NGÂN HÀNG TMCP SÀI GÒN – HÀ NỘI

SHB

Solid partners, flexible solutions

HỒ SƠ YÊU CẦU CHÀO HÀNG

TRIỂN KHAI GIẢI PHÁP TƯỜNG LỬA ỨNG DỤNG WEB VÀ GIẢI PHÁP PHÒNG CHỐNG TẤN CÔNG TỪ CHỐI DỊCH VỤ DDOS ĐỂ BẢO VỆ CHO CÁC ỨNG DỤNG CỦA SHB

2025

SHB
Solid partners, flexible solutions

NGÂN HÀNG TMCP SÀI GÒN - HÀ NỘI

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Hà Nội, ngày 23.. tháng 7... năm 2025

THƯ MỜI

***Kính gửi*: Quý Công ty**

Ngân hàng TMCP Sài Gòn - Hà Nội có nhu cầu Triển khai giải pháp tường lửa ứng dụng web và giải pháp phòng chống tấn công từ chối dịch vụ DDoS để bảo vệ cho các ứng dụng của SHB. Trân trọng kính mời Quý Công ty tham dự chào hàng gói thầu nêu trên.

Quý Công ty có thể tìm hiểu thêm các thông tin cần thiết trong Hồ sơ yêu cầu chào hàng kèm theo.

Hồ sơ chào hàng được gửi tới địa chỉ: Trung tâm mua sắm, Ngân hàng TMCP Sài Gòn - Hà Nội, Toà nhà 81 Trần Hưng Đạo, Phường Cửa Nam, TP Hà Nội.

Thời gian nhận hồ sơ: trước 15h00 ngày..30.. tháng 7 năm 2025.

Người nhận: Nguyễn Ngọc Cầu – Phòng Đấu thầu-Trung tâm mua sắm

Điện thoại di động: 0977901188

Trân trọng kính mời./.

NGÂN HÀNG TMCP SÀI GÒN HÀ NỘI

M.S.D.N: 1800278630 - C.T.C.P
NGÂN HÀNG THƯƠNG MẠI CỔ PHẦN SÀI GÒN - HÀ NỘI
Q. HOÀN KIẾM - TP. HÀ NỘI

Đào Ngọc Dũng

PHẦN I.
CÁC YÊU CẦU VỀ HỒ SƠ CHÀO HÀNG

I. Yêu cầu về Hồ sơ chào hàng

- Hồ sơ chào hàng phải được lập thành 02 bản **(01 bản gốc + 01 bản sao)**, đóng trong thùng đựng kín có niêm phong và phải được gửi tới đúng địa điểm trước thời gian quy định trong hồ sơ yêu cầu chào hàng.
- Hồ sơ chào hàng được đóng trong phong bì riêng biệt. Bên ngoài phong bì ghi rõ: Hồ sơ chào hàng: "**Triển khai giải pháp tường lửa ứng dụng web và giải pháp phòng chống tấn công từ chối dịch vụ DDoS để bảo vệ cho các ứng dụng của SHB.**"
- Hồ sơ chào hàng phải có đầy đủ các nội dung sau :

o Đơn chào hàng: Phải có chữ ký của người đại diện theo pháp luật của công ty hoặc người được ủy quyền (Có giấy ủy quyền kèm theo);

o Bảng chào giá chi tiết (phải chào đầy đủ số lượng, chủng loại, giá trước VAT, giá sau VAT…) theo như Phần III Mục 2 của hồ sơ yêu cầu;

o Hiệu lực của Hồ sơ chào hàng tối thiểu **60** ngày kể từ thời điểm hết hạn nộp hồ sơ;

o Đơn vị có 02 hợp đồng tương tự cung cấp giải pháp phần mềm công nghệ thông tin cho hệ thống công nghệ thông tin của ngân hàng bất kỳ có giá trị từ 02 tỷ đồng trở lên kèm hóa đơn VAT và Biên bản nghiệm thu hoặc biên bản bàn giao hoặc thanh lý hợp đồng;

o Đơn vị phải có thư hỗ trợ của hãng, thư nhà phân phối chính hãng, đại lý chính hãng.

o Danh sách cán bộ kỹ thuật kèm bằng cấp chứng chỉ liên quan phục vụ cho công tác triển khai;

o Báo cáo tài chính 02 năm gần nhất kiểm toán hoặc bản nộp qua cổng thông tin điện tử đảm bảo doanh thu bình quân từ 30 tỷ trở lên và có lãi;

o Cam kết chấp nhận yêu cầu về kỹ thuật, chất lượng, theo yêu cầu tại Phần II của Hồ sơ yêu cầu chào hàng;

o Cam kết chấp nhận yêu cầu về điều kiện tài chính thương mại theo yêu cầu tại Phần III của Hồ sơ yêu cầu chào hàng;

II. Thời gian và địa điểm nộp Hồ sơ chào hàng

- **Thời gian:** trước 15h00' ngày 30/7/2025.
- **Địa điểm:** Phòng đấu thầu - Trung tâm mua sắm, Ngân hàng TMCP Sài Gòn Hà Nội, tại Toà nhà số 81 Phố Trần Hưng Đạo, Phường Cửa Nam, TP Hà Nội (Liên hệ Nguyễn Ngọc Cầu, Điện thoại: 0977901188).

