and wireless users • Underlay network configuration automation • Integrate with the NAC solution to provide automated way to configure user policy and segmentation • Solution must be supporting two type of services segmentation Marco segmentation: using different virtual networks Micro segmentation: using Scalable group tags (SGTs) • Have the option to be either physical appliance / virtualized form / cloud form
2- VRF leaking devices (Fusion Devices)	2	• To provide routing between different Macro segmentation virtual networks • To provide connectivity for services like Wireless LAN controllers, NAC, DC firewalls
3- Control nodes	2	• fabric control plane node is based on the LISP Map-Server and Map-Resolver functionality combined on the same node. The control plane node's database tracks all endpoints in the fabric site and associates the endpoints to fabric nodes, decoupling the endpoint IP address or MAC address from the location (closest router) in the network.
4- Border nodes	2	• Provides the connection between the Fabric and non-fabric traffic • Can be collocated on the same nodes as the control nodes
5- Edge devices	22	• Provides wired access to the users to the network • Endpoint registration—Each edge node has a LISP control-plane session to all control plane nodes. • Anycast Layer 3 gateway • Mapping of user to virtual network—Endpoints • VXLANencapsulation/de-encapsulation—Packets and frames received from endpoint
6- Wireless LAN controller	2	• Provides management for the access points
7- Access Points	57	• Provides access for the wireless users
8- NAC	2	• Provides authentication for both wired and wireless users • End points profiling services • Security assessment (posturing) • Integrates with the SDN controller
9- WAN Switches	2	• Traffic Routing and Load Balancing • Failover and Redundancy • Traffic Shaping and QoS (Quality of Service)

Centralized SDN controller:

- Single SDN controller with the following specification

. Hardware Specifications

- **Form Factor:**
  - **Physical Appliance:** 1RU rack-mounted server (typical for on-premises deployment)
  - **Virtual Appliance:** Specifications vary based on the hypervisor (e.g., VMware, Hyper-V)
  - **Cloud-Based:** Specifications depend on the cloud provider and instance type
- **Processors:**
  - **Type:** Multi-core processors (e.g., Intel Xeon or AMD EPYC)
  - **Cores:** Minimum of 8 cores, ideally 16 or more for performance and scalability
- **Memory:**
  - **Capacity:** 64 GB to 128 GB DDR4 RAM
  - **Configuration:** Dual-channel or higher for performance
- **Storage:**
  - **Type:** SSDs or NVMe storage for fast read/write access
  - **Capacity:** 1 TB to 2 TB, depending on logging and data retention requirements
  - **RAID:** RAID 1 or RAID 5 for redundancy
- **Networking:**
  - **NICs:** Dual 10GBASE-T or 25GBASE-T Ethernet ports for high-speed connectivity
  - **Management Interface:** Dedicated management port for out-of-band management

. Software and Features

- **Controller Software:**
  - **Type:** SDN controller software with support for standard protocols (e.g., OpenFlow, NETCONF)
  - **Features:** Network provisioning, traffic management, policy enforcement, and automation

- **Scalability:**
  - **Device Management:** Capable of managing up to 150 network devices with high performance and low latency
  - **Concurrent Sessions:** Support for a high number of concurrent management and monitoring sessions

- **High Availability:**
    - **Redundancy:** Support for high availability and failover configurations (e.g., active/passive or active/active)
    - **Backup and Recovery:** Built-in backup and disaster recovery features
- **Security:**
    - **Authentication:** Role-based access control (RBAC) and multi-factor authentication (MFA)
    - **Encryption:** Support for data encryption in transit and at rest
    - **Logging and Auditing:** Comprehensive logging and audit trails for security and compliance
- **API and Integration:**
    - **APIs:** RESTful APIs and/or gRPC for integration with other network management tools and automation systems
    - **Third-Party Integration:** Support for integration with security information and event management (SIEM) systems, orchestration platforms, and monitoring tools

4. Performance and Capacity

- **Throughput:** Sufficient throughput to handle control plane traffic for 150 devices, including configuration updates, telemetry, and policy enforcement
- **Latency:** Low latency for network control and configuration changes

5. Management and Usability

- **User Interface:**
    - **Web-Based UI:** Intuitive and responsive web-based management interface
    - **CLI Support:** Command-line interface for advanced configuration and troubleshooting
- **Monitoring and Analytics:**
    - **Dashboards:** Real-time monitoring dashboards for network performance, traffic patterns, and device status
    - **Analytics:** Advanced analytics capabilities for network health, traffic analysis, and capacity planning

Fusion devices – combined border and control nodes

Number of required switches	4
Port density	24x 1/10/25G Gigabit Ethernet + 4x 40/100G Uplink

ASIC performance numbers:

