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

I. Giới thiệu chung về PAMS, gói thầu:

- Tên của Phương án mua sắm: Trang bị mở rộng hệ thống Tường lửa ứng dụng Web.
- Tên gói thầu: Mua sắm hệ thống Tường lửa ứng dụng Web chuyên dụng.
- Nội dung công việc chính của gói thầu: Mua sắm hệ thống Tường lửa ứng dụng Web chuyên dụng (bao gồm thiết bị và bản quyền WAF) kèm bảo hành, dịch vụ hỗ trợ kỹ thuật 03 năm.
- Lĩnh vực LCNT: Mua sắm hàng hóa
- Thời gian thực hiện gói thầu: 44 tháng kể từ thời điểm Hợp đồng có hiệu lực.
- Tên Chủ đầu tư: Ngân hàng TMCP Đầu tư và Phát triển Việt Nam

II. Yêu cầu về kỹ thuật:

1. Yêu cầu chung

- Phạm vi mua sắm

#	Hạng mục mua sắm	Số lượng	Đơn vị tính
1	Thiết bị tường lửa ứng dụng Web kèm bảo hành, dịch vụ hỗ trợ kỹ thuật 03 năm	04	Thiết bị
2	Gói bản quyền tường lửa ứng dụng Web và quản trị tập trung cho 04 thiết bị WAF mua sắm tại mục 1 kèm dịch vụ hỗ trợ kỹ thuật 03 năm và dịch vụ triển khai	01	Gói

- Thời gian thực hiện hợp đồng 44 tháng, trong đó:
  - Thời gian bàn giao, nghiệm thu hàng hóa: 02 tháng kể từ ngày hợp đồng có hiệu lực.
  - Thời gian triển khai cài đặt: 04 tháng kể từ ngày nghiệm thu hàng hóa.
  - Thời gian bảo hành, hỗ trợ kỹ thuật: 36 tháng kể từ ngày nghiệm thu hoàn thành triển khai đưa vào sử dụng.
  - Thời gian nghiệm thu thanh lý hợp đồng: 02 tháng.
- Thiết bị chưa có thông tin công bố của hãng về việc ngừng bán (end-of-sales), ngừng hỗ trợ (end-of-support) tại thời điểm nộp HSDT.
- Thiết bị cung cấp kèm theo bản quyền chính hãng (bản quyền dạng vĩnh viễn hoặc subscription trong tối thiểu 03 năm) và 03 năm (36 tháng) bảo hành, hỗ trợ kỹ thuật tiêu chuẩn từ hãng sản xuất.
- Địa điểm bàn giao hàng hóa và triển khai: Các Trung tâm dữ liệu (TTDL) của BIDV tại Hà Nội (TTDL chính Duy Tân, TTDL Dự phòng IDC Viettel Hòa Lạc).

2. Yêu cầu về tiêu chuẩn kỹ thuật cho thiết bị chuyên dụng

STT	YÊU CẦU TỐI THIỂU
1	**Phần cứng và hiệu năng**
	WAF (L7) Throughput: ≥ 5 Gbps
	SSL/TLS Performance (RSA-2K): ≥ 30K TPS
	L7 RPS (Non-SSL) >=4M hoặc L7 RPS (SSL/TLS) >=200K
	Form factor: ≤ 2U
	Cổng mạng: tối thiểu 4x 10GbE Fiber SR (kèm 04 transceiver 10G SR)

