Edge NGFW Specifications

General Requirements	Comply (Yes/No)
1- NGFW Must support: • Embedded machine learning (ML) in the core of the firewalls to provide inline signature less attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts. • Cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW. • Behavioral analysis to detect Internet of Things (IoT) devices and make policy recommendations; cloud-delivered and natively integrated service on the NGFW. • Automated policy recommendations that save time and reduce the chance of human error. • Visibility and the ability to restrict applications using non-standard ports in a single security policy rule • Visibility and control over all the SaaS apps in use and their shadow IT risks and can intelligently keep up with the unstoppable SaaS growth. • Automatically protect against tens of millions of malicious domains identified with real-time analysis and continuously growing global threat intelligence.	
2- The proposed firewall solution must be two firewalls for high availability purposes: **Firewall box include:** - Firewall software - Windows or Linux-based server (including thehardware). - The proposed server must be able to have minimum: 4x SFP+ (10 Gbps) - The firewall box components shall be Rack Mountable -The proposed software solution should have the minimum 4xvCPU NGFW	
3- NGFW must be equipped with the required licenses to enable the following advanced security capabilities: • Advanced Threat Prevention (NGIPS, Anti-Malware and Anti-Virus) • Advanced Mobility & Host Information Profiling • Vulnerability protection • Inline ML Anti-virus protection • Advanced URL Filtering & Credential Theft Protection • ML-based sandboxing • DNS Security	
• Support type and period = 24/7 (3) years support	
• Minimum quantity of SR 10Gb optical transceiver = 4	
• The NGFW must support context-based policies to adopt a Zero Trust Model.	
• The NGFW must support explicit proxy and transparent proxy method	
• The NGFW must support the ability to enforce Multi-Factor Authentication to internal applications	
• The advanced malware analysis (malware sandboxing) solution must have macOS and Linux executable scanning by default.	
• The NGFW must be able to acquire User Identities from LDAP, Captive Portal, VPN, NACs (XML or API), Syslog, Terminal Services, XFF Headers, Server Monitoring, AND client probing	
• The NGFW must offer full and unfettered open API Support without a paywall (subscription) to access Dev toolkit, Tools and Scripts and samples.	
• The NGFW must support the ability to dynamically and automatically regroup user/s based on security events relating to that user. No manual response is needed	
• The Sandbox must detect and prevent zero-day malware using dynamic/static analysis and Intelligent Run-time Memory Analysis to detect highly evasive threats and create protections to block malware.	
• The NGFW must provide scalable clustering and multi-DC clustering.	
• The NGFW must be able to enable any new security offering without impacting the performance of the traffic flowing through it	
• The NGFW must support App-ID capability to get visibility into the applications on the network and learn how they work their behavioral characteristics and their relative risk.	