- Switching capacity Up to 3.2 Tbps
- Forwarding rate Up to 1 Bpps
- Total MAC addresses Up to 82,000
- Total IPv4 routes (indirect routes) Up to 256,000 indirect + direct
- Total IPv4 host routes (direct routes and ARP) Up to 90,000 host/ARP
- Total IPv6 routes (indirect routes) Up to 256,000 indirect + direct
- DRAM 16 GB
- Flash 16 GB
- VLAN IDs 4,094
- PVST Instances 4,000
- STP Virtual Ports (Port* VLANs) for PVST: 16000
- STP Virtual Ports (Port* VLANs) for MST: 100,000
- Total Switched Virtual Interfaces (SVIs):4,000

Supports the following Resiliency and High Availability mechanism:

- Software Maintenance Upgrade (SMU)
- Stateful Switchover (SSO)
- In-Service Software Upgrade (ISSU)
- Graceful Insertion and Removal (GIR)

Supports the following Security features

- Trustworthy Solutions
- Image Signing
- Secure Boot
- MACsec Encryption (256-bit AES-GCM)

Supports the following IP Routing Protocols

- Routing Information Protocol version 2 (RIPv2), and next generation [RIPng]
- Open Shortest Path First version 2 (OSPFv2), and OSPFv3
- Enhanced Interior Gateway Routing Protocol (EIGRP), and EIGRPv6
- Intermediate System-to-Intermediate System Version 4 (IS-ISv4)
- Border Gateway Protocol Version 4 (BGPv4), and BGPv6
- Protocol-Independent Multicast (PIM) Sparse-Mode (PIM-SM)
- PIM Source-Specific Mode (PIM-SSM)
- Bidirectional PIM (PIM-BIDIR)
- IPv6 routing
- L3 Routed Sub-Interfaces

Licensing: licensing model used on the switches must consist of the following

- **1- Permanent license:** This license covers the switching fundamentals, management automation, troubleshooting, and advanced switching features.

- **2-Subscription based license:** This license covers updates, advanced support analytics, and designated service management (Assurance)

Edge Switches:

Switch Port Count	Quantities
48 port PoE+	13
48 port UPOE, 36 ports 100M/1G/2.5G + 12 ports Multigigabit (10G/5G/2.5G/1G/100M)	8
24 port PoE+	1
2 x 25GE Network Module	4
8 x 10GE Network Module	9

General Technical specs

1. **Switching Architecture:**
   - Switches should utilize a modern ASIC-based architecture with programmable pipelines and micro engine capabilities. They should support template-based and configurable allocation of Layer 2 and Layer 3 forwarding, Access Control Lists (ACLs), and Quality of Service (QoS) entries.
2. **CPU and Memory:**
   - Switches should be equipped with an advanced CPU architecture, such as x86, with at least 8GB of memory to support the hosting of applications or containers directly on the switch.
3. **Uplink and Downlink Flexibility:**
   - Switches should offer flexible and dense uplink options including 1G, Multigigabit, 10G, 25G, 40G, and 100G, available as fixed or modular uplink configurations.
   - The downlink options should support a range of interfaces, including 1G Copper and Fiber, and provide high-density Multigigabit connectivity.
4. **Flow Collection and Forwarding:**
   - Switches should support line-rate, hardware-based flow collection, with the capability to handle up to 128,000 flows, ensuring efficient traffic monitoring and management.
5. **IPv6 and Dual-Stack Support:**
   - Full hardware support for IPv6 is required, providing wire-rate forwarding for IPv6 networks.
   - Support for both IPv4 and IPv6 (dual-stack) and dynamic hardware forwarding table allocations should be available to facilitate seamless migration from IPv4 to IPv6.
6. **Advanced Operating System Features:**
   - The operating system should provide enterprise-grade features, including model-driven programmability (e.g., NETCONF, RESTCONF, YANG), on-box Python scripting, streaming telemetry, container-based application hosting, and patching capabilities for critical bug fixes.
   - Integrated security features to protect against runtime attacks are essential.
7. **Network Visualization and Management:**
   - Capability for end-to-end visualization of network paths, from campus/branch locations to cloud/data centers, for effective network management and monitoring.

8. **IP Unicast Routing Protocols:**

   - Support for various IP unicast routing protocols, including static routes, RIP, RIPng, OSPF, BGP, and IS-IS, to provide robust routing capabilities for diverse network topologies.

11. **Multicast Routing Protocols:**

    - Support for Protocol-Independent Multicast (PIM) protocols, including PIM Sparse Mode (PIM SM) and Source-Specific Multicast (SSM), for efficient multicast traffic management.