PHẦN II.
YÊU CẦU CỤ THỂ

I. Mục tiêu, Phạm vi gói chào hàng

1. Hiện trạng hệ thống ứng dụng của SHB

Hệ thống CNTT của SHB hiện được phân chia thành 02 site, trong đó có 01 site chính - DC tập trung phần lớn các kết nối và giao dịch của SHB, và 01 site dự phòng - DR được xây dựng với mục đích để dự phòng cho site DC trong trường hợp có sự cố bất ngờ xảy ra. Ngoài ra SHB cũng đang triển khai các ứng dụng trên môi trường Cloud AWS và Azure. SHB có hơn 30 hệ thống ứng dụng phục vụ công việc kinh doanh hàng ngày đang cung cấp dịch vụ ra bên ngoài Internet.

2. Mục tiêu của gói chào hàng

Mục tiêu của gói thầu này nhằm lựa chọn nhà thầu có đầy đủ năng lực để thực hiện các công việc thuộc gói chào hàng, cụ thể như sau:

- Cung cấp bản quyền giải pháp tường lửa ứng dụng web và phòng chống tấn công từ chối dịch vụ DDoS để bảo vệ cho các ứng dụng của SHB trong 01 năm, đáp ứng đúng và đầy đủ các yêu cầu theo Hồ sơ yêu cầu chào hàng (HSYCCH).
- Cung cấp dịch vụ triển khai, cài đặt, cấu hình và tích hợp giải pháp để bảo vệ cho các ứng dụng của SHB tại Onprem và Cloud.
- Cung cấp dịch vụ hỗ trợ kỹ thuật 24x7 theo tiêu chuẩn của hãng đối với giải pháp do nhà thầu cung cấp trong 01 năm.

3. Phạm vi của gói chào hàng

Nhà thầu cần thực hiện đầy đủ các công việc sau :

- Cung cấp bản quyền giải pháp tường lửa ứng dụng web và phòng chống tấn công từ chối dịch vụ DDoS để bảo vệ cho các ứng dụng của SHB trong 01 năm, đáp ứng đúng và đầy đủ các yêu cầu theo Hồ sơ yêu cầu chào hàng (HSYCCH).
- Cung cấp dịch vụ triển khai, cài đặt, cấu hình giải pháp và tích hợp giải pháp để bảo vệ cho các ứng dụng của SHB tại Onprem và Cloud.
- Cung cấp dịch vụ hỗ trợ kỹ thuật 24x7 theo tiêu chuẩn của hãng đối với giải pháp do nhà thầu cung cấp trong 01 năm.
- Bàn giao đầy đủ Bản quyền, tài liệu đi kèm sản phẩm (nếu có).
- Bảng dưới đây liệt kê phạm vi cung cấp hàng hóa và dịch vụ:

STT	DANH MỤC HÀNG HÓA	ĐƠN VỊ	SL
1	Bản quyền giải pháp tường lửa ứng dụng web và phòng chống tấn công từ chối dịch vụ DDoS để bảo vệ cho các ứng dụng của SHB.	License/ năm	01
2	Dịch vụ triển khai, cài đặt, cấu hình giải pháp và tích hợp giải pháp để bảo vệ cho các ứng dụng của SHB tại Onprem và Cloud.	Gói	01
3	Dịch vụ hỗ trợ kỹ thuật 24x7 theo tiêu chuẩn của hãng đối với giải pháp do nhà thầu cung cấp trong 01 năm.	Gói	01

II. Yêu cầu kỹ thuật

Nhà thầu cung cấp các tài liệu chứng minh đáp ứng các yêu cầu về kỹ thuật như sau:

1. Yêu cầu chung về giải pháp

Nhà thầu cung cấp giải pháp tường lửa ứng dụng web và phòng chống tấn công từ chối dịch vụ DDoS để bảo vệ cho các ứng dụng của SHB đáp ứng yêu cầu kỹ thuật tối thiểu dưới đây:

- Giải pháp thuộc một trong ba nhà cung cấp: Akamai, Cloudflare hoặc Imperva.
- Giải pháp tường lửa ứng dụng web (WAF) và giải pháp phòng chống tấn công DDOS (Anti DDoS) được cung cấp dịch vụ trên cùng một nền tảng Cloud
- Giải pháp hỗ trợ bảo vệ đa nền tảng Onprem và Public Cloud. Nhà thầu đề xuất mô hình triển khai chi tiết.
- Giải pháp đã triển khai thành công cho khách hàng khối Ngân hàng tại Việt Nam (nhà thầu nêu cụ thể các Ngân hàng đã sử dụng).
- Giải pháp có tối thiểu 06 điểm hiện diện (PoP), được đặt tại tối thiểu ba thành phố lớn tại Việt Nam: Hà Nội, Đà Nẵng và Thành phố Hồ Chí Minh. Các PoP này là các PoP xử lý (processing PoP), có khả năng thực hiện các chức năng tính toán như kiểm tra bảo mật, xử lý WAF, caching, lọc bot, và tối ưu hiệu suất truy cập, không chỉ là các node chuyển tiếp, mạng hoặc edge node thụ động.
- Hạ tầng PoP được triển khai trên nhiều nước khác nhau ngoài Việt Nam, tối thiểu bao gồm các quốc gia sau: Singapore, Hong Kong, Châu Âu, Mỹ nhằm đảm bảo khả năng phòng chống tấn công DDoS và đảm bảo khả năng sẵn sàng truy cập từ các quốc gia ngoài Việt Nam.
- Hỗ trợ môi trường Staging/UAT nhằm kiểm tra toàn bộ các các cấu hình bao gồm cấu hình WAF, DDoS, BOT mà không làm ảnh hưởng tới lưu lượng người dùng thực tế.
- Giải pháp phải tính phí theo top level domain, unlimited subdomain.
- Giải pháp hỗ trợ Machine Learning hoặc Behavior Analysis để phát hiện tấn công bất thường.
- Cam kết về uptime dịch vụ của nhà cung cấp: Tối thiểu từ 99% trở lên.
- Đảm bảo lưu lượng xử lý tối thiểu mỗi tháng: Bản quyền giải pháp chào thầu đảm bảo khả năng xử lý tối thiểu 400 triệu request mỗi tháng và lưu lượng truyền tải từ mạng của nhà cung cấp tối thiểu 23 TB mỗi tháng, với độ ổn định cao và không làm suy giảm hiệu suất dịch vụ.
- Cho phép SHB tải lên và quản lý tối thiểu 40 chứng chỉ SSL riêng biệt, phục vụ cho nhiều tên miền hoặc ứng dụng khác nhau trong cùng một hệ thống.

