Phần 2. YÊU CẦU VỀ KỸ THUẬT
Chương V. YÊU CẦU VỀ KỸ THUẬT

1. Giới thiệu chung về dự toán gói thầu

- Tên dự toán: Gia hạn bảo hành Hệ thống cân bảng tải và tường lửa API chuyên dụng (NGINX Plus)

- Tên gói thầu: Gia hạn bảo hành Hệ thống cân bảng tải và tường lửa API chuyên dụng (NGINX Plus)

- Tên Chủ đầu tư: Chi nhánh Tổng công ty Điện lực miền Nam TNHH – Trung tâm Chăm sóc khách hàng.

- Nguồn vốn: Sản xuất kinh doanh năm 2026

- Địa điểm: 12, Thi Sách, Phường Sài Gòn, TP. Hồ Chí Minh

- Thời gian thực hiện gói thầu: 30 ngày

- Loại hợp đồng: trọn gói

2. Mục tiêu công việc:

Mục tiêu công việc của gói thầu này là chọn đơn vị triển khai thực hiện dịch vụ gia hạn bảo hành Hệ thống cân bằng tải và tường lửa API chuyên dụng (NGINX Plus) nhằm đảm bảo tính ổn định tuyệt đối cho hệ thống điều phối lưu lượng, triệt tiêu nguy cơ gián đoạn dịch vụ đồng thời nâng tầm trải nghiệm cho khách hàng qua các ứng dụng CSKH

3. Yêu cầu kỹ thuật của gói thầu:

Stt	Thành phần tối thiểu các tính năng của bản quyền	Yêu cầu
Gia hạn (renewal) bản quyền tính năng cho gói phần mềm hiện hữu NGINX cân bằng tải và bảo vệ ứng dụng dụng Web với thời hạn bắt đầu từ ngày ký hợp đồng đến ngày 30/01/2028		
I	**Yêu cầu chung**	
1	**Nhà sản xuất**	**Nhà Thầu khai báo**
2	**Mã hiệu**	**Nhà Thầu khai báo**
3	Đính kèm đường link tham chiếu Catalogue trên website nhà sản xuất. Đính kèm tài liệu xác nhận cung cấp hỗ trợ gia hạn từ nhà phân phối chính thức của nhà sản xuất tại Việt Nam.	Có
II	**Yêu cầu các tính năng tối thiểu phải có**	
1	Giải pháp phần mềm (software-based) bản quyền (cho 2 instance) với thời hạn ***bắt đầu từ ngày ký hợp đồng đến ngày kết thúc: 30/01/2028*** gồm: NGINX PLUS PREMIUM SUPPORT (tương đương hoặc cao hơn) NGINX APP PROTECT DOS PREMIUM (tương đương hoặc cao hơn) NGINX APP PROTECT WAF PREMIUM (tương đương hoặc cao hơn)	Có

Stt	Thành phần tối thiểu các tính năng của bản quyền	Yêu cầu
2	Hỗ trợ cài đặt trên các hệ điều hành Linux phổ biến, bao gồm: CentOS, Debian, Ubuntu, và RHEL.	Có
3	Giải pháp phải có khả năng triển khai trong các môi trường sau: Máy chủ vật lý (bare metal server) Máy ảo (virtual machines) Public Cloud Container (ví dụ: Docker, Kubernetes)	Có
4	Giải pháp phải hỗ trợ chế độ Cluster và/hoặc High Availability (HA)	Có
5	Giải pháp phải hỗ trợ các phương thức xác thực sau: Xác thực bằng JSON Web Token (JWT) Đăng nhập một lần OpenID Connect (Single Sign-on) Xác thực qua OAuth 2.0 Token Introspection	Có
6	Giải pháp phải hỗ trợ giải mã TLS (TLS offloading) lên đến phiên bản TLS 1.3	Có
7	Hỗ trợ cấu hình Mutual TLS (mTLS) để bảo mật lưu lượng giữa client và server	Có
8	Giải pháp phải hỗ trợ các thuật toán cân bằng tải (load balancing algorithms) sau: Round Robin Least Connections Least Time Hash Key (ví dụ: theo địa chỉ IP, request URI, v.v.)	Có
9	Hỗ trợ cơ chế duy trì phiên (session persistence) để đảm bảo các yêu cầu từ cùng một client được chuyển đến cùng một origin server, bao gồm: Sticky Cookie Sticky Route Sticky Learn	Có
10	Hỗ trợ Passive Health Check	Có
11	Hỗ trợ Active Health Check dựa trên status code và response body bằng cách gửi yêu cầu kiểm tra riêng và xác minh phản hồi	Có
12	Có chức năng dynamic discovery các máy chủ thông qua truy vấn DNS	Có
13	Hỗ trợ tính năng Content Rewrite trong HTTP request và HTTP response	Có
14	Hỗ trợ giao thức HTTP/2 Gateway	Có
15	Hỗ trợ giao thức gRPC	Có
16	Giải pháp phải có khả năng giám sát trực tiếp (live monitoring) thông qua bảng điều khiển thời gian thực (real-time dashboard)	Có
17	Hỗ trợ chuyển tiếp nhật ký (syslog forwarding) tới hệ thống thu thập log của bên thứ ba	Có
18	Layer 7 request routing	Có

Stt	Thành phần tối thiểu các tính năng của bản quyền	Yêu cầu
19	Bảo vệ ứng dụng web, API, và gRPC trước các tấn công tầng ứng dụng (Layer 7) bao gồm OWASP Top 10, bot signatures, hoặc threat campaign protection.	Có
20	Hỗ trợ mask thông tin PII với tính năng Data Guard, đáp ứng chuẩn PCI DSS và các quy định bảo vệ dữ liệu.	Có
21	Hỗ trợ tự động tạo dynamic signatures, và sử dụng adaptive learning để điều chỉnh chính sách bảo vệ trước các mối đe dọa mới	Có
22	Bảo vệ chống lại nhiều loại tấn công DoS phức tạp như GET/POST flood, Slowloris, Slow Read, Slow POST, và Challenger Collapsar	Có
23	Thời gian hỗ trợ: 24x7 chính hãng Hỗ trợ qua email and phone chính hãng Thời gian phản hồi: **30 phút đến 24 tiếng** tùy theo cấp độ Severity Level	Có

4. Giải pháp và phương pháp luận:

Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Chương này, gồm các phần như sau:

1. Giải pháp và phương pháp luận;

2. Kế hoạch công tác.

5. Quy định về kiểm tra, nghiệm thu sản phẩm:

Mục này quy định về quy trình kiểm tra, nghiệm thu sản phẩm, trình tự giao nộp sản phẩm (nếu có)... để phục vụ công tác thanh, quyết toán hợp đồng.