# **Next Generation Firewall**

## **Technical Requirement**

1. **Introduction:**

MIC2 manages a mobile network in Lebanon since June 2004. In collaboration with the Lebanese Ministry of Telecommunications, touch continues to enhance its network capacity while consistently providing its customers with cutting-edge products and services. It also seeks to improve the quality and variety of its services, without compromising on cost-effective pricing modules.

MIC2 intends to deploy redundant firewalls at its Internet Gateway core sites in addition to switches and other accessories. These firewalls are expected to integrate with the existing MIC2 live network, thereby enhancing the overall client experience.

* + Bidder must submit a minimum 5 years roadmap for the proposed solution.
  + Bidder must provide on-site and/or remote support based on the requested service level agreement.
  + Bidder must have the needed skills and existing professional resources to deploy the solution.

1. **General Requirements :**

* Bidder should provide complete Design and plan for the solution
* Bidder is responsible for solution installation and implementation.
* Bidder is responsible for provisioning, testing and system integration.
* Bidder is responsible for migration from existing FWs in the three core sites.
* Bidder is responsible complete equipment supply and delivery.
* Bidder must ensure validation of system integration with various systems used.
* Bidder must submit 5 years roadmap highlighting the committed features
* Vendor should have at least 5 references in similar deployment
* Bidder must specify where the solution has been integrated and what are the implemented use cases
* Bidder must submit total compliance with the launching date that should not be by any means more than 3 months for the whole project.
* Bidder must submit responsibility matrix, including human resource requirements.
* Bidder must submit global and provisional acceptance test procedures.
* Bidder must provide validation of system integration with various systems used.
* Bidder must provide extended maintenance and support/warranty.
* Bidder must provide on-site assistance after the final acceptance.
* Bidder is requested to provide benchmark performance indicators based on the proposed solution and on the hardware recommended.
* Bidder must have back-to-back support from the vendor
* Bidder must be willing to demonstrate the various system elements of the solution.
* Bidder must also be prepared to give a presentation of the solution if required.
* Bidder should provide details of relevant operational reference sites.
* Bidder must provide Gartner report for 2023 concerning the proposed product.
* The proposed firewall must be a L7 - Application aware - NGFW from day one

1. **Next Generation Firewall Technical Requirements :**

* **Operating System Compatibility**: Bidder must provide management solution that can provide single interface for operations, alarm generation and performance monitoring and reporting.
* **Network Connectivity**: Sufficient network interfaces, including Ethernet and fiber-optic ports, to accommodate network connections. Support for various network speeds (e.g., Gigabit Ethernet, 10, 25, and 40 Gigabit Ethernet ). At least 8 SFP/SFP+ ports for fiber connectivity to be used for future expansion – 8 ports will be used for initial deployment.
* **Scalability**: The ability to scale resources to meet increasing network demands. Support for expansion modules or additional hardware for increased capacity.
* **Redundancy and High Availability**:
  + Support for high availability (HA) and failover configurations to ensure uninterrupted service in case of hardware or software failure.
  + Redundant power supplies and fans for hardware resilience.
* **Virtualization Support**: Compatibility with virtualization platforms for deploying virtual NGFW instances.
* **Authentication and Access Control**:
  + Integration with authentication systems such as LDAP, Active Directory,TACACS or RADIUS.
  + User and group-based access control policies.
* **Security Services:**
  + Capability to install antivirus, anti-malware, and anti-phishing services.
  + Intrusion detection and prevention capabilities.
  + Application control and URL filtering.
  + SSL/TLS inspection capacity.
  + Botnet detection and protection.
* **Content Filtering**:
  + URL filtering and categorization capabilities.
  + Integration with threat intelligence feeds.
  + Customizable content filtering policies.
* **VPN Support**:
  + Support for various VPN protocols (e.g., SSL VPN, IPsec).
  + Remote access VPN capabilities.
  + VPN load balancing and failover options.
* **Compliance and Certifications**:
  + Compliance with industry regulations and standards (e.g., GDPR, HIPAA).
  + Certifications such as Common Criteria.

