नेपाल सरकार
भौतिक पूर्वाधार तथा यातयात मन्त्रालय
सडक विभाग
योजना तथा अनुगमन महाशाखा
(HMIS-ICT शाखा)

वेव: https://dor.gov.np
इमेल: mis@dor.gov.np
ict@dor.gov.np
फोनः +९७७-०१-
बबरमहल, काठमाडौं ।

प.सं. :- ०८०/८१

मिति :- २०८१/०८/१९

च.नं. :- HMIS/ICT/६४

विषयः लागत अनुमान तयार गर्ने प्रयोजनका लागि बजारभाउ उपलब्ध गराउने बारे ।

यस विभागको लागि आवश्यक Enterprise Network Firewall खरिदको लागि लागत अनुमान तयार गर्नुपर्ने भएकोले सोको लागि बजारभाउ आवश्यक रहेको हुँदा यसै सूचना साथ संलग्न प्राविधिक स्पेशिफिकेशन भएको Firewall को बजारभाउ ७ दिन भित्र उपलब्ध गराई सहयोग गरिदिनुहुन सम्बन्धित सबैलाई अनुरोध गरिन्छ ।

.....

(सुप्रितम राज श्रेष्ठ)
कम्प्युटर इन्जिनियर

Government of Nepal
Ministry of Physical Infrastructure and Transport
Department of Roads
Babarmahal, Kathmandu

| Technical Description, Specifications, and Standards for Enterprise Firewall | | |
|---|---|---|
| **S.No.** | **Particulars** | **Requirements** |
| 1. | Brand | (To be mentioned by the bidder) (To be mentioned by the bidder) |
| 2. | Model | (To be mentioned by the bidder) (To be mentioned by the bidder)<br>The proposed model should not be declared as End of Sales/End of Support |
| 3. | Industry Compliance | OEM must be part of leader or challenger quadrant in the latest Gartner Magic Quadrant for Network Firewall |
| 4. | Connectivity | Min. 10 x 1 GbE Ports (RJ45)<br>Min. 4 x 1GbE Ports (SFP)<br>Min. 2 x 10 GbE Ports (SFP+)<br>1 Management Port<br>1 Console Port<br>USB Port |
| 5. | Concurrent Sessions | Min. 2.5 million |
| 6. | New Connections/Second | 120K |
| 7. | Firewall Throughput | Minimum 30 Gbps |
| 8. | IPS Throughput | Minimum 4.5 Gbps |
| 9. | NGFW Throughput | Minimum 2.5 Gbps |
| 10. | Threat Protection Throughput (FW + AVC + IPS+ Antivirus +Anti Malware) | Min. 2 Gbps |
| 11. | IPSec VPN Throughput | Minimum 25 Gbps |
| 12. | Features | 1. Virtual Firewall Instances<br>The firewall solution must support virtual firewall instances from the initial deployment. All necessary licenses required to enable this feature must be included.<br>2. Operational Modes<br>The system must support both Transparent (bridge) mode, ensuring minimal disruption to the existing network infrastructure, and NAT/Route mode. These modes must be operable concurrently.<br>3. VPN Capabilities<br>The solution must support IPSEC and SSL VPN functionality. Licensing for at least 100 SSL VPN clients must be included from day one.<br>4. Traffic Shaping<br>Advanced traffic shaping and quality of service (QoS) functionalities must be integral to the proposed system. |

| | | |
|---|---|---|
| | | 5. Next-Generation Firewall Features<br>The firewall must support configurable actions for TCP session management.<br>6. Multi-Factor Authentication (MFA)<br>The system must either have inbuilt support or integrate with third-party multi-factor authentication platforms.<br>7. Real-Time Monitoring and Dashboard<br>The solution must feature real-time event monitoring through pre-defined dashboards for SD-WAN, VPN, Wi-Fi, inbound/outbound traffic, applications, and websites.<br>8. Low Latency<br>The firewall must ensure latency does not exceed 4 microseconds under normal operating conditions.<br>9. Intrusion Prevention System (IPS)<br>The IPS be capable of mitigating Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.<br>10. Web Filtering<br>The firewall must include URL filtering based on a real-time categorization database.<br>11. SSL Inspection<br>The system must support SSL inspection with a throughput of at least 3 Gbps, incorporating features like safe search enforcement and automatic or manual signature updates.<br>12. Antivirus and File Control<br>The firewall must provide granular control to block, allow, or monitor traffic using antivirus signatures and file-blocking rules. Policies must be configurable by firewall rules or authenticated user groups.<br>13. Anti-APT Integration<br>The system must integrate bi-directionally with an Anti-Advanced Persistent Threat (APT) solution to enable zero-day malware detection and threat intelligence sharing for attack mitigation.<br>14. Email Filtering and Anti-Spam<br>The proposed solution must support email filtering with the ability to allow or block mail based on predefined criteria. It must also include anti-spam capabilities to detect and block spam emails across IMAP, SMTP, POP3, and MAPI protocols.<br>15. High Availability |

| | | |
|---|---|---|
| | | The firewall must support high availability configurations, including both Active/Active and Active/Passive modes.<br>16. Redundant Power Supplies<br>The device must include redundant power supplies to ensure uninterrupted operation in the event of power supply failure. |
| 13. | Routing and Networking | 1. Routing Capabilities<br>The proposed solution must support static routing, policy-based routing, identity-based routing, multicast routing, and dynamic routing protocols<br>2. ISP Failover and Load Sharing<br>The system must support seamless ISP failover and load sharing to ensure uninterrupted connectivity and optimized bandwidth utilization.<br>3. NAT and Address Translation<br>The solution must support: Dynamic NAT and PAT, NAT46, NAT64, DNS64 and DHCPv6<br>4. SD-WAN Capabilities<br>The system must include comprehensive SD-WAN functionality from the initial deployment. Any necessary licensing must be provided. The SD-WAN throughput must not be less than 20 Gbps.<br>5. Simultaneous WAN Link Utilization<br>The firewall must be capable of utilizing all configured WAN links simultaneously to maximize network efficiency and throughput. |
| 14. | Management, Monitoring and Usability | 1. Centralized management with GUI, CLI, and API support.<br>2. Real-time monitoring<br>3. Automated Threat Response<br>4. Role-based access control (RBAC) for multi-user environments.<br>5. Logging and reporting with storage for at least 30 days of logs.<br>6. Automated firmware updates and vulnerability patching. |
| 15. | License | 3 years |
| 16. | Warranty and Support | Minimum 3 years with hardware replacement and 24*7 support |
| 17. | Accessories | Related Accessories |
| 18. | Installation site | IDMC, Singhadarbar,<br>DOR, Babarmahal and<br>DRC Hetauda |