	- Cổng quản trị tối thiểu: 1 x GbE Copper 1 x Serial Console RJ45 1 x USB 2.0 hoặc cao hơn
	RAM Memory: ≥ 128 GB
	Nguồn (Power Supply): ≥ 2 nguồn, 100-240 VAC
	Có card phần cứng tăng tốc giải mã SSL (SSL ACCELERATION)
2	**Tính năng bảo vệ cơ bản**
	Chống lại được các tấn công vào ứng dụng được nêu trong OWASP Top 10, bao gồm (nhưng không giới hạn): Injection, Broken Authentication, Sensitive Data Exposure và các dạng tấn công phổ biến khác.
	Cung cấp các phương pháp bảo vệ cookie: cookie injection, cookie tampering, cookie signing, cookie encryption.
	Bảo vệ dữ liệu nhạy cảm với mẫu dữ liệu định nghĩa sẵn, và tùy biến được mẫu dữ liệu nhạy cảm theo yêu cầu của BIDV.
	Có chức năng bảo vệ web service / API với các định dạng phổ biến như SOAP, XML, JSON.
	Có tích hợp dịch vụ Intelligence (Reputation Services) nhận diện và ngăn chặn các nguồn truy cập được biết đến là độc hại gồm: Malicious Ips/Botnet, Anonymous Proxies, TOR IP addresses; nhận diện Phishing URLs - giả mạo domain website được bảo vệ.
	Có khả năng phát hiện và ngăn chặn các hành vi truy cập tự động hoặc tấn công bot với các cơ chế chống bot như: CAPTCHA, Javascript Challenge hoặc Fingerprint.
3	**Mô hình triển khai**
	Hỗ trợ các mô hình triển khai với tính sẵn sàng cao (Active/Standby, Active/Active…).
	Hỗ trợ các mô hình triển khai: Reverse Proxy, Transparent Reverse Proxy/Transparent Bridge…
	Cho phép cấu hình để bảo vệ nhiều ứng dụng Web/API khác nhau bằng cách thiết lập các bộ chính sách riêng cho từng ứng dụng được bảo vệ.
4	**Hỗ trợ SSL/TLS**
	Có chức năng giải mã và phân tích sâu các gói tin mã hóa, hỗ trợ chức năng SSL Offload.
	Hỗ trợ TLS từ 1.2 trở lên.
	Hỗ trợ HTTP/1 và HTTP/2.
5	**Kiểm soát truy cập dựa trên địa chỉ nguồn (IP/Domain), quốc gia, vùng miền địa lý (Geolocation)**
	Có chức năng thiết lập danh sách các IP, quốc gia được phép hoặc không được phép truy cập.
6	**Phòng chống các hình thức tấn công từ chối dịch vụ (DDoS), Bot và các công cụ tự động**
	Có chức năng phát hiện và ngăn chặn, giảm thiểu mức độ ảnh hưởng của các hình thức tấn công từ chối dịch vụ DDos.
	Có chức năng phát hiện và ngăn chặn các hành động truy cập bất thường, như web scanning, scraping tools….
	Có chức năng tự động yêu cầu xác thực challenge-response để ngăn chặn các công cụ duyệt web tự động.
7	**Kiểm soát tuân thủ giao thức HTTP/HTTPS**

	Có chức năng thiết lập chế độ kiểm tra đảm bảo tuân thủ giao thức HTTP/HTTPS, phát hiện, cảnh báo và ngăn chặn các trường hợp vi phạm giao thức HTTP/HTTPS.
8	**Bảo vệ ứng dụng Web, API**
	Có chức năng học, phân tích cấu trúc, nội dung của website/ứng dụng để xây dựng whitelist, các chính sách bảo vệ phù hợp.
	Có chức năng phát hiện và bảo vệ ứng dụng khỏi các cuộc tấn công khai thác lỗ hổng bảo mật ứng dụng web: OWASP Top 10 (Injection, Broken Authentication, Broken Access Control, Sensitive Data Exposure, Cross-Site Scripting, CSRF…).
	Có chức năng kiểm tra, bảo vệ, phát hiện và ngăn chặn các hình thức tấn công chèn mã độc (malicious code injection), thay đổi tham số, cookie (parameter tampering, cookie tampering).
	Có chức năng tự động phát hiện và ngăn chặn các hình thức tấn công dò tìm mật khẩu (brute-force) các trang đăng nhập của ứng dụng.
	Có chức năng kiểm tra, giám sát phiên giao dịch của người dùng (session/user tracking); có cơ chế kiểm tra, bảo vệ, phát hiện và ngăn chặn các hình thức tấn công chiếm phiên làm việc (session hijacking).
	Có chức năng phân tích kiểm tra đảm bảo các API request đúng định dạng được quy định, có chức năng kiểm tra dữ liệu, kiểm tra độ dài giá trị tham số API.
	Có chức năng vá ảo (virtual patching), có tích hợp với các công cụ rà quét điểm yếu về bảo mật (vulnerability scanner) (vui lòng liệt kê các công cụ mà giải pháp hỗ trợ).
9	**Quản lý cấu hình và chính sách bảo mật**
	Có sẵn các mẫu chính sách bảo mật (policy templates) giúp quản trị viên tạo các chính sách bảo mật dễ dàng, nhanh chóng.
	Có chức năng sao lưu, phục hồi cấu hình hệ thống.
10	**Quản trị tập trung**
	Hỗ trợ SNMP, SMTP/Email, syslog, real-time monitoring cho giám sát.
	Cung cấp chức năng quản trị, bao gồm triển khai và cấu hình chính sách, giám sát và báo cáo cho nhiều thiết bị WAF trên cùng một giao diện console.
	Cung cấp dashboard giám sát các sự kiện an ninh trong thời gian thực.
	Quản trị theo vai trò: Cho phép tạo các tài khoản quản trị theo các vai trò khác nhau (Role-Based Access Control).
	Giám sát trạng thái sức khỏe hệ thống WAF triển khai.
	Có chức năng ghi nhật ký và trích xuất nhật ký các hành động của người dùng theo thời gian.