1. **Next Generation Firewall Hardware Requirements**
   * Hardware Requirements: CPU and memory must not exceed at peak traffic 60% to allow to handle traffic inspection and security services Adequate storage for logs and firmware updates.
   * The proposed appliance must have minimum 8 x 1/10/25/40 Gigabit Ethernet ports from day one.
   * The appliance must be scalable to add another module of 8 x 1/10/25/40 or 100 Gigabit Ethernet ports from day one.
   * The Appliance must have minimum 4 x 40G QSFP module from day one. All modules, transceivers & license need to be provisioned from day one. HA, Sync & Management port must be provided separately.
   * Solution must support all hardware redundancy including control board, switching board, Power/FAN module.

* The proposed appliance must have:
  + 1 x 1G port for out of band management
  + 2 x 1G port for HA connectivity
  + 2 x 10G to sync config / session between HA pair
  + These ports must be in addition to production ports mentioned earlier.
* The proposed solution must have minimum 240GB SSD drive for storing operating system image, system files, system logs & network traffic logs.
* The Appliance must have minimum 128 GB RAM from day one.
* The appliance must have 2 x redundant power supplies from day one. Power supplies must be hot swappable
* The appliance must have hot swappable fans.
* The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle:
  + Management functions like configuration,
  + reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#)
  + Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc)
  + Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc).
* The administrator must be able to view report on the CPU usage for management activities and CPU usage for other activities.

