Request for Proposal (RFP)

Project Title: NextGen Firewall Procurement for KFON Head Office, 2nd Floor, B Block, Jeevan Prakash, Pattom, TVM

1. **Introduction**: KFON Head Office at LIC Pattom, Trivandrum, intends to procure a NextGen Firewall (NGFW) solution to enhance its network security infrastructure. This Request for Proposal (RFP) outlines the specifications and requirements for the NGFW solution.

2. **General Requirements:**

- The Firewall must be appliance-based, rack-mountable, and equipped with internal redundant power supplies from inception.
- The proposed vendor must be positioned as a Leader/Challenger in the Gartner Magic Quadrant for Enterprise Network Firewall.
- NGFW must feature a built-in GUI and CLI for real-time policy management and troubleshooting.
- Secure SD-WAN capabilities with support for advanced routing protocols such as BGP are essential.
- SD-WAN functionality should include link failover between various connections, load balancing based on multiple parameters, and configurable SLA settings.
- Central management solution should facilitate centralized management of SD-WAN links with clear dashboard visualization.
- Support for multicast routing, firewalling, and policy routing is required.
- Identity-based routing option for traffic routing based on authentication rather than IP address.
- Integrated Traffic Shaping functionality with the option to configure it within firewall policies or separately.
- Built-in GUI should display logical network topology and provide security recommendations.

3. **Performance Parameters:**

- Minimum 2.5 Gbps IPS throughput and 1.5 Gbps NGFW throughput on real-world/enterprise mix traffic.
- Minimum 900 Mbps threat protection throughput.
- Support for 8 Gbps IPSec VPN throughput with 1500 tunnels.
- Minimum 1,500,000 concurrent connections and 50,000 new sessions per second.
- Minimum of 12 interfaces including auto-sensing 10/100/1000 capability, 2 Gigabit SFP ports, and 2 10-GbE SFP+ interfaces.

4. **Firewall Features:**

- Single firewall policy for all features including IPS, application control, URL filtering, antivirus, SSL inspection, logging, and NAT.
- Support for Zoning and User-based authentication.

- Ability to configure firewall policies directly from the NGFW GUI in emergency situations.
- Support for various NAT types including NAT46, NAT66, NAT64, and multicast NAT.
- Geo-based IP address blocking, DNS translation, and FQDN-based policies.
- Option for packet capture within firewall policies for troubleshooting.
- Configurable option to quarantine attack-generating source addresses.

5. **Virtualization:**

- Support for virtualization with licenses for a minimum of 5 Virtual Firewalls.
- Virtualization for all features including IPS, application control, antivirus, URL filtering, SSL inspection, VPNs, and user authentication.
- Seamless virtualization without downtime or reboot, with configurable resource limits for each virtualized system.

6. **VPN Features:**

- Built-in support for IPSec VPN and SSL VPN without user license restrictions.
- Support for gateway-to-gateway and gateway-to-client VPN configurations.
- Route-based IPSec VPN with SD-WAN support.
- Support for SHA-1, SHA-2, and various DH groups.
- Integration with local AD or RADIUS server for 2-factor authentication.

7. **Intrusion Prevention System:**

- Signature-based detection with real-time updates.
- Anomaly-based detection with threshold configurations.
- Configurable IPS signatures with fail-open capability.
- Protection against DOS and DDOS attacks with customizable rate-based protection.

8. **Antivirus:**

- Integrated antivirus solution with configurable actions.
- Blocking, allowing, or monitoring based on AV signatures and file blocking.
- Configurable thresholds for oversize file blocking.

9. **Web Content Filtering:**

- Integrated solution without external hardware.
- Enable/disable web filtering per firewall policy or user groups.
- Features include blocking web plug-ins, URL blocking, keyword blocking, and exempt lists.
- Real-time database updates based on local Sandboxing solutions.

10. **Application Control:**

- Detection, logging, and action against network traffic based on over 4000 application signatures.

- Manual or automatic updates for application signatures.
- Configurable application control lists independent of URL filtering.

11. **High Availability:**

- Built-in high availability features with no extra cost or hardware requirements.
- Support for stateful session maintenance during failover.
- Configurable Active/Active or Active/Passive configurations.

12. **OEM Certifications:**

- NGFW OEM should be EAL 4 certified.

13. **Submission**: Interested vendors should submit proposals via email to **am.it@kfon.in by 22/03/2024 – 4PM.**

14. **Evaluation Criteria**: Evaluation of proposals will be based on compliance with specifications, vendor experience and reputation, pricing, support and maintenance offerings, and any additional value-added services.

15. **Terms and Conditions:** KFON reserves the right to reject any or all proposals, waive any irregularities or informalities in the proposals received, and accept any proposal deemed to be in the best interest of the organization. All costs associated with proposal preparation are the responsibility of the vendor. Installation, configuration, and commissioning of the NGFW are required and should be included in the proposal. Device with UTP support licenses should be valid for a period of 3 years from the date of commissioning.

Contact Information: For any inquiries or clarification regarding this RFP, please contact **Anurup M, System Administrator – 8907130449** , **am.it@kfon.in**