2. Yêu cầu về tính năng và khả năng của giải pháp

2.1. Yêu cầu về 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 vùng miền địa lý, quốc gia được phép hoặc không được phép truy cập (cho phép/ từ chối theo IP, dải IP, quốc gia, geolocation, URI, ...)

- IP Reputation dựa trên việc phân loại địa chỉ IP nguồn kết nối như Tor, Phishing, Proxy, Botnet

2.2. Yêu cầu về Bot management

- Nhà cung cấp cung cấp khả năng phát hiện, phân loại và giảm thiểu lưu lượng truy cập bot tự động.
- Người dùng có thể tạo các quy tắc tùy chỉnh để thực hiện các hành động cụ thể bao gồm ngăn chặn, ghi log.
- Nhà cung cấp có khả năng xác định các bot uy tín đã được công nhận bằng cách sử dụng cơ sở dữ liệu chữ ký được cập nhật tự động lên các bot uy tín mới.
- Nhà cung cấp cung cấp một cơ chế để đưa một đoạn mã Javascript vào trình duyệt để giúp xác định bot.
- Số lượng loại BOT có thể nhận dạng và phản hồi tối thiểu 100 loại.
- Có khả năng nhận diện các loại Bot giả mạo browser.

2.3. Yêu cầu phòng chống tấn công từ chối dịch vụ DDOS

- Cho phép phòng chống DOS/DDoS không giới hạn bất kể số lần, kích thước hoặc thời lượng tấn công mà không tính thêm phí.
- Hỗ trợ phát hiện và ngăn chặn các cuộc tấn công Zero-day và DDOS attack.
- Phát hiện và chặn các hình thức tấn công từ chối dịch vụ thông dụng từ L3-L7.
- Có khả năng chống DDoS Layer 4 tại từng PoP trên toàn cầu mà không cần chuyển về các trung tâm chống DDoS tập trung gây thêm độ trễ.
- Giải pháp cung cấp tối thiểu 100 Tbps thông lượng toàn cầu để chống tấn công DDoS, đảm bảo khả năng xử lý các cuộc tấn công có quy mô cực lớn và đa dạng hình thức mà không ảnh hưởng đến hiệu suất truy cập của người dùng hợp lệ. Việc ngăn chặn DDoS được thực hiện ngay tại PoP nhận traffic, mà không cần chuyển tiếp đến scrubbing center hoặc các PoP xử lý trung gian.
- Có khả năng tự động phát hiện và phản ứng với các cuộc tấn công DDoS trong thời gian không quá 03 giây kể từ khi tấn công được xác định, mà không cần sự can thiệp thủ công của người quản trị.
- Có tính năng ngăn chặn tấn công từ chối dịch vụ xuất phát từ các mạng botnet
- Khả năng chọn lọc lưu lượng tấn công:

  + Đảm bảo khả năng phát hiện và chọn lọc lưu lượng tấn công tối thiểu 80%.

  + Đảm bảo khả năng bảo vệ lưu lượng sạch tối thiểu 85%.

- Giám sát và phân tích sự cố tấn công DDoS:

  + Cho phép giám sát băng thông theo địa chỉ IP và dải mạng phục vụ phân tích tấn công;

  + Cho phép giám sát theo dõi hiệu quả chặn lọc thông qua lưu lượng bằng thông trước và sau khi đi qua bộ lọc.

  + Cho phép giám sát thông tin các cuộc tấn công xảy ra theo thời gian thực và tìm kiếm trong các cuộc tấn công đã xảy ra;"

- Có thể ngăn chặn các hình thức tấn công từ chối dịch vụ (bao gồm tối thiểu nhưng không giới hạn):

  + Tấn công làm tràn ngập băng thông: UDP reflection (DNS, NTP amplification, SSDP attack, Chargen attack), IP fragment, ICMP flood và các dạng tấn công tương tự;

  + Tấn công cạn kiệt tài nguyên qua giao thức TCP: SYN flood, ACK flood, RST flood, SYN-ACK flood và các dạng tấn công tương tự;

  + Tấn công sử dụng gói tin không hợp lệ: malformed, invalid packet;

  + Tấn công gửi gói tin yêu cầu với tần suất cao, đột ngột;

  + Tấn công qua phân tích hành vi người dùng:HTTP page flood, DNS flood, brute force;"

- Có khả năng đếm số request theo các thông tin nâng cao, ít nhất phải hỗ trợ các trường sau: IP nguồn, quốc gia, user agent, HTTP methods, cookies, URI path, …
- Có tính năng cho phép người dùng lựa chọn chủ động các nguồn lưu lượng để ngăn chặn khi lượng request rate gần tới ngưỡng cấu hình và hỗ trợ cấu hình bảo vệ rate limiting đến từng path trên URL hoặc API endpoint.