1. **Next Generation Firewall Performance Requirement**
   * The proposed firewall must provide NGFW functionality from day one. All required license must be provided from day one.
   * The proposed firewall must provide minimum 65 Gbps of throughput with NGIPS
   * The proposed appliance must support minimum 15 Million concurrent sessions with Real world HTTP applications and not based on UDP / Lab environment / ideal testing environment
   * The proposed appliance must support TLS with minimum throughput of 20Gbps
   * The proposed firewall must support minimum 350,000 new session per second with real world HTTP application and not based on UDP / Lab environment / Ideal testing environment
2. **Next Generation Firewall Features**
   * The proposed firewall must be a L7 - Application aware - NGFW from day one
   * It must allow to create security policies based on L7 parameters such as Application, Users, File Type etc in addition to IP & Port numbers.
   * While creating application based policy the firewall must auto select all default port numbers without need of admin to mention it separately. Example - while allowing Active Directory as an application, firewall must auto include all relevant port numbers used for AD communications such as 135, 138, 139, 389, 445 etc
   * Preferred to have informational or warning message to admin about dependent application to be included in policy to avoid application misbehavior
   * the proposed solution must support at least 4000 applications
   * The Firewall must support Active - Passive & Active – Active deployment option with IPV4 & IPV6 with seamless failover between HA pairs.
   * The proposed solution must provide capability to develop custom application detector rules
   * The proposed solution must support importing open source application rules.
   * The proposed solution must support blocking based on security intelligence information with IP, URL.
   * The NGFW must have GUI based packet capture utility within its management console with capability of creating packet capture filters for IPv4 and IPv6 traffic and ability to define the packet and byte count limit for the capture
   * The proposed solution must support Policy Based forwarding based on:
     + Zone
     + Source or Destination Address
     + Source or destination port
     + Application (not port based)
     + AD/LDAP user or User Group
     + Services or ports
   * The proposed solution should support the ability to create QoS policy on a per rule basis:
     + by source address
     + by destination address
     + by application (such as Skype, Bit torrent, YouTube, azureus)
     + by static or dynamic application groups (such as Instant Messaging or P2P groups)
     + by port and services
   * The NGFW must provide immediate visibility into applications bypassing traditional security policy & running on non-standard ports.
   * The Firewall must able to provide comprehensive report with Source/Destination IP, Application name (real application name & not protocol), source & destination Zone, data transfer amount & file name transfer, source port and destination port.
   * The product shall support Authentication, Authorization, and Accounting (AAA) protocols and support certificate-based authentication as well as integrate with Microsoft Active Directory/ Lightweight Directory Access Protocol (AD/LDAP) and Remote Authentication Dial-In User Service (RADIUS) to associate traffic to users for multiple domains, authenticate VPN client users, etc.
   * The NGFW must be able to acquire User Identities from: LDAP, Captive Portal, VPN.
   * The product must function as a next generation firewall by providing the following services and capabilities: Intrusion Prevention, Detection, malware/file integrity scanning, sandboxing, and threat intelligence feeds.
   * Firewall should be able to detect command & control Centers and automatically block them based on Intelligence feeds
3. **Next Generation Firewall Security Features**
   * The firewall must support comprehensive threat prevention security features including IPS, Antivirus, Anti Spyware, Anti Bot, DoS/DDOS etc from day one.
   * The proposed firewall must have integrated Intrusion Prevention Systems - IPS with ability to prevent SBI CAP SECs critical trading applications and digital asset against minimum 15,000 + vulnerability exploit attempts.
   * The firewall must detect & prevent minimum 12,000 + CVE exploit attempts to safeguard SBI CAP SEC environment. OEM to provide full list of IPS signatures along with CVE numbers.
   * The proposed firewall must support attack recognition for IPv6 traffic the same way it does for IPv4
   * The proposed solution must support different actions in the policy such as deny, drop, reset client/server
   * The proposed solution must have functionality of Geo Protection to Block the traffic country wise per policy and per applications as per customer requirement and shouldn’t be a global parameter
   * The proposed solution must have an option to create custom signatures. It should also support importing of rules automatically from other open source solutions like, SNORT or Suricata, etc.
   * The Firewall must support ability to decrypt & inspect TLS 1.3 traffic
   * The NGFW must support QoS marking and reclassification based on source/destination IP, port, protocol, user, applications, security zone etc.
   * The proposed firewall should have the ability to create custom application signatures and categories directly on firewall without the need of any third-party tool or technical support. Also the device should have capability to provide detailed information about dependent applications to securely enable an application
   * All the proposed threat prevention functions like IPS/vulnerability protection, Antivirus, C&C protection etc should work in isolated air gapped environment without any need to connect with Internet.
   * Firewall should have specific DNS Security Signature Categories of domains based on the risk that these domains pose to SBI Cap Sec. SBI CAP SEC should be able to block DNS based attacks for include C2 (encompasses DGA and DNS tunnelling), malware, DDNS, newly registered domains, and phishing
   * Firewall should have simple policy formation for dynamic action to block domain generation algorithms or sinkhole DNS queries.
   * The NGFW must have ability to detect credential theft attempts on SBI CAP SEC employees. In such cases, NGFW must block the traffic & reset the session immediately. NGFW must provide ability to enable / disable it as per SBI CAP SEC requirement.
   * The NGFW Anti-virus & anti Malware must able to analyse & prevent malicious file, virus, malware, ransomware etc traversing on following protocols: HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP, and SMB.
   * The NGFW must be able to support decryption of the following protocols: SSL, SSH
4. **Next Generation Firewall Threat Intelligence Features**
   * Solution must have the option to provide all threat intel feeds to other devices
   * Solution must take decision based on URL reputation
   * Solution must take decision based on DNS reputation
   * Solution must block based on malicious file attachment (i.e: doc, docx, xls, xlsx, pdf, etc.)
   * Solution Security intelligence must come from multiple sources
   * Solution Security intelligence must come from different product types
   * Solution Must integrate with 3rd party security intelligence sources
5. **Next Generation Firewall Management Features**
   * The firewall must support on device management for config changes in case of emergency & non availability of centralized management.
   * The firewall must have CLI, SSH & HTTPS based on device management
   * The firewall must have full-fledged on device management allowing all possible config to be performed directly on the firewall.
   * The firewall must have comprehensive logging, log analyser, log correlation, search, filter, unified logs available directly on firewall or on a separate logging server
   * Solution will be preferred if it can correlate between config change & CPU / Resource utilization to make it easy to identify which config change has caused increased in CPU utilization
   * The management solution must provide Executive Dashboard -Highlight Customizable Dashboard to provide quick insight to Applications / Users / Content / Files / Threat / Top Country / Top Rule Usage
   * Proposed NGFW solution should have separate control and data plane with their own resources like CPU, Memory & Storage to ensure continuous & uninterrupted access without any lag or delay to NGFW irrespective load & CPU utilization. In an unplanned & unforeseen event, Security admin must able to login to NGFW, collect logs, make necessary changes and commit changes in to NGFW
   * In case of wrong config push / human error resulting in firewall isolation & lost communication with central management, Firewall must auto restore last known good config and restore communication with Central management without any manual intervention.
   * The administrator must be able to import the NGFW configuration into the central management platform
   * The administrator must be able to view report on the CPU usage for management activities and CPU usage for other activities.
   * The firewall must have the ability to manage firewall policy even if management server is unavailable
   * Firewall must identify the amount of TLS traffic, non-TLS traffic, decrypted traffic, and non-decrypted TLS traffic, number of ssl sessions in a separate section for better visibility and troubleshooting. Firewall should also show decryption failure (if any) reason data in GUI for troubleshooting
   * The management solution must have the native capability to optimize the security rule base and offer steps to create application based rules
   * The proposed solution must allow single policy rule creation for application control, user based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS and scheduling at single place within a single rule and not at multiple locations. There must not be different places and options to define policy rules based on these parameters.