12. **Multiprotocol Label Switching (MPLS) Support:**

    - Support for MPLS deployments, including MPLS L3 VPN, Virtual Private LAN Service (VPLS), Ethernet over MPLS (EoMPLS), and MPLS over GRE, to provide advanced network segmentation and traffic engineering.

13. **Advanced security that must be available in the switches:**

- **Encrypted Traffic Analysis:**
  The solution must have the capability to identify malware in encrypted traffic originating from the access layer, providing enhanced network security without compromising encryption.

- **Layer 2 Encryption:**
  The network solution must support standards-based encryption protocols, such as the IEEE 802.1AE MACsec, to authenticate and encrypt data packets between switches, ensuring data confidentiality and integrity.

- **Hardware and Software Authenticity:**
  The switching solution must support robust mechanisms to ensure authenticity and mitigate risks of man-in-the-middle attacks or unauthorized modifications to software and firmware, including:

- Image Signing:
  Cryptographic signing of firmware, BIOS, and software images to ensure they are authentic and have not been tampered with.

- Secure Boot Sequence:
  Layered protection for the boot sequence to prevent the persistence of illicitly modified firmware.

- Hardware Authenticity:
  Unique identification mechanisms to verify the authenticity of hardware components and ensure the product is genuine.

14. **DNS Security Integration:**
    The solution should allow for customizable DNS filtering policies at a granular level (e.g., user or group level) to control access to malicious or inappropriate websites for BYOD, IoT, guest, or corporate users.

High Availability: The network switches must support robust high-availability features, including:

- Link Aggregation Across Devices: Ability to configure aggregated interfaces across different devices or members of a stack for enhanced resiliency.
- Redundant Interfaces and Port Channels: Capability to configure active and backup interfaces or port channels, providing Layer 2 failover redundancy without relying on the Spanning Tree Protocol (STP).
- Fast Upgrade and Reload: The ability to upgrade platform software or reload the system with minimal traffic impact (under 30 seconds), applicable for both stand-alone and stack configurations.
- Multiple Spanning Tree Protocol (MSTP) Support: Support for IEEE 802.1s MSTP, enabling rapid spanning tree convergence independent of timers and allowing Layer 2 load balancing and distributed processing.
- Non-Stop Data Forwarding: Support for continuous data forwarding to minimize traffic downtime during switchovers.

Licensing: licensing model used on the switches must consist of the following

1- Permanent license: This license covers the switching fundamentals, management automation, troubleshooting, and advanced switching features.

2- Subscription based license: This license covers updates, advanced support analytics, and designated service management (Assurance)

The proposed NAC Solution should support below features:

- **Endpoint Classification & Visibility**

The NAC solution must detect both new and existing endpoints and categorize them by type (e.g., Windows, Linux/Unix, printers, IP cameras, smartphones, tablets, network devices, etc.).

- **Endpoint Profiling**

The NAC should identify new network connections and determine if the device is part of the corporate network or domain. It should support device-specific templates and authorization policies based on device type. Additionally, the solution should support downloadable access lists and URL redirection.

- **Endpoint Compliance**

The NAC must verify and assess compliance for various parameters including antivirus signatures, operating system updates, registry settings, server services, and peer-to-peer applications.

- **Deployment Options**

The NAC solution should support deployment either within Layer 2 (L2) proximity of users or multiple hops away, depending on the network design.

- **Deployment Method**

The NAC appliance should offer both in-band (IB) and out-of-band (OOB) deployment options. In-band deployment places the NAC appliance in line with user traffic, while out-of-band allows users to bypass the NAC appliance after certification during vulnerability assessments.

- **Endpoint Access Control**

The NAC should block non-compliant or unknown users across wired, wireless, and VPN networks.

- **Endpoint Remediation**

The NAC solution should redirect non-compliant endpoints to quarantine segments and apply remediation policies to address compliance issues.

- **Multivendor Support**

The NAC should support devices from multiple vendors to enhance network intelligence and visibility.

- **Multi-Identity Support**

The NAC must support multiple authentication and authorization sources, such as Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and Authentication, Authorization, and Accounting (AAA) systems.

- **High Availability**

The NAC solution should support both Active/Active and Active/Standby high availability configurations

- **Guest Management**

The NAC should be able to identify guest users and devices, distinguish them from registered users and devices, and enforce access limitations based on predefined policies.

- **Alert Mechanism**

The NAC must provide email notifications with detailed information when there is a violation of defined policies.

- **Reporting**

The NAC dashboard should offer detailed reports to provide comprehensive visibility into network endpoints.

- **Integration with SDN Controller**

The NAC solution should integrate with a Software-Defined Networking (SDN) controller to automate segmentation policies.