2.4. Yêu cầu tính năng lường lửa ứng dụng web (WAF)

- Cho phép tạo mới, chỉnh sửa các chính sách bảo vệ và hỗ trợ bộ lọc để tìm kiếm. Ngoài ra có thể bật, tắt, xóa, nhân bản các chính sách bảo vệ
- Cho phép người dùng tự viết Rule phục vụ việc phát hiện và ngăn chặn các cuộc tấn công theo các tham số:
  - Request method
  - Request URI
  - Query string
  - Protocol (name and version)
  - Header name
  - Header value
  - Request body
  - Cookie name
  - Cookie value
- Các thuộc tính tùy chỉnh trong rule có thể được thiết lập bằng:
  - Value
  - Range value
  - Regular expression.
- Hỗ trợ việc giải mã các truy cập Web qua SSL/TLS (HTTPS).
- Hỗ trợ giao thức HTTP/2 và HTTP/3, QUIC.
- Hỗ trợ SSL/TLS version 1.2, version 1.3.

- Cho phép cấu hình tính năng rewrite hoặc redirect trong các request và respond (Ví dụ: Khi phản hồi ra chén thêm cookie vào bản tin respond).
- Có khả năng phát hiện và bảo vệ ứng dụng khỏi các cuộc tấn công khai thác lỗ hổng bảo mật ứng dụng web thuộc Top 10 OWASP.
- Có khả năng chặn lọc các loại file không được cho phép.
- Giải pháp đi kèm nguồn thông tin tình báo về các mối nguy hại được cập nhật thường xuyên giúp nâng cao khả năng bảo vệ với các mối nguy hại mới.
- Có chức năng phát hiện và ngăn chặn, giảm thiểu mức độ ảnh hưởng của các hình thức tấn công từ chối dịch vụ lớp ứng dụng (Layer-7 DoS attack).
- Giải pháp có tính năng tự động cập nhật các chính sách WAF mới nhất.
- Cung cấp khả năng tự động phân tích và đưa ra khuyến cáo WAF rule cho quản trị viên.
- Các bộ quy tắc được cập nhật tự động và thường xuyên để đối phó với các cuộc tấn công mới.
- Có tính năng chặn/cho phép IP, dải mạng, hoặc vùng miền địa lý.
- Có chức năng tự động phát hiện và ngăn chặn các hình thức tấn công dò tìm mật khẩu (brute-force, credential stuffing) 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).
- Cho phép mã hoá các trường thông tin nhạy cảm (sensitive fields) ở phía Client Side (Browser), hỗ trợ HTML Field Obfuscation, Identify Stolen Credentials, và Full AJAX Encryption.
- Cung cấp các phương pháp bảo vệ cookie và session: cookie injection, cookie tampering, session hijacking, session fixation.
- Giải pháp phải có khả năng bảo vệ chống lại các bot thực hiện các hành động sau: Site Scraping; Vulnerability scanning và Comment spamming.
- Có chức năng tự động yêu cầu xác thực challenge-response (như CAPTCHA) để ngăn chặn các công cụ duyệt web tự động và xác thực người dùng khi nghi ngờ.

2.5. Yêu cầu về tính năng API Security

- Có khả năng tự động phát hiện và phân loại các kết nối API đang hoạt động trên hệ thống (API Discovery).
- Có khả năng ngăn chặn lại các tấn công DoS vào các kết nối API.
- Có khả năng tạo các chính sách Rate limiting cho các request API.
- Có chức năng xác thực 2 chiều giữa client và server (Mutual TLS) và quản lý xác thực chứng chỉ số.
- Có cơ chế kiểm tra và xác thực dữ liệu của URL và tham số truyền vào API nhằm đảm bảo dữ liệu hợp lệ, đúng định dạng và không chứa nội dung độc hại trước khi API xử lý.

- Có cơ chế xác minh tính hợp lệ của JSON Web Tokens (JWT) nhằm đảm bảo rằng các yêu cầu API hoặc phiên làm việc được xác thực và bảo mật.
- Có chức năng phân tích request để phát hiện và ngăn chặn các hành vi bất thường sử dụng Machine learning - Sequence Analytics, Sequence Mitigation.
- Hỗ trợ API Schema Validation (kiểm tra định dạng dữ liệu theo OpenAPI/Swagger) để kiểm tra các API hợp lệ.

2.6. Yêu cầu về quản trị, giám sát

- Cho phép quản trị thông qua giao diện Web User Interface, API.
- Cho phép cấu hình cảnh báo qua email.
- Cho phép thực hiện tạo báo cáo có khả năng tùy chỉnh nội dung theo nhu cầu, có sẵn các báo cáo mẫu và có thể trích xuất.
- Cho phép xem và tải về các báo cáo về tuân thủ OWASP, PCI-DSS cùng với chi tiết các bước cần thực hiện trong trường hợp chưa tuân thủ.
- Có thể đặt lịch gửi báo cáo tự động qua email.
- Có chức năng phân quyền quản trị theo chức năng nhiệm vụ của nhân viên (role-based access control). xác thực 2 lớp (2FA).
- Các log, cảnh báo của hệ thống được thu thập đầy đủ về hệ thống SIEM của SHB (Sử dụng IBM Qradar).
- Hỗ trợ tạo báo cáo giám sát theo các thông số:Time range, IP address, Attack type, Location…
- Có chức năng sao lưu, phục hồi cấu hình hệ thống.
- 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 ghi nhật ký và trích xuất nhật ký các hành động của người dùng theo thời gian.
- Có khả năng phát hiện các sự kiện bảo mật và cảnh báo theo thời gian thực.
- Cho phép ẩn các dữ liệu nhạy cảm như số tài khoản, mã PIN, mật khẩu, số thẻ, … trong phần nhật ký log để tránh lộ lọt thông tin.
- Ghi log đầy đủ request/response, headers (phục vụ điều tra sự cố, phân tích hành vi).
- Hỗ trợ lưu trữ log với thời gian tối thiểu 30 ngày.

