Solution specification

Below is the list of specifications and capabilities that should be provided by the proposed Solution unless stated otherwise, provide details of the proposed features and specifications where needed.

- **NOTE: Below specifications are the minimum accepted spec. Equivalent or higher specs are accepted as well**

Minimum Specification for NGFW		
Performance		**Comply**
New Session/sec	Min 65,000	
Firewall throughput	10,000Mbps	
Threat protection throughput	Min 850 Mbps	
Next generation firewall throughput	2.4 Gbps	
Concurrent connections	4.900,000	
IPsec throughput	Min 4.8 Gbps	
Mounting	1U rackmount OR Desktop	
Hardware		
Integrated Storage Capacity	Min 64GB Capacity SSD	
Network Interfaces		

Integrated Port	8 x 1Gbps 2x 10 GE SFP+ 1 RG45 Mgmt	
Other port	USB, Console port	
General		
The proposed system should be able to support the following security features on the same box: ○ State full Firewall ○ IPS ○ Web and Content Filtering (URL filtering) ○ Application Control Settings ○ Advanced Malware Protection ○ Threat protection ○ IPsec VPN ○ SSL offloading and forward proxy ○ Deep packet inspection (DPI) and file blocking		
NGFW configuration shall be based on the best practices recommended configuration by the vendor to ensure the highest NGFW performance		
Platform should be optimized for layer 7 application level content processing		
IPsec VPN (using SSL or TLS)		
Remote Access VPN (IPsec and SSL or TLS)		
High Availability: Active/Active and Active/Passive		
SSL Decryption for all application traffic, and ability to block any unknown encryption standard		
Ability to block any detected unknown application		

شادي منيزل
مدير مديرية تكنولوجيا المعلومات

The proposed firewall shall support 802.1Q virtual Local Area Networks (VLANs) tagging (in tap, transparent, layer 2 and layer 3)	
The proposed firewall shall support policy based forwarding based on zone, source or destination address, source or destination port, application and Active Directory (AD)/ Lightweight Directory Access Protocol (LDAP) Remote Authentication Dial in User Service (RADIUS) user or user group	
Should support network traffic classification which identifies applications across all port irrespective of port/protocol tactic	
The proposed firewall shall support in-box logging and reporting mechanism The following report output formats must be supported: HTML, PDF, CSV and others	
should integrate user-identification allowing Active Directory groups and specific user to access a particular application while denying others	
Firewall should support Voice based protocols (H.323, SIP, SCCP, MGCP etc.)	
Firewall should support Bandwidth customization / QoS Based on users, application category, and Web category	
The firewall should be capable of identifying and optionally preventing transfer of various files (i.e. MS Office, PDF etc.) via identified applications (i.e. P2P, IM, SMB etc.)	
The Firewall should take decision based on different matching parameters not based on layer 4 parameters. It should be based on applications, URL categories, IP address, security zones, username/group (s)	
Policies based on port-and-protocol and Application as the match criteria (application decision should not be done separately)	
Policy-based control by user, group or IP address (user control should be flexible to support a single user not only AD groups)	

Support Geographical Location policy in a security rule, where connections going to a country or countries can be blocked	
OS and Management Specs	
• The device must have the latest software version	
• The OS software and configuration shall be easily backed up and restored Support Auto Backup to Email, FTP and Cloud method •	
• Administration and System Management: web-based configuration or CLI, Role-based access control, Logging/Monitoring Facilities	
Authentication	
• Authentication : XAUTH/RADIUS, AD,SSO, LDAP, Terminal Services, Internal user Database	
• Supports automatic security updates directly over a secure connection (i.e no dependency of any intermediate device)	
Anti-Spyware	
• Botnets detection/blocking	
• Malware Site Blocking	
• DNS-based botnet signatures	
• DNS Sink holing for malicious domains	
URL-Filtering	
• URL-filtering on the same NGFW box	
• Customizable allow and block lists	
• Customizable categories	
• Supports URL reputation-based filtering	
• User identification: should support the following authentication services for user-identification: o Active Directory, LDAP, Radius, Kerberos, Client Certificate o Populate all logs with user identity (traffic, IPS, URL, Data, etc.)	

○ Logged user-identification correlated in real-time Active Directory		
IPS Requirement		
• The IPS detection methodologies Signature based detection		
• IPS Signatures can be updated in different ways: manually and automatically		
Warranty		
warranty: including hardware, software update (minor or major), licenses and hands labor or any services The warranty starts from date of preliminary acceptance	3 years	
Others		
Winning bidder must provide all necessary requirements (Cables, Connectors, mount kit, etc.)		
The Bidder must have at least 2 qualified and trained engineer/technicians		
The bidder should have fully understood the Scope of Work.		

2. Scope of work:

Important Notes:

- There are certain activities to be performed and deliverables to be provided by winning bidder during execution of the Project. More detailed information on each of them is given in the next paragraphs.
- The winning bidder shall provide such Hardware, software, professional services, deliverables and support. The cost of these requirements or activities should be included in the fixed lump sum price submitted by the winning bidder.
- Final deliverables submitted by the winning bidder should be attached to an original official letter properly bounded, stamped and signed by the winning bidder as shall be defined and approved by ……..

شادي منيزل
مدير مديرية تكنولوجيا المعلومات

- The duration time for the project will be 150 calendar days starting from the commencement date. In addition to 36 months support and maintenance from the mother company.

Note: that the winning bidder should provide any additional requirements needed for the proper delivering of the project and its cost should be included in the price submitted by the bidder.

3.1 Component 1: Firewall installation, configuration and training

Winning Bidder Activities

For the proper completion of the Project, the winning bidder is required to perform the activities mentioned below. The winning bidder should provide any additional related activities needed for the proper fulfillment of the project and its cost should be included in the price submitted by the bidder.

- Procure, supply, deliver, install, configure, integrate, tune, and test the hardware and software listed in Section 5: BoQ, along with related software functionalities/features in section 2.
- Provide High- and Low-Level Design Documents (HLD/LLD) for the Firewall.
- Provide all needed equipment's including (cables, transceivers). Any equipment needed to make the Firewall work properly should be provided by the winning bidder even if not listed in section 5: BoQ
- Configure and hardening the firewall based on the Vendor best practices
- Do a proper Network segmentation
- Enable and test all the firewall features
- Developing firewall Management policy and service publishing policy as part of engagement to assure secure operation deployment approach that includes designing, configuring, testing, and migrating. This might include:
    - Firewall Change Management policy
    - Firewall Rules access request policy
    - Firewall Publishing Service policy
    - Firewall rules review and Audit policy
    - Firewall monitoring policy
- Provide Support for 36 months for all provided items listed in the project scope of work, starting from the date of preliminary acceptance.
- The Bidder shall provide complete documentation covering all aspects of the project, including but not limited to: user manuals, operations manual and configuration manuals and as built document.

- Provide the necessary licenses for the firewall, which are valid for 3 years starting from the date of activate the license after receiving and accepting the Hardware.
- Provide Technical support during the official working hours of the institution or outside the official working hours for emergency cases after the approval of the concerned department in the institution and as per the SLA in Annex 6.3.
- Provide onsite Training course for the Firewall covering administration and analysis aspects of the Firewall for two engineers from DPA
- Handle All Project Management tasks and prepare necessary work plans to ensure the successful project delivery.
- The winning bidder after finishing the installation and configuration of the Firewall should check all the policies setting on the new firewalls, enhance them if needed and make sure they follow the Vendor security best practice