Wireless LAN Controller:

Item	**Specification**
Quantity	2
Maximum number of access points	Up to 250, expandable to 500 with additional licensing
Maximum number of clients	Up to 5,000, expandable to 10,000 with additional licensing
Maximum throughput	Up to 5 Gbps, expandable to 10 Gbps with additional licensing
Maximum WLANs	4096
Maximum VLANs	4096
Fixed uplinks	2x 10G/Multigigabit fiber
Power supply	110W, 12V DC, AC/DC adapter

Access Points

Item	Specification
Quantity	57
802.11n version 2.0 (and related) capabilities	● Supports 4x4 Multiple-Input, Multiple-Output (MIMO) with four spatial streams ● Maximal Ratio Combining (MRC) for improved signal quality ● Beamforming support for 802.11n and 802.11a/g standards ● Channel width options of 20 MHz and 40 MHz ● Physical (PHY) data rates up to 890 Mbps (40 MHz at 5 GHz, 20 MHz at 2.4 GHz) ● Packet aggregation support: A-MPDU (transmit and receive), A-MSDU (transmit and receive) ● Dynamic Frequency Selection (DFS) for interference avoidance ● Cyclic Shift Diversity (CSD) support
802.11ac	● Supports 4x4 downlink Multi-User MIMO (MU-MIMO) with four spatial streams ● Maximal Ratio Combining (MRC) ● Beamforming support for 802.11ac standard ● Channel width options of 20 MHz, 40 MHz, 80 MHz, and 160 MHz ● Physical (PHY) data rates up to 3.47 Gbps (160 MHz at 5 GHz) ● Packet aggregation support: A-MPDU (transmit and receive), A-MSDU (transmit and receive) ● Dynamic Frequency Selection (DFS) for interference avoidance ● Cyclic Shift Diversity (CSD) support
802.11ax	● Supports 4x4 downlink Multi-User MIMO (MU-MIMO) with four spatial streams ● Supports uplink and downlink Orthogonal Frequency Division Multiple Access (OFDMA) ● Target Wake Time (TWT) for improved power efficiency ● Basic Service Set (BSS) Coloring for reducing co-channel interference ● Maximal Ratio Combining (MRC) ● Beamforming support for 802.11ax standard ● Channel width options of 20 MHz, 40 MHz, 80 MHz, and 160 MHz ● Physical (PHY) data rates up to 5.38 Gbps (160 MHz at 5 GHz, 20 MHz at 2.4 GHz) ● Packet aggregation support: A-MPDU (transmit and receive), A-MSDU (transmit and receive) ● Dynamic Frequency Selection (DFS) for interference avoidance ● Cyclic Shift Diversity (CSD) support
Integrated antenna	● 2.4 GHz, peak gain 3 dBi, internal antenna, omnidirectional in azimuth ● 5 GHz, peak gain 4 dBi, internal antenna, omnidirectional in azimuth
Interfaces	● 1x 100, 1000, 2500 Multigigabit Ethernet (RJ-45) – IEEE 802.3bz ● Management console port (RJ-45) ● USB 2.0
Available transmit power settings	**2.4 GHz** ● 23 dBm (200 mW) ● -4dBm (0.39mW) **5 GHz** ● 23 dBm (200 mW) ● -4dBm (0.39mW)

WAN Switches

Switch Port Count	Quantities
24-port Data 4x10G uplink Switch,	2

With the following technical specifications

Item	Specification
Switching capacity	• Switching Capacity: Minimum of 100 Gbps or higher.
Stacking bandwidth	• Stacking Bandwidth: Minimum of 60 Gbps or higher.
Total number of MAC addresses	• MAC Address Table Size: Support for at least 15,000 MAC addresses.
IPv4 routing entries	• IPv4 Routing Table Size: Support for a minimum of 2,500 entries or higher.
IPv6 routing entries	• IPv6 Routing Table Size: Support for a minimum of 1,000 entries or higher.

Licensing: licensing model used on the switches must consist of the following

1- Permanent license: This license covers the switching fundamentals, management automation, troubleshooting, and advanced switching features.

2- Subscription based license: This license covers updates, advanced support analytics, and designated service management (Assurance)

SFP Modules

SFP Module	Quantity
100GBASE QSFP Active Optical Cable, 5m	4
10GBASE Active Optical SFP+ Cable, 5M	4
10GBASE-SR SFP Module, Enterprise-Class	20
Dual Rate 10/25GBASE-CSR SFP Module	8

Collaboration Solution

- All the solution components end points, video conferencing, licenses, voice gateway , call control must be of the same vendor
- The vendor must provide enterprise agreement system which provides free licenses and licenses for future growth
- Solution must have the following component

Item	Quantity
On Prem call control	1
C Level IP Phones	12
Employees IP Phones	218
General Use IP Phones	259
Conference room IP Phone	3
Licenses	**Calling Professional:** 12 **Calling Enhanced:** 218 **Calling Access:** 259
Voice Gateway	1

On Prem Call control

General Technical specs

Server Requirements:

- The server must host all unified communications applications with a preinstalled virtualization hypervisor and preloaded software. Which can support up to 1000 users.
- The server must be equipped with a single processor having at least 10 cores and a clock speed of 2.20 GHz.
- The server must include a modular RAID controller with at least 2GB of cache.
- The server must offer a minimum storage capacity of 300 GB with hot-swappable drives.