3. Yêu cầu về triển khai

- Hệ thống được triển khai và bàn giao theo phương thức trọn gói. Vì vậy, nhà thầu đóng vai trò tích hợp hệ thống, chủ trì và phối hợp với các hãng sản xuất liên quan tới các sản phẩm trong gói thầu để thực hiện cài đặt, cấu hình, thiết lập tham số, tinh chỉnh theo đúng kiến trúc hệ thống đảm bảo đáp ứng các yêu cầu của SHB đưa ra. Đề nghị Nhà thầu cung cấp thư Cam kết đáp ứng yêu cầu này trong trường hợp có đáp ứng.
- Thời gian triển khai: 04 tháng kể từ khi ký hợp đồng.

- Nhà thầu cần nêu rõ về sự tham gia của nhân sự mỗi bên (nhân sự của Hãng cung cấp giải pháp, nhân sự của nhà phân phối giải pháp, nhân sự đối tác của Hãng tại Việt Nam, nhân sự kỹ thuật của SHB, trong bản kế hoạch đệ trình trong HSDT. Trong đó, Nhà thầu làm rõ kế hoạch và hình thức làm việc của nhân sự tại các giai đoạn.
- Trong HSDT, Nhà thầu cung cấp chi tiết phương pháp luận triển khai, kế hoạch triển khai tổng thể và chi tiết theo từng giai đoạn (giai đoạn thiết kế, giai đoạn triển khai, cài đặt, tích hợp). Kế hoạch của Nhà thầu phải bao gồm tối thiểu các hạng mục sau: kế hoạch đặt hàng, cấu hình, tích hợp, thử nghiệm, tối ưu hóa hệ thống, triển khai, nghiệm thu đáp ứng đúng các tiến độ do SHB đưa ra. Việc triển khai có thể tiến hành theo từng cấu phần để đảm bảo đáp ứng yêu cầu về tiến độ và chất lượng triển khai dự án. Khuyến khích Nhà thầu trình bầy chi tiết và mở rộng các yêu cầu, khuyến cáo về triển khai để chứng minh kinh nghiệm và năng lực của Nhà thầu.
- Nhà thầu đề xuất số lượng ứng dụng sẽ thực hiện triển khai Giải pháp tường lửa ứng dụng web (WAF) và phòng chống tấn công DDOS (Anti DDoS), đảm bảo tối thiểu 05 ứng dụng của SHB sẽ được triển khai WAF và Anti DDoS.

4. Yêu cầu dịch vụ hỗ trợ kỹ thuật chính hãng

- Nhà thầu cung cấp cam kết chất lượng dịch vụ hỗ trợ kỹ thuật chính hãng (SLA) bao gồm ngưỡng leo thang và thời gian xử lý.
- Nhà thầu phải cung cấp dịch vụ hỗ trợ kỹ thuật 24/7 theo đúng tiêu chuẩn chính hãng hiện hành.
- Trường hợp SHB cần hỗ trợ liên quan đến các tấn công vào hệ thống của SHB, nhà cung cấp dịch vụ (kỹ sư hỗ trợ) phải có phản hồi chậm nhất 01h kể từ khi nhận được yêu cầu hỗ trợ của SHB.
- Có kênh liên lạc hỗ trợ bằng điện thoại, email. Cung cấp thời gian cam kết phản hồi, xử lý, hỗ trợ thông tin của hãng nếu có giải pháp triển khai thêm mới trên hạ tầng của SHB.
- Kỹ sư của hãng, hoặc kỹ sư của nhà thầu được chứng thực bởi hãng phải có mặt tại địa điểm của SHB trong vòng 01h (một giờ) sau khi nhận được thông báo và yêu cầu về việc khắc phục, xử ly sự cố. Trong vòng 04h (bốn giờ) từ thời điểm có mặt tại địa điểm của SHB phải đề xuất được giải pháp khả thi để khắc phục sự cố và hoàn thành thực hiện theo giai pháp được sự đồng ý của SHB.
- Trường hợp có sự cố từ phía nhà cung cấp dịch vụ gây gián đoạn dịch vụ, nhà cung cấp phải đảm bảo chủ động thông báo cho SHB chậm nhất 15 phút sau khi sự cố xảy ra và tham gia xử lý sự cố.
- Hỗ trợ khách hàng tối ưu hóa hệ thống và triển khai cho hệ thống mới khi có yêu cầu.

5. Yêu cầu về nhân sự

5.1. **Yêu cầu về nhân sự quản lý dự án:**

- Số lượng: 01 người.
- Tốt nghiệp đại học chuyên ngành Công nghệ thông tin hoặc tương đương.

- Có tối thiểu 03 năm kinh nghiệm làm quản trị dự án.
- Có kinh nghiệm quản trị ít nhất 02 dự án triển khai về bảo mật.
- Có một trong các chứng chỉ về quản trị dự án: PMP® hoặc PRINCE2.
- Cung cấp thông tin về bằng cấp, chứng chỉ liên quan của các cán bộ thực hiện vị trí này.

5.2. Yêu cầu về nhân sự triển khai, tích hợp

- Số lượng tối thiểu: 02 người.
- Tất cả nhân sự có kinh nghiệm triển khai thành công giải pháp của nhà cung cấp được nhà thầu chào trong gói thầu này.
- Tất cả nhân sự tốt nghiệp đại học chuyên ngành Công nghệ thông tin hoặc tương đương.
- Tất cả nhân sự có chứng chỉ chuyên môn được cấp từ hãng hãng về giải pháp đề xuất triển khai.
- Cung cấp thông tin về bằng cấp, chứng chỉ, kinh nghiệm liên quan của các cán bộ thực hiện vị trí này.