3. Yêu cầu về bảo hành, hỗ trợ kỹ thuật

- Địa điểm thực hiện: Các Trung tâm dữ liệu (TTDL) của BIDV tại Hà Nội (TTDL chính Duy Tân, TTDL Dự phòng IDC Viettel Hòa Lạc).
- Thời gian thực hiện: 36 tháng theo tiêu chuẩn của hãng kể từ ngày nghiệm thu hoàn thành triển khai đưa vào sử dụng.
- Tần suất thực hiện: Định kỳ 06 tháng/lần vào tuần thứ 2, tháng đầu tiên của kỳ bảo trì, hoặc đột xuất khi phát sinh lỗi/sự cố trên thiết bị, hệ thống.

- Hình thức thực hiện: tại chỗ (On-site) và từ xa (Off-site), tùy thuộc vào mức độ cấp thiết và khẩn cấp của sự việc cần hỗ trợ.
- Hỗ trợ kỹ thuật 24*7, bảo hành phần cứng, bản quyền phần mềm cho tối thiểu 03 năm.
- Được cung cấp tài khoản và có thể truy cập vào trang web hỗ trợ của hãng để tìm kiếm, tải về các tài liệu, tài nguyên, liên quan đến sản phẩm, và có thể tạo yêu cầu hỗ trợ.
- Được phép cập nhật miễn phí tất cả các phiên bản phần mềm (software/firmware) mới nhất, bản vá lỗi, bản vá bảo mật của thiết bị được hãng phát hành.
- Yêu cầu chung:
    - o Đảm bảo duy trì hoạt động liên tục, ổn định của hệ thống bảo mật cho các ứng dụng web nhằm cung cấp dịch vụ với chất lượng cao, ổn định, thuận tiện và an toàn.
    - o Đảm bảo ngăn ngừa lỗi, hạn chế phát sinh sự cố đối với hệ thống, góp phần nâng cao tính bảo mật, an toàn trong công tác vận hành hệ thống.
    - o Đảm bảo khả năng sửa chữa nhanh những hỏng hóc, khắc phục kịp thời sự cố phát sinh nhằm khôi phục và đảm bảo khả năng sẵn sàng hoạt động một cách nhanh nhất cho hệ thống đảm bảo an toàn cho ứng dụng web.
    - o Cung cấp quy trình xử lý nhanh để giảm thiểu tối đa ảnh hưởng đến hệ thống, người dùng do chặn nhầm request.
- Bảo hành, hỗ trợ kỹ thuật định kỳ:
    - o Định kỳ 06 tháng/lần vào tuần thứ 2, tháng đầu tiên của kỳ bảo trì, nhà thầu thực hiện kiểm tra tình trạng hoạt động của phần cứng và phần mềm thiết bị và đưa ra những khuyến nghị nhằm đảm bảo và nâng cao hiệu quả hoạt động của thiết bị.
    - o Các yêu cầu kiểm tra cụ thể:
        - Thực hiện phân tích đánh giá các vấn đề kỹ thuật của hệ thống định kỳ dựa trên file log của hệ thống, có báo cáo đầy đủ về các vấn đề phát sinh và nội dung thực hiện.
        - Thực hiện phân tích đánh giá mức tăng trưởng dữ liệu của hệ thống định kỳ có báo cáo đề xuất thiết lập tham số và tối ưu hệ thống.
        - Thực hiện cập nhật bản vá lỗi của hệ thống định kỳ và có báo cáo kết quả thực hiện.
- Bảo hành, hỗ trợ kỹ thuật đột xuất:
    - o Thay thế sửa chữa miễn phí (chi phí tính trong chi phí bảo trì) các thiết bị, linh kiện hỏng hóc, khắc phục sự cố, cài đặt, hiệu chỉnh, nâng cấp phần mềm hệ thống đảm bảo hoạt động liên tục, ổn định, an toàn của các thành phần trong phạm vi áp dụng.
    - o Kênh hỗ trợ: Tùy theo tính chất và mức độ của sự cố phát sinh, các yêu cầu hỗ trợ có thể được tiếp nhận thông qua các kênh sau:
        - Thông qua websites hỗ trợ của hãng.
        - Thông qua email tới bộ phận tiếp nhận yêu cầu hỗ trợ từ hãng, hoặc đầu

mối nhà thầu.