Call Control System:

- The system should operate with redundancy; active calls must continue uninterrupted if the primary call manager fails.
- Quality of Service (QoS) parameters, including support for 802.1p/q, RSVP, and Call Admission Control, must be present.
- All IP phones should be compatible with the call control system, support Power over Ethernet (PoE), and not require additional electrical cables or adapters.
- All devices and applications must use IP and SIP for communication.
- The IP Phone Call Manager Software and equipment, including IP phones, IVR, and call control applications, should be from the same manufacturer.
- The system must support automatic and scheduled backups of the software.
- System updates should not interrupt operations.
- Centralized user management must be supported via a secure web-based interface.
- User licenses must match the number of phones, with all necessary software and hardware included for internal communication.

- The system must support a PC-based operator console for switchboard operations.
- Subscriber settings should be transferable between phones, allowing users to log in and retain their configurations.
- Voice traffic must comply with AES standards for encryption.
- The system should include a point-to-point video solution and a personal address book.
- All configurations and plans must be stored in a database.
- Support for H.323 and SIP trunking protocols is required, with direct connection capabilities for H.323-based clients.
- Error situations must trigger alerts for users, including both voice and visual notifications.
- Users should be able to customize phone ringtones and adjust volume settings.
- The Call Manager must support the following audio codecs:
  - G711 a-law
  - G711 u-law
  - G729 a
  - G729 b
  - G729 EU
  - G722
- The Call Manager must support the following video codecs:
  - H263
  - H264

- The Call Manager must support the following fax/modem codecs:
  - Fax Pass Through
  - T.38 Fax Relay
  - SIP T.38
  - MGCP T.38

- Caller number information should be displayed on screen for internal and external calls.
- Phones should be able to automatically register with the call manager and start working; this feature should be optional.
- The Call Manager interface must identify H.323, SIP, and MGCP audio paths.
- The system should support TLS and SIP SRTP for signaling and media encryption with at least AES 256 encryption. Minimum SHA-512 and RSA-3072-bit encryption should be supported.
- If a subscriber is busy, the caller should be able to activate a callback feature for later contact.
- Incoming calls should be redirectable to another number if the user is busy.
- Call parking should be supported, allowing users to retrieve parked calls from any phone by dialing a system-provided number.

C-Level IP Phone

Feature	Specification
Display	● 7-inch LCD monitor ● 1024 * 600 resolution ● IPS LED panel ● Contrast ratio: 1200:1 (typical) ● Viewing angle: +/- 85° (typical) ● Brightness: 350 cd/m2 color depth 16.7M colors
Camera	● 72° horizontal field of view, 45° vertical field of view ● f/2.2 aperture ● 4MP image sensor, supports up to 30 fps ● 1/3-inch CMOS ● Face detection–based automatic focus and exposure ● Automatic white balance ● Focus distance: 20 cm (about 7.87 in) to infinity ● Privacy shutter and LED light in front (indicating camera status)
Audio	● Frequency response: 150 Hz – 20 kHz full band support ● AEC (Acoustic Echo Cancellation) ● BGN (Background Noise Reduction) ● AGC (Automatic Gain Control) ● CNG (Comfort Noise Generation) ● VAD (Voice Activity Detection) ● Silence Suppression ● Acoustic Shock Protection (Handset/headset) ● Packet Loss Concealment ● Adaptive Jitter Buffer ● Dual Tone Multi-Frequency (DTMF) tone generation (RFC 2833 and in-band) ● TIA-920 WB/HD audio compliant
Audio codec support	G.711 a-law and mu-law, G.722, G.729a, Internet Low Bitrate Codec (iLBC), OPUS and Internet Speech Audio Codec (iSAC)
Video	● Video stream: full HD 1080p30 ● H.264 AVC
Hard keys	● Hold/Resume, Transfer, and Conference keys ● Messaging, Application, and Directory keys ● Standard keypad ● Volume-control toggle key ● Speakerphone, Headset, and Mute keys ● Home button ● Power button
Speakerphone	The full-duplex speakerphone gives you flexibility in placing and receiving calls with hands free. For added security, the audible Dual Tone Multifrequency (DTMF) tones are masked when the speakerphone mode is used.