5.3. Yêu cầu về nhân sự hỗ trợ kỹ thuật

- Số lượng tối thiểu: 02 người.
- Tất cả nhân sự tốt nghiệp đại học chuyên ngành Công nghệ thông tin hoặc tương đương.
- Tất cả nhân sự có chứng chỉ chuyên môn được cấp từ hãng hãng về giải pháp đề xuất triển khai.
- Tất cả nhân sự có kinh nghiệm cung cấp dịch vụ của nhà cung cấp được nhà thầu chào trong gói thầu này với vai trò nhân sự hỗ trợ kỹ thuật.
- Mô tả thành tích, kinh nghiệm, chứng chỉ trong lĩnh vực an toàn thông tin (có cung cấp thông tin chi tiết về bằng cấp, chứng chỉ, kinh nghiệm).

6. Yêu cầu về tài liệu

Nhà thầu phải xây dựng và cung cấp tối thiểu các loại tài liệu sau:

- Kế hoạch triển khai chi tiết.
- Quy trình triển khai.
- Tài liệu kiến trúc và thiết kế hệ thống.
- Tài liệu kỹ thuật chi tiết về cài đặt, cấu hình hệ thống.
- Kịch bản kiểm thử hệ thống.
- Tài liệu mô tả các quy trình và hướng dẫn vận hành hệ thống.
- Tài liệu phân quyền quản trị và người sử dụng hệ thống.
- Các giấy phép chứng nhận.
- Các tài liệu khác theo chính sách, quy trình của SHB.

PHẦN III.
YÊU CẦU VỀ TÀI CHÍNH THƯƠNG MẠI

1. Yêu cầu về thương mại

1.1. Đồng tiền chào giá: Việt Nam đồng.

1.2. Đồng tiền thanh toán: Việt Nam đồng.

1.3. Phương thức thanh toán: Chuyển khoản vào tài khoản của nhà thầu (nhà thầu mở tài khoản tại SHB).

1.4. Điều kiện thanh toán

-Bên mua tạm ứng cho bên bán 30% giá trị hợp đồng kể từ ngày 2 bên ký hợp đồng và cung cấp cho bên bán hồ sơ sau :

Bảo lãnh tạm ứng bằng giá trị tạm ứng (nếu nhà thầu thực hiện tạm ứng)

Bảo đảm thực hiện hợp đồng có giá trị bằng 10% tổng giá trị hợp đồng.

Đề nghị tạm ứng.

-Bên Mua thanh toán cho Bên Bán 100 % (có khấu trừ 30% giá trị tạm ứng) tổng giá trị hợp đồng trong vòng 07 (bảy) kể từ ngày Bên Bán bàn giao cho bên mua các giấy tờ, tài liệu sau:

Biên bản nghiệm thu tổng thể;

Giấy đề nghị thanh toán;

Hóa đơn tài chính hợp lệ.

Các giấy tờ tài liệu liên quan khác (nếu có)

2. Bảng chào giá chi tiết

Nhà thầu trình bày bảng chào giá chi tiết như sau

STT	Tên hàng hóa	ĐVT	SL	Đơn giá VNĐ	Thành tiền VNĐ
1	Cung cấp bản quyền giải pháp tường lửa ứng dụng web và phòng chống tấn công DDoS điện toán đám mây để bảo vệ cho các ứng dụng của SHB trong 01 năm	License/ năm	01		
2	Dịch vụ triển khai, cài đặt, cấu hình giải pháp và tích hợp giải pháp để bảo vệ cho các ứng dụng của SHB tại Onprem và Cloud	Gói	01		
3	Dịch vụ hỗ trợ kỹ thuật 24x7 theo tiêu chuẩn của hãng đối với giải pháp do nhà thầu cung cấp trong 01 năm	Gói	01		
Cộng					

STT	Tên hàng hóa	ĐVT	SL	Đơn giá VNĐ	Thành tiền VNĐ
Thuế VAT					
Thành tiền bao gồm VAT					

3. Điều kiện xem xét lựa chọn nhà thầu

Nhà thầu được xem xét lựa chọn là đơn vị cung cấp khi đáp ứng các yêu cầu sau:

-Đáp ứng yêu cầu về năng lực kinh nghiệm, kỹ thuật.

-Có giá chào thấp nhất.