1. **Reporting:**

* Provide user-friendly management and effective reporting capabilities with useful user dashboards.
* Solution should provide advanced reporting tool
* Centralized logging and reporting capabilities for security events and network activity.
* Customizable dashboards and alerting features.
* Reporting tool must have visualization dashboard
* Reporting tool should have investigation capability
* Solution must have a visualized root cause analysis reporting capability
* The NGFW must support the ability to create custom reports directly from the WebGUI of the NGFW or reporting tool.
* Solution should provide Geo-IP maps (geolocation)
* Solution should provide user capability to create- modify dashboards and locked to his profile
* Solution must provide long term trend analysis of events in the reports.
* Solution must have health check reports
* Solution should provide user capability to create- modify dashboards and locked to his profile
* Ability to export logs to third party solution (SIEM)
* Ability to export reports and schedule based on set criteria (Example, CPU usage higher than a set threshold to automatically alert).

1. **Next Generation Firewall Integration :** 
   * Integration with SIEM, SOAR, and EMC storage to analyze and parse security events, activity events / logs generated.
   * Integration with ISE, active directory to import OU & groups for administration task and management.
   * Integration with mail server for email alerts and reports.
   * Support for exporting logs to SIEM (Security Information and Event Management) systems.
   * Integration with existing network infrastructure, including routing protocols and other security appliances.
   * Support of APIs and scripting support for automation.
2. **SLA and KPI :** 
   * Bidder must provide support services, including response times and escalation procedures.
   * Bidder must provide availability of software updates and patches.
   * Bidder must provide hardware warranty and replacement policies.
   * Bidder must provide **3 years warranty** and support for the overall solution.
   * Vendor must provide support for 3 years that start with the acceptance of the solution
   * Bidder must provide support services, including response times and escalation procedures.
   * Solution should run on the latest version during acceptance, and throughout the 3 years of support the latest version should be provided and installed as part of the support agreement
   * Bidder must attach escalation chart email address and helpdesk number to contact in case of a breach or support.
   * Bidder support must be backed up with vendor support
   * Bidder must provide on-site support and/or remote support: 24 hours a day, 7 days a week and a maximum response time based on the below SLA :

|  |  |  |
| --- | --- | --- |
| * + Crucial Priority (severity A) (system down, threat or malware) | * + Response immediate by phone or email | * + Maximum 1-2 hours response time 24 hours -7 days a week and maximum 1 day for resolution |
| * + Average Priority (system urgent or severity B) | * + Response back phone or email within 2 -3 hours | * + Maximum 5-6 hours response time 24 hours – 7 days a week , max 5 days for resolution |
| * + Not critical (system is running and no threat) | * + Response back phone or email within 4-5 hours. | * + Response by email or phone, site visit upon our request, max 2 weeks for resolution |

1. **Project Delivery & Deployment:** 
   * MIC2 expects the bidder to clearly outline and detail the expected delivery, installation, and integration and validation times.
   * Detailed project implementation plan (PIP), mentioning each milestone
   * Delivery of the project should adopt Agile methodology
   * Vendor must provide and share previous implementations of such projects
   * Replacement of existing solution and installation of the new solution within 3 months.
   * Vendor must provide reference of large-scale implementations for similar solutions
   * Vendor is responsible for end-to-end integration including hardware racking, cabling, and power connectivity
   * Bidder must submit a minimum 5 years roadmap for the proposed solution.
2. **Documentation:** 
   * Bidder must provide product description
   * Installation Guide
   * User Manual: Detailed and complete user manual for the solution that contain all the parameters and configurations.
   * System features along with provided licenses and explanation of the license model.
   * Acceptance test plan
   * Bidder must provide Low level design document (LLD) detailing the scope of this project.
   * Bidder must provide Network Implementation plan document detailing the implementation of this project
   * Bidder must provide Network ready for use document (NRFU) detailing the acceptance tests.
3. **Supplier Experience and References:** 
   * Vendor must provide in table format references for similar deployments
   * Vendor must provide reference and details about deployment in telecom operators/ or similar environment
   * Vendor should have deployment in more than 5 similar environments.
4. **Professional Services :**