USB	● One USB-C and one USB-A port enhance the usability of call handling by enabling wired or wireless headsets, in addition to providing. charging capability to mobile devices such as smartphones or tablets. ● A side USB-A port provides up to 2.1A power output at 5V or 10.5W for charging.
Ethernet switch	● An internal 2-port Ethernet switch allows for a direct connection to a 10/100/1000BASE- T Ethernet network (IEEE 802.3i/802.3u/802.3ab) through an RJ-45 interface with single LAN connectivity for both the phone and a co-located PC. ● The system administrator can designate separate VLANs (IEEE 802.1Q) for the PC and phone, providing improved security and reliability of voice and data traffic.
Bluetooth	● The phone offers Bluetooth 4.2 LE, Enhanced Data Rate (EDR) Class 1 technology (up to 66-ft [20m] range). ● Hands-Free Profile (HFP) is supported for untethered headset connections and voice communications.
Wi-Fi	● Wi-Fi 802.11a/b/g/n/ac ● 2.4 GHz/5 GHz dual bands ● Authentication: WPA, WPA2, EAP-FAST, PEAP-MSCHAPv2, PEAP- GTC ● IEEE 802.11d ● IEEE 802.11r ● IEEE 802.11e ● IEEE 802.11h ● Call Admission Control (CAC)
Security	● Secure boot ● SIP OAuth ● Secure credential storage ● Device authentication ● Configuration file authentication and encryption ● Image authentication ● Random bit generation ● Hardware cryptographic acceleration ● Secure Unique Device Identifier (SUDI) ● Ethernet 802.1x supplicant options: Extensible Authentication ● Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) and Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) ● Signaling authentication and encryption using TLS ● Media authentication and encryption using SRTP ● HTTPS for client and server ● TLS 1.0 disabled ● Phone local password lock for setting menu *
Language Support	● Arabic (Arabic Area) ● English (United States)

Employees Phone

Feature	Specification
Graphical display	White backlit, greyscale, 3.5” 396×162 pixel-based display
Headset	The analog headset jack is a standard wideband-capable RJ-9 audio port
Volume control	A volume-control toggle provides easy decibel-level adjustments of the handset, monitor speaker, and ringer.
Wall-mountable	The phone can be installed on a wall using optional wall-mount kit
Keys	● The phone has the following keys ◦ Line keys ◦ Soft-keys ◦ Two-way navigation and select keys ◦ Hold/Resume, Transfer and Conference keys ◦ Messaging, Service and Directory keys ◦ Standard key pads ◦ Volume control toggle key ◦ Speakerphone, headset and mute keys
Key call features support	● + Dialing (E.164) ● Abbreviated dial

Codec support	G.711a/ *μ*, G.722, G.729a/b, iLBC, OPUS
Language support	● Arabic (Arabic Area) ● Catalan (Spain) ● English (United Kingdom) ● French (France)

Features	● Adjustable ringing and volume levels ● Adjustable display contrast ● Agent greeting ● Auto-answer ● Auto-detection of headset ● Busy Lamp Field (BLF) ● Call back ● Call forward ● Call history ● Call Park ● Call Pickup ● Call timer ● Call waiting ● Caller ID

Features	● cBarge ● Corporate directory ● Conference ● Cross Cluster Extension Mobility (EMCC) ● Dial from the list ● Direct transfer ● Do not disturb ● Extension Mobility (EM) ● Forced access codes and client matter codes ● Group call pickup ● Hold/resume ● Immediate divert ● Intercom ● Join ● Message-waiting indicator ● Meet me conference ● Mobility ● Music on hold ● Mute ● Network profiles (automatic) ● On- and off-network distinctive ringing ● Personal directory ● Privacy ● Private Line Automated Ringdown (PLAR) ● Redial ● Ring tone per line appearance ● Shared line ● Silent monitoring and recording ● Speed dial ● Time and date display ● Transfer ● Voicemail ● Whisper coaching

General Use IP Phones

Feature	Specification
Graphical display	Non-backlit, greyscale, 3.28” 384×106 pixel-based display
Full duplex speakerphone	Full-duplex speakerphone allows gives you flexibility in placing and receiving calls. For added security, the audible Dual Tone Multifrequency (DTMF) tones are masked when the speakerphone mode is used.
Volume control	A volume-control toggle provides easy decibel-level adjustments of the handset, monitor speaker, and ringer.
Wall-mountable	The phone can be installed on a wall using optional wall-mount kit
Keys	● The phone has the following keys ◦ Line keys ◦ Soft-keys ◦ Two-way navigation and select keys ◦ Hold/Resume, Transfer and Conference keys ◦ Messaging, Service and Directory keys ◦ Standard key pads ◦ Volume control toggle key
Key call features support	● + Dialing (E.164) ● Abbreviated dial ● Adjustable ringing and volume levels ● Adjustable display contrast ● Agent greeting ● Auto-answer ● Call back ● Call forward ● Call history ● Call park ● Call Pickup ● Call timer ● Call waiting ● Caller ID ● cBarge ● Corporate directory ● Conference ● Cross Cluster Extension Mobility (EMCC) ● Dial from the list ● Direct transfer ● Do not disturb ● Extension Mobility (EM) ● Forced access codes and client matter codes ● Group call picku