NGÂN HÀNG TMCP SÀI GÒN – HÀ NỘI

M.S.D.N: 1800278630 - C.T.C.P
NGÂN HÀNG THƯƠNG MẠI CỔ PHẦN SÀI GÒN - HÀ NỘI
Q. HOÀN KIẾM - TP. HÀ NỘI

Đào Ngọc Dũng

BẢNG CHẤM NĂNG LỰC KINH NGHIỆM

STT	NỘI DUNG	YÊU CẦU CỤ THỂ	ĐIỂM TỐI ĐA	ĐIỂM TỐI THIỂU
1	Đơn chào hàng	Phải có chữ ký của người đại diện theo pháp luật của công ty hoặc người được ủy quyền (Có giấy ủy quyền kèm theo)	5	5
2	Bảng chào giá chi tiết	Chào đầy đủ số lượng, chủng loại, giá trước VAT, giá sau VAT…	5	5
3	Hiệu lực của Hồ sơ chào hàng	Tối thiểu 60 ngày kể từ thời điểm hết hạn nộp hồ sơ chào hàng	5	5
4	Kinh nghiệm	Đơn vị phải có tối thiểu 03 năm kinh nghiệm trong lĩnh vực cung cấp các giải pháp phần mềm công nghệ thông tin.	5	5
5	Hợp đồng tương tự	Đơn vị có 02 hợp đồng tương tự cung cấp giải pháp phần mềm công nghệ thông tin cho hệ thống công nghệ thông tin của ngân hàng bất kỳ có giá trị từ 02 tỷ đồng trở lên kèm hóa đơn VAT và Biên bản nghiệm thu hoặc biên bản bàn giao hoặc thanh lý hợp đồng.	**30**	
	Có từ 3 hợp đồng trở lên		30	
	Có 2 hợp đồng		20	20
	Có 1 hợp đồng		10	
	Không có hợp đồng		0	
6	Thư hỗ trợ của hãng	Đơn vị phải có thư hỗ trợ của hãng, thư nhà phân phối chính hãng, đại lý chính hãng.	20	20
7	Đội ngũ nhân sự triển khai	Cung cấp danh sách cán bộ kỹ thuật triển khai kèm bằng cấp chứng chỉ liên quan.	10	10
8	Tình hình tài chính	Báo cáo tài chính 02 năm gần nhất kiểm toán hoặc bản nộp qua cổng thông tin điện tử đảm bảo doanh thu bình quân từ 30 tỷ trở lên và có lãi.	10	5

STT	NỘI DUNG	YÊU CẦU CỤ THỂ	ĐIỂM TỐI ĐA	ĐIỂM TỐI THIỂU
9	Các cam kết	Cam kết chấp nhận yêu cầu về kỹ thuật, chất lượng, theo yêu cầu tại Phần II của Hồ sơ yêu cầu chào hàng Cam kết chấp nhận yêu cầu về điều kiện tài chính thương mại theo yêu cầu tại Phần III của Hồ sơ yêu cầu chào hàng.	10	10
	Tổng cộng		**100**	**85**

Nhà thầu được đánh giá đáp ứng năng lực kinh nghiệm khi tổng điểm đánh giá tối thiểu đạt 85 điểm và phải đáp ứng các yêu cầu điểm tối thiểu của bảng trên.

BẢNG CHẤM KỸ THUẬT

STT	NỘI DUNG YÊU CẦU	M/O	ĐIỂM TỐI THIỂU	ĐIỂM TỐI ĐA
A. YÊU CẦU CHUNG VỀ GIẢI PHÁP				
1	Nhà thầu phải đề xuất và cung cấp giải pháp thuộc một trong ba nhà cung cấp: Akamai, Cloudflare hoặc Imperva.	M	10	10
2	Giải pháp tường lửa ứng dụng web (WAF) và phòng chống tấn công DDOS (Anti DDoS) được cung cấp dịch vụ trên cùng một nền tảng Cloud	M	10	10
3	Giải pháp tường lửa ứng dụng web (WAF) và phòng chống tấn công DDOS (Anti DDoS) hỗ trợ bảo vệ đa nền tảng On-premise và Public Cloud. Nhà thầu đề xuất mô hình triển khai chi tiết.	M	10	20
4	Giải pháp đã triển khai thành công cho khách hàng khối Ngân hàng tại Việt Nam (nhà thầu nêu cụ thể các Ngân hàng đã sử dụng)	M	10	20
5	Giải pháp có tối thiểu 06 điểm hiện diện (PoP), được đặt tại tối thiểu ba thành phố lớn tại Việt Nam: Hà Nội, Đà Nẵng và Thành phố Hồ Chí Minh. Các PoP này là các PoP xử lý (processing PoP), có khả năng thực hiện các chức năng tính toán như kiểm tra bảo mật, xử lý WAF, caching, lọc bot, và tối ưu hiệu suất truy cập, không chỉ là các node chuyển tiếp, mạng hoặc edge node thụ động	M	10	20
6	Hạ tầng PoP được triển khai trên nhiều nước khác nhau ngoài Việt Nam, tối thiểu bao gồm các quốc gia sau: Singapore, Hong Kong, Châu Âu, Mỹ nhằm đảm bảo khả năng phòng chống tấn công DDoS và đảm bảo khả năng sẵn sàng truy cập từ các quốc gia ngoài Việt Nam.	M	10	20
7	Hỗ trợ môi trường Staging/UAT nhằm kiểm tra toàn bộ các các cấu hình bao gồm cấu hình WAF, DDoS, BOT mà không làm ảnh hưởng tới lưu lượng người dùng thực tế	M	10	10
8	Giải pháp phải tính phí theo top level domain, unlimited subdomain	M	10	10
9	Hỗ trợ Machine Learning hoặc Behavior Analysis để phát hiện tấn công bất thường.	M	10	10
10	Cam kết về uptime dịch vụ của nhà cung cấp: Tối thiểu từ 99% trở lên	M	10	10
11	Có tích hợp công nghệ AI, ưu tiên các mô hình ngôn ngữ lớn như GPT, nhằm hỗ trợ quản trị viên trong việc phân tích log và sự kiện, điều tra sự cố bảo mật, và gợi ý việc xây dựng các rule, policy hoặc cảnh báo tùy chỉnh.	O	0	10
12	Có khả năng tương tác tự nhiên với người dùng thông qua giao diện chat bằng ngôn ngữ tự nhiên, có khả năng tóm tắt và giải thích ý nghĩa, mục đích và tác dụng của các rule hiện có nhằm giúp quản trị viên hiểu rõ và tối ưu cấu hình hệ thống.	O	0	10
13	Đảm bảo lưu lượng xử lý tối thiểu mỗi tháng: Bản quyền giải pháp chào thầu đảm bảo khả năng xử lý tối thiểu 400 triệu request mỗi tháng và lưu lượng truyền tải từ mạng của nhà cung cấp tối thiểu 23 TB mỗi tháng, với độ ổn định cao và không làm suy giảm hiệu suất dịch vụ.	M	50	70
14	Cho phép SHB tải lên và quản lý tối thiểu 40 chứng chỉ SSL riêng biệt, phục vụ cho nhiều tên miền hoặc ứng dụng khác nhau trong cùng một hệ thống.	M	20	30
B. YÊU CẦU VỀ TÍNH NĂNG VÀ KHẢ NĂNG CỦA GIẢI PHÁP				