- Thông qua điện thoại trực tiếp tới đầu mối tiếp nhận hỗ trợ của nhà thầu.

o Thời gian hỗ trợ trực tuyến: 24x7x365.

o Thời gian phản hồi: Đối với các yêu cầu hỗ trợ sự cố được tạo trên website của hãng sẽ được phản hồi trong khoảng thời gian theo tiêu chuẩn của từng hãng. Đối với các yêu cầu hỗ trợ sự cố khác, thời gian phản hồi và hình thức hỗ trợ tùy theo mức độ cần đáp ứng như sau:

o Yêu cầu thời gian phản hồi với sự cố:

Cấp độ nghiêm trọng	Mô tả	Thời gian đáp ứng	Phương thức hỗ trợ
1	Lỗi gây cho sản phẩm không hoạt động, hoặc gây ảnh hưởng nghiêm trọng như ảnh hưởng toàn hệ thống, hoặc hệ thống bị dừng.	0.5 giờ	Tại chỗ 24x7
2	Lỗi làm giảm hiệu năng của sản phẩm, hoặc hạn chế các dịch vụ kinh doanh như ảnh hưởng nhẹ đến hệ thống, làm treo hệ thống.	04 giờ	Tại chỗ 24x7
3	Lỗi gây ra ảnh hưởng nhỏ đến việc sử dụng sản phẩm, các ảnh hưởng nhẹ đến hệ thống, các ảnh hưởng đến hiệu năng và chức năng.	04 giờ	Từ xa 8x5
4	Lỗi liên quan đến phần mềm mà không ảnh hưởng nhiều đến việc sử dụng chức năng sản phẩm để thực hiện hoạt động kinh doanh.	04 giờ	Từ xa 8x5

o Yêu cầu công việc:

- Thực hiện hỗ trợ đột xuất theo thực tế các phát sinh của hệ thống trong quá trình vận hành.
- Thực hiện hỗ trợ BIDV trong quá trình khai báo tham số theo yêu cầu của nghiệp vụ.

4. Yêu cầu bàn giao, nghiệm thu hàng hóa

- Nhà thầu phải bàn giao đầy đủ thiết bị và bản quyền phần mềm của thiết bị và các bản quyền phần mềm liên quan khác nếu có.
- Nhà thầu phải bàn giao đầy đủ các tài liệu theo quy định.

Danh mục tài liệu/báo cáo cần cung cấp:

STT	Tài liệu/Báo cáo	**Thời điểm thực hiện** (Trong vòng khoảng thời gian yêu cầu tính từ ngày bàn giao hàng hóa)
1	Tài liệu thiết kế đảm bảo các nội dung theo yêu cầu của BIDV.	90
2	Tài liệu hướng dẫn cài đặt, triển khai dịch vụ, vận hành hệ thống.	90
3	Quy trình bảo hành, bảo trì, nâng cấp sản phẩm, hỗ trợ kỹ thuật, xử lý sự cố.	90

4	Tài liệu hướng dẫn chuyển đổi dự phòng DC-DC, DC-DR.	90

5. Yêu đối với Dịch vụ triển khai/ tích hợp.

- Nhà thầu thực hiện khảo sát và đề xuất kế hoạch triển khai chi tiết trước thời điểm bàn giao hàng hóa tối thiểu 05 ngày làm việc.
- Nội dung triển khai bao gồm (nhưng không giới hạn) các công việc lắp đặt, cấu hình thiết bị và bản quyền, tích hợp chuyển đổi ứng dụng từ thiết bị cũ sang thiết bị mới, đảm bảo triển khai tích hợp chuyển đổi thành công các ứng dụng đang triển khai trên thiết bị tường lửa ứng dụng Web cũ của BIDV sang thiết bị tường lửa trang bị mới không làm giảm yêu cầu về bảo mật.
- Có phương án và nhân sự hỗ trợ triển khai tích hợp đảm bảo hạn chế tối đa thời gian downtime hệ thống và các hành động phản ứng của WAF không chính xác.