Conference room IP Phone

Feature	Specification
Display	6-inch 1080p full HD touch
Buttons	Dedicated mute and volume buttons with cap touch
Video inputs	One HDMI input supports up to 1080p30
Video outputs	One HDMI output supports up to 1080p30
Audio	• OPUS, G.722, G.729a/ab, and G.711 (u/a) • Automatic gain control • Comfort noise generation • Silence suppression/voice activity detection • Acoustic echo cancellation and noise reduction
Speakers (integrated)	• 2 speakers (woofer and tweeter) • High-quality 22-kHz speaker • Maximum adjustable volume: 89 dB within 0.5 m
Security features	• Secure credential storage • Image authentication • Random bit generation • Manufacturer-Installed Certificates (MICs) • Secure boot • SHA-256 enabled for advanced security features • Signaling authentication and encryption using TLS v1.2 • Media authentication and encryption using Secure Real-Time Transport Protocol (SRTP)
Network interfaces	One Ethernet (RJ-45) 10/100/1000 for LAN with Power over Ethernet (PoE) support
IEEE POE	IEEE PoE Class 3

Security Solutions

- Security solution must consist of the following blocks
  1- Data Center Firewalls
  2- Multifactor authentication
  3- DNS Security Solution
- All the components of the security solutions must be from the same vendor
- Security solutions must be the same as the Network infrastructure and collaboration vendors

Data Center Firewalls:

Feature	Specification
Quantity	2 Firewalls operating as an HA (High Availability) pair.
Total Throughput (Firewall + Application Visibility and Control) (1024B)	10 Gbps
Required licenses	Threat intelligence licenses Malware defense
Maximum Concurrent Sessions (with Application Visibility and	1.5 million
Maximum new connections per second, with AVC	90,000
Throughput: NGIPS (1024B)	10.0 Gbps
Maximum VPN Peers	2,000
Form factor (rack units)	1RU
Integrated I/O	8 x 10/100/1000 Mbps Ethernet interfaces (RJ-45) 8 x 1/10 Gigabit Ethernet interfaces (SFP)
Weight	1 x power supplies, 1 x NM, fan module, 1x SSD
Integrations	
Threat intelligence	• Solution MUST have the option to provide all threat intel feeds to other devices in STIX format • Must take decision based on IP reputation • Must take decision based on URL reputation • Must take decision based on DNS reputation • Must take decision based on FILE reputation • Security intelligence must come from multiple sources • Security intelligence must come from different product types • Must integrate with 3rd party security intelligence sources
IPS requirements	• Solution MUST have an IPS included on the same box • IPS must be able to analyze and detect unused signatures, and provide recommendations on signatures to be applied or removed • IPS must be able to detect QUIC protocols

	• Capable of prioritizing and tuning signatures based on vulnerability scanner feedback • Compliant with industry definitions for Next-Generation IPS • Should support Network Discovery • Must support the import of Snort rules • Capable of dynamic tuning based on context awareness • Should defend against evasion techniques with appropriate traffic processing • Must include file-based policy controls for file types • Should provide visibility and statistics on applications based on risk and business relevance • Capable of dynamically adjusting attack priority based on host profiles • Should perform automated event impact assessment by correlating attacks to targets • Must identify and manage Host Profiles for all IP addresses in communication
Decryption	• Solution must be able to decrypt TLS 1.3 • Firewall must be able to detect encrypted traffic with a high level of confidence without the need to decrypt it. Utilizing handshakes analysis, machine learning and other techniques for fingerprinting. • Must Security features such as SSL decryption, application awareness, application visibi lity, advanced malware protection, security intelligence, intrusion detection, intrusion prevention, quality of service, data loss prevention, address translation • The product shall decrypt outbound and inbound SSL and TLS traffic.