4- Gartner and Third-Party Testing:	
• Firewall vendor should be in the Leader's Quadrant of the Gartner Report for Enterprise Firewalls	
• Leader in SecureIQLab for Next-Generation Firewall	
5- Performance Specifications:	
• Active/Standby & Active/Active High availability support	
• Minimum of 4 Gbps of Layer 7 Application Mix firewall throughput	
• Minimum of 3 Gbps of Threat Prevention Application Mix, throughput with services of IPS, Antivirus, Antispyware, DNS Protection, Advanced Anti-Malware, Data Filtering/DLP Enforcement, URL, DNS protection, and File Blocking enabled all at the same time	
• Minimum of 1.5 Gbps of IPSEC throughput	
• Minimum of 800K concurrent sessions	
• Minimum of 30K New sessions per second	
• 120 GB SSD Storage	
6- Firewall Security Policy Control features:	
• Security policies control based on Layer 7 applications irrelevant to the TCP/UDP port number (non-profile-based application control)	
• Management of unknown traffic (unidentified applications) through security policies	
• Built-in Security Optimizer in the Firewall User Interface to convert legacy Layer 4 Port-based security policies to Next Generation Layer 7 application-based security policies by automatically detecting applications utilization of each security policy rule and hence allowing the admin to match the correct applications for each legacy rule	
• Built-in Policy Match Testing capability in the Firewall User Interface including the support of field Criteria like Layer 7 application and Active Directory User ID	
• Schedule & time-based security policy control	
• Rule use tracking includes a timestamp for the most recent rule match, a timestamp for the first rule match, and a rule hit counter.	
7- Firewall Decryption & Tunnel Inspection features:	
• SSL decryption policies covering SSL encapsulated protocols such as HTTP(S), IMAP(S), POP3(S), SMTP(S), FTP(S), and Secure Shell (SSH) traffic	
• SSL decryption mirroring and SSL decryption broker for inline inspection	
• SSL decryption with full TLS 1.3 handling, not just certificate	
• SSH decryption to detect SSH tunneling	
• Decryption policy control based on Active Directory users, groups, IP addresses, URL categories, or countries	
• Integration with Hardware Security Module (HSM) like Thales nShield and SafeNet	
• SSL session blocking profile for sessions with untrusted issuers, expired certificates, client-based certificates, unsupported SSL versions, and unsupported SSL cipher suites	
• VxLAN and GRE tunnel content inspection	
8- Firewall Threat Prevention (IPS, Credential Theft Prevention, AV, and Anti-Spyware) features:	
Vulnerability Protection (IPS) against: • Block viruses, spyware, malware and network worms and vulnerability exploits within content of application content • File blocking by type and application • Data Leakage Prevention (scan for keywords and credit card numbers) • Anonymous Botnet Detection • Blocks application vulnerabilities • Block known network and application-layer vulnerability exploits • Block buffer overflow attacks	
9- Anti-Spyware protection against: • Per-application scanning options – AntiSpyware • Per-category scanning options • Phone-home detection/blocking • Malware site blocking • DNS-based botnet signatures	

• DNS Sink holing for Malicious and fast-flux domains • Per-application antivirus scanning options	
• Anti-Virus support following applications: HTTP, HTTPS, FTP, SMB (V3 & V3.1), SMTP, IMAP, & POP3	
• Creation of custom user-defined IPS signatures (payload based)	
• Creation of custom user-defined Anti-Spyware/Command & Control signatures (payload based)	
• Scheduled External Dynamic IP Address, Domain DNS and URL list import	
• Threat packet capture for up to 50 packets from IPS, Ani-Spyware and Anti-Malware engines	
• Selection between allow, alert, reset client, reset server & client & server, block for detected threats	
• File blocking based on file type, application, file direction (upload/download), user id, URL category or country	
• DLP enforcement & data match support through Predefined Patterns, Regular Expressions and File Properties	
• Zone based Flood, Reconnaissance/scan, and Packet based attack protection support	
• Policy based DoS protection against flooding of new sessions	
• Packet Buffer Protection to protect firewall buffers from single source DoS attacks	
10- Firewall User Identification, and Authentication features:	
• Must support AD User Identification, and Authentication • Identifying User AD ID by integrating with Active Directory through WinRM and WMI • Identifying User AD ID by integrating with Exchange through WinRM and WMI • Identifying User AD ID by running as syslog receiver • Identifying User AD ID by Integrating through XML APIs with Third Party solutions • Identifying User AD ID through captive portal • Identifying User AD ID in terminal servers • Identifying User AD ID by running an Agent at user machines	
• Must natively support cloud identity sources to facilitate transition from on-prem IdP and move directly to hybrid or cloud IdPs	
• Sharing "IP Address to User ID" mapping with centralized management and other firewalls	
• The NGFW must send a multi-factor authentication request via the existing MFA vendor to secure access to critical Apps.	
• Direct Multi-Factor Authentication integration with RSA, Okta, PingID and Duo	
• Single Sign-on authentication support	
• Enforcing user authentication including single sign-on and multi-factor authentication through authentication policies based on user id, server name/Ip address, URL, and URL category	
• SAML 2.0, RADIUS, LDAP, TACACS+, and Kerberos	
11- Firewall Remote VPN & Advanced URL Filtering features:	
• Split tunneling based on IP addresses, domains and applications for remote user VPN	
• VPN Authentication override using cookies	
• Exclusion of video traffic from main remote user VPN tunnel	
• Trusted root certificates push to remote VPN user devices to help enable features: SSL decryptions	
• VPN Gateway selection criteria based on source user id, region, OS and ip address and Downloading the VPN agent software from firewall VPN portal page	
12- Advanced URL Filtering must support the following: • Real-time URL analysis per request • Customizable allow and block lists • Customizable block page & coaching pages • Custom categories • Database located locally on the device • When a user visits a URL designated as risky, the firewall submits the URL to the advanced URL filtering service for machine learning analysis and searches DB for the site's category. • Analyze URLs and display the category real-time-detection and threat type in the logs.	
13- Firewall Advanced Mobility & Host Information Profiling features:	
• Remote user VPN agent for Windows, MAC, Linux, Chrome, IOS, and Android	
• App-Level VPN for IOS and Android devices	