STT	NỘI DUNG YÊU CẦU	M/O	ĐIỂM TỐI THIỂU	ĐIỂM TỐI ĐA
1	Yêu cầu về kiểm soát truy cập dựa trên địa chỉ nguồn (IP/Domain), quốc gia, vùng miền địa lý (Geolocation)			
1.1	Có chức năng thiết lập danh sách các vùng miền địa lý, quốc gia được phép hoặc không được phép truy cập (cho phép/ từ chối theo IP, dải IP, quốc gia, geolocation, URI, ...)	M	5	5
1.2	IP Reputation dựa trên việc phân loại địa chỉ IP nguồn kết nối như Tor, Phishing, Proxy, Botnet	M	5	5
2	Yêu cầu về Bot management			
2.1	Nhà cung cấp cung cấp khả năng phát hiện, phân loại và giảm thiểu lưu lượng truy cập bot tự động	M	5	5
2.2	Người dùng có thể tạo các quy tắc tùy chỉnh để thực hiện các hành động cụ thể bao gồm ngăn chặn, ghi log	M	5	5
2.3	Nhà cung cấp có khả năng xác định các bot uy tín đã được công nhận bằng cách sử dụng cơ sở dữ liệu chữ ký được cập nhật tự động lên các bot uy tín mới	M	5	5
2.4	Nhà cung cấp cung cấp một cơ chế để đưa một đoạn mã Javascript vào trình duyệt để giúp xác định bot	M	5	5
2.5	Số lượng loại BOT có thể nhận dạng và phản hồi tối thiểu 100 loại	M	5	5
2.6	Có khả năng nhận diện các loại Bot giả mạo browser	M	5	5
3	Yêu cầu phòng chống tấn công từ chối dịch vụ DDOS			
3.1	Cho phép phòng chống DOS/DDoS không giới hạn bất kể số lần, kích thước hoặc thời lượng tấn công mà không tính thêm phí	M	5	5
3.2	Hỗ trợ phát hiện và ngăn chặn các cuộc tấn công Zero-day và DDOS attack	M	5	5
3.3	Phát hiện và chặn các hình thức tấn công từ chối dịch vụ thông dụng từ L3-L7	M	5	5
3.4	Có khả năng chống DDoS Layer 4 tại từng PoP trên toàn cầu mà không cần chuyển về các trung tâm chống DDoS tập trung gây thêm độ trễ.	M	5	5
3.5	Giải pháp cung cấp tối thiểu 100 Tbps thông lượng toàn cầu để chống tấn công DDoS, đảm bảo khả năng xử lý các cuộc tấn công có quy mô cực lớn và đa dạng hình thức mà không ảnh hưởng đến hiệu suất truy cập của người dùng hợp lệ. Việc ngăn chặn DDoS được thực hiện ngay tại PoP nhận traffic, mà không cần chuyển tiếp đến scrubbing center hoặc các PoP xử lý trung gian.	M	5	20
3.6	Có khả năng tự động phát hiện và phản ứng với các cuộc tấn công DDoS trong thời gian không quá 03 giây kể từ khi tấn công được xác định, mà không cần sự can thiệp thủ công của người quản trị.	M	10	10
3.7	Có tính năng ngăn chặn tấn công từ chối dịch vụ xuất phát từ các mạng botnet	M	5	5
3.8	Khả năng chọn lọc lưu lượng tấn công: + Đảm bảo khả năng phát hiện và chọn lọc lưu lượng tấn công tối thiểu 80%. + Đảm bảo khả năng bảo vệ lưu lượng sạch tối thiểu 85%.	M	5	5

STT	NỘI DUNG YÊU CẦU	M/O	ĐIỂM TỐI THIỂU	ĐIỂM TỐI ĐA
3.9	Giám sát và phân tích sự cố tấn công DDoS: + Cho phép giám sát băng thông theo địa chỉ IP và dải mạng phục vụ phân tích tấn công; + Cho phép giám sát theo dõi hiệu quả chặn lọc thông qua lưu lượng bằng thông trước và sau khi đi qua bộ lọc. + Cho phép giám sát thông tin các cuộc tấn công xảy ra theo thời gian thực và tìm kiếm trong các cuộc tấn công đã xảy ra;	M	5	5
3.10	Có thể ngăn chặn các hình thức tấn công từ chối dịch vụ (bao gồm tối thiểu nhưng không giới hạn): + Tấn công làm tràn ngập băng thông: UDP reflection (DNS, NTP amplification, SSDP attack, Chargen attack), IP fragment, ICMP flood và các dạng tấn công tương tự; + Tấn công cạn kiệt tài nguyên qua giao thức TCP: SYN flood, ACK flood, RST flood, SYN-ACK flood và các dạng tấn công tương tự; + Tấn công sử dụng gói tin không hợp lệ: malformed, invalid packet; + Tấn công gửi gói tin yêu cầu