Multi-factor authentication

Feature	Specification
Licenses count	500 user
MFA Features	• MFA with security keys, FIDO2, OTP, phone callback, SMS and hardware tokens • Multi-Factor Authentication with Push for iOS and Android • Unlimited application integrations • User self-enrollment & self-management • Telephony credits: 100 credits/user/year
Push Phishing Protection	• Customizable number-matching with Verified push MFA • Enforce utilization of phishing-resistant factors • Immediate alert of suspicious logins
Trusted Endpoints	• Allow only managed and registered devices to access applications • Enforce trust on BYOD and 3rd party devices through device registration • Limit device access to applications based on enrollment in endpoint management systems such as LANDesk, JAMF, Microsoft Intune
Adaptive Access Policies	• Ability to assign and enforce authentication policies globally or by user group • Policy enforcement based on network authorization • Security policy assignment and enforcement on a per-application basis

DNS Security Solution

Feature	Specification
Licenses count	500 user
Infrastructure	• DNS requests are transparently sent to the fastest available node and automatically re-routed in the event of downtime.
Global cloud architecture	• The solution should provide insights based on a diverse, global, and real-time dataset. • Must process a large volume of DNS requests daily, supported by a substantial number of active users across multiple countries. • Real-time data enriched with diverse public and private data feeds
Statistical and machine learning models	• The solution should use statistical and machine learning models to automatically score and classify data, detect anomalies, and uncover both known and emerging threats. • Must have the capability to predict potentially malicious destinations and identify threats that could be used in future

DNS-layer enforcement	• The solution should be capable of resolving DNS queries and enforcing security policies against malicious domains without adding latency. • Should provide comprehensive visibility to protect internet access across all network devices, office locations, and roaming users.
Selective proxy	• The solution should include a selective proxy feature, where only requests to a set of risky domains (those hosting both malicious and legitimate content) are proxied for deeper inspection, minimizing performance impacts. • It should be able to check files attempted to be downloaded from risky sites against antivirus engines and file reputation services.
On-network coverage	• Leverage existing DNS and DHCP infrastructure to provision across your network. This also includes any device that connects to the network, even those not owned by your organizationwith no hardware to install or software tomaintain.
Roaming client	• The solution should provide DNS-level protection for laptops beyond the network perimeter and pinpoint activity to specific endpoints on or off the network to expedite remediation. The client software should be lightweight, with all enforcement occurring in the cloud.

UPS

Specification	Requirement
UPS Quantity	2 Units
Redundancy Configuration	High Availability (HA) Setup
Backup Time	Minimum 16 minutes at full load
Capacity	40 kVA
Input Voltage	400V, 3-phase input
Output Voltage	400V, 3-phase output
UPS Topology	Online double conversion (VFI)
Efficiency	High efficiency at full load (e.g., > 95%)
Battery Type	Valve Regulated Lead Acid (VRLA) or Lithium-Ion
Battery Replacement	Hot-swappable battery modules
Communication Interface	SNMP, Modbus, and dry contact support
Monitoring and Management	Network management and monitoring capabilities
Environment	Suitable for data center environments
Compliance	Must comply with IEC or other relevant standards

Passive Components

Item Description	Quantity	Unit
Fiber Patch Panel 12 Port LC	10	Each
Splice Tray Kit for Fiber Patch Panel	10	Each
1U Patch Cord Organizer	10	Each
Optical Fiber Adapter (OM4, LC/LC)	60	Each
Fiber Pigtail OM4, LC, 2M	120	Each
Fiber Patch Panel 24 Port LC	6	Each
Splice Tray Kit for Fiber Patch Panel	6	Each
1U Patch Cord Organizer	6	Each
Optical Fiber Adapter (OM4, LC/LC)	72	Each
Fiber Pigtail OM4, LC, 2M	144	Each
Fiber Patch Cords LC-LC 3M	15	Each
Fiber Patch Cords LC-LC 1.5M	40	Each
Fiber Patch Cords LC-LC 1.5M	12	Each
Fiber Jumper Cable, LSZH, Duplex, LC/LC, 10ft	79	Each
1U Patch Cord Organizer	52	Each
Patch Cord 25cm, Cat 6, UTP, LSZH	1188	Each
Patch Cord 3m, Cat 6, UTP, LSZH	500	Each
Patch Cord 1m, Cat 6, UTP, LSZH	550	Each
Service Installation	1	Lot

Accept Vendor List

Category	Accepted Brands
Active Network	
Switches	Cisco, Juniper, HPE Aruba, Huawei
Routers	Cisco, Juniper, HPE Aruba, Huawei
Wireless LAN Controllers (WLC)	Cisco, Aruba, Huawei
Access Points	Cisco, Aruba, Huawei
NAC Solution	Cisco ISE, Aruba ClearPass, Huawei
Firewall	Palo Alto Networks, Fortinet
Data center firewall	Palo Alto Networks, Cisco
DNS Security	Cisco Umbrella, Cloudflare
Collaboration	Cisco, Avaya, Grand stream
SDN Management Software	Cisco DNA, HPE Aruba Central, Huawei
Passive Components	
Passive Components	CommScope, R&M, Corning ” Should be same as approved copper and fiber cables”
UPS	APC, EATON, Huawei