• Portal based & clientless SSL VPN support	
• Multi-Factor Authentication support	
• Host Info Check by collecting & reporting device information & attributes back to the firewall	
• Host Info Profiling attributes based on Managed/Unmanaged certificates status, OS type, Client version, Host name, Host ID, Serial number, Mobile model, Phone number, Root/Jailbroken status, Passcode presence, Installed Applications, Patch presence & status, Firewall agent presence & status, Antimalware agent presence & status, Disk backup agent presence & status, Disk encryption agent presence & status, DLP agent presence & status, process list presence & status, registry key presence & status and list presence & status	
• Security policies control & decision based on Device/Host Information Profiles	
• Distribution of Host Information Profiles directly between firewalls	
• Integrating with Third Party MDM solutions like AirWatch or MobileIron to get Host Information Attributes	
14- Firewall Networking features:	
• IP version 4 and version 6 support	
• Layer 1 Deployment Mode (Virtual Wire Mode)	
• Layer 2 Deployment Mode (Bridge Mode)	
• Layer 3 Deployment Mode (Routed Mode)	
• Monitoring Deployment Mode (Tap Mode)	
• Network address translation (NAT) using static IP, dynamic IP, dynamic IP and port (PAT)	
• DNS Proxy support	
• LLDP support	
• RIPv2, OSPFv2, OSPFv3, BGP & ECMP support	
• PIM-SM, PIM-SSM, IGMPv1, IGMPv2, and IGMPv3 multicast support	
• Equal Cost Multi-Path (ECMP) Support	
• Bidirectional Forwarding Detection (BFD) support	
• LACP and Aggregate interfaces (802.3ad) support	
• Quality of Service Traffic Shaping Policy support (priority, guaranteed, maximum) based on IP Addressing, Layer 7 Application, User ID, Tunnel, URL Category, and DSCP classification	
• Policy based forwarding support	
• High-Availability link & path monitoring support	
15- Firewall Built-in Management, Logging & Reporting features:	
Must support: • Command Line Interface (CLI) • Built-in web interface, non-Java base (GUI) • XML Rest API based management support • Commit based configuration management • Config audit support by comparing running config against candidate config • Built-in web interface, non-Java base (GUI) • XML Rest API based management support • Commit based configuration management • Config audit support by comparing running config against candidate config	
• Automated security action based on any firewall log fields. For example, a firewall can automatically block a specific IP address/user and can automatically initiate some API calls to a ticketing system to create a help desk ticket if one firewall threat log reports one host as being infected/compromised	
• Interactive graphical summaries around the applications, users, URLs, threats, and content traversing the network	
• Customized graph-based network activity for applications using non-standard ports	
• Customized graph-based blocked activities including blocked applications activity, blocked Users activity, blocked Content activity, blocked threats activity, and security policies blocking activity	
• Customized graph-based tunnel activities including tunnel ID/Tag, tunnel application usage, tunnel user activity, and tunnel IP source/destination activity	
16- NGFW Must support:	

• Aggregated logging and event correlation • Custom reporting support with the ability to generate a report per user, ad group, application, network protocol etc. • Export reports to PDF and ability to send reports by email • Dedicated SaaS application report (like office365 and others) • Dedicated log set for traffic, threats, URL filtering, host info profile, data filtering, file control, user id mapping, authentication, configuration, system and alarms • Scheduled log exports • Policy rules to support dedicated description, tagging, and audit fields with the capability to enforce these fields • Integration with VMware vCenter, VMware ESXi, AWS VPC, and google Cloud Engine for VM information fetching • Custom admin roles • Customizable application blocking, URL blocking, file blocking & malware html user response pages • Syslog, Email, Netflow & Authenticated NTP • SNMP and SNMP Traps	
17- IoT device Visibility, Risk Management, Security anomaly detection	
• The proposed NGFW must support IoT subscription that support an ML-based approach to discover unmanaged devices, detect behavioral anomalies, recommend policy based on risk, and automate enforcement without the need for additional sensors or infrastructure.	
• Prevent Known and Unknown Threats	
• Implement Trust Policies with Automated Risk-Based Recommendations	
• Prioritize Risk with Continuous Vulnerability Assessments	
• Must obtain SOC 2 Type II certification	
• Must support Native playbook-driven integrations with third-party systems such as ITAM/ITSM, NAC, and SIEM	
• Must be able to identify Domain Generating Algorithms to protect against data exfiltration	
18- Sandbox Malware and Day-Zero Protection:	
• Prevent Unknown Threats at the Firewall Level with Inline Machine Learning	
• Using content signatures for prevention instead of hashes	
• Identify threats in all traffic across hundreds of applications, including web traffic; email protocols like SMTP, IMAP, and POP; and file-sharing protocols like SMB and FTP, regardless of ports or encryption.	
• Monitor all network activity produced by a suspicious file, including backdoor creation, downloading of next-stage malware, visiting low-reputation domains, and network reconnaissance.	
• Must support Fileless attack and script detection such as JScript and PowerShell	
19- NGFW Must Prevent Highly Evasive Malware using the following key features: • Stealthy Observation • Automated Unpacking • Dependency Emulation • Intelligent Runtime Memory Analysis • Malware Family Fingerprinting	
20- NGFW Must support the following file type: • Android application package • Adobe Flash • Java Archive • Microsoft Office • Portable executable • Portable Document Format • Mac OS X • Archive • Linux • BAT, JS, VBS, PS1, ETC scripts	
21- DNS Security	
• Support for stockpile domain and Ultra Slow DNS tunnelling detection	

- Support for DNS-over-DoH and DNS-over-TLS	
- Support for DNS Infiltration, Anomaly and Wildcard DNS detection	
- Support for Ad Tracking, phishing and malicious NRD domain detection	
- Support for malware compromised DNS (domain shadowing and newly observed hostnames) and newly observed domain detection.	
- Support for strategically aged and fast-flux domain detection	
- Support for Dangling DNS and DNS Rebinding Detection.	
- Support for 'parked' and grayware domain detection.	
- Support for proxy avoidance and anonymizer detection.	
- Support for NXNS Attack and Dictionary DGA domain detection.	
- Support for dynamic DNS (DDNS) and newly registered domain detection.	

- **الشروط الخاصة:**

1- أن تكون مدة تجديد التراخيص **ثلاث سنوات شمسية** اعتباراً من تاريخ التشغيل للجهاز ولجميع البنود أعلاه.

2- تقديم الدعم الفني (في الموقع أو عن بعد) حسب الحاجة وحسب الطلب لمدة ثلاث سنوات من تاريخ التشغيل.

3- أن يتم تقديم التدريب الفني والتقني داخل الجامعة وخارجها على جهاز جدار الحماية لمهندسي الشبكات في مركز الحاسوب وعددهم 3 مهندسين.

4- تقوم الشركة الموردة بتوريد وتركيب وتشغيل جهاز جدار الحماية الجديد، ونقل جميع الاعدادات الموجودة حالياً من جهاز جدار الحماية الحالي الى جهاز جدار الحماية الجديد.