* Bidder must install and replace existing solution.
  + Bidder must submit a project implementation plan for the whole project lifecycle.
  + Bidder shall provide a detailed profile for the company and summary of the executed projects of similar nature inside and outside the telco environment.
  + Onsite engineer to have full knowledge about the solution to be available for 6 months after Final acceptance.
  + Onsite engineer must handle all the needed tasks
  + Onsite engineer must perform knowledge-transfer to the team
  + The bidder needs to provide all the needed network cabling and network devices confirming and abiding to the following guidelines:
    - All cabling should be terminated on Patch Panels.
    - Needed patch cords (Fiber and copper should be provided).
    - Cabling quality report should be provided for each link.
    - All cables should be labeled.
    - Cable organizer should be provided

1. **Training :**

* Documentation and Training:
  + Comprehensive user manuals and configuration guides.
  + Availability of training programs and resources for IT staff.
* Training shall cover all areas of the solution.
* Bidder shall provide the needed training material in soft and hard copy.
* Provide actual hands-on session on the real system similar to what Touch will be facing in the Live environment.
* Bidder shall provide advanced technical training for 5 Engineers
* Bidder should include travel expenses
* Bidder should include accommodation expenses

1. **Dimensioning and Capacity:**In the current setup, MIC2 operates three Internet Gateway (IGW) sites. The plan is to install six firewalls in a redundant configuration. The expected dimensioning figures, which will be reviewed when the RFP is launched, are as follows:

* 3 million Connections in Site 1, 2 million connections in site 2 and 1 million connections in site 3
* 23 Gbps in site 1, 17Gbps in site 2 and 8Gbps in site 3
* Appliances will be connected redundantly as active standby in each site
* Type of Connections: Copper 1Gbps, and Firber (1G, 10 G)\

1. **Accessories :**

* 2 Routers with below specifications:
  + Routing Throughput: Minimum 10 Gbps.
  + Support for at least 1,000 routing entries.
  + Redundancy and failover capabilities.
  + IPv6 support.
  + QoS (Quality of Service) capabilities.
  + Number and Types of Ports:
  + WAN Interfaces: 2 x 10 Gigabit Ethernet, 2 x Gigabit Ethernet
  + LAN Interfaces: 8 x Gigabit Ethernet
  + Management Interfaces: 1 x Out-of-Band Management Port
  + Expansion Slots: 2 x Flexible Interface Cards (FIC) for future scalability
* 2 switches with the below specifications:
  + 24 copper interfaces (RJ-45) with auto-negotiation.
  + 8 SFP+ (10-Gigabit Ethernet) fiber module slots.
  + Layer 2 and Layer 3 functionality.
  + Minimum switching capacity of 128 Gbps.
  + Support for at least 32,000 MAC addresses.
  + VLAN support with a minimum of 512 VLANs.
  + Advanced Quality of Service (QoS) features.
  + Each switch should have 24 copper interfaces (10/100/1000 Mbps) with auto-negotiation capabilities.
  + Compliance with IEEE 802.3 and 802.3ab standards.
  + Fiber Modules
  + Number of Fiber Module Slots:
  + Each switch should have 8 SFP fiber module slots for high-speed fiber connectivity.
  + Supported Fiber Module Types:
  + Compatibility with standard SFP and SFP+ modules.
  + Support for multi-mode and single-mode fiber modules.
* Compatible SFPs to be provided as part of the solution:
  + At least 16

1. **Killing Factors :**

* The proposed firewall must provide NGFW functionality from day one. All required license must be provided from day one.
* Support for IPSec encryption over GRE tunnels
* The appliance must have 2 x redundant power supplies from day one. Power supplies must be hot swappable
* Bidder must provide on-site and/or remote support based on the requested service level agreement.
* Bidder must have the needed skills, certifications and existing professional resources to deploy the solution.

1. **Bill of Quantity :**

* Bidder must provide pricing summary for the next 3 years.
* Bidder must provide detailed unbilled BoQ for the technical evaluation

|  |  |
| --- | --- |
| **Description** | **Quantity** |
| Firewall 3 locations | 6 |
| Advanced training seats | 5 |
| 3 years Warranty and support | 3 |
| Routers | 2 |
| Switches | 2 |
| SFP | 16 |
| Certified Onsite engineer for 6 months | 1 |

1. **Pricing :**

* Break down of all the prices must be provided
* Unbilled price list to be provided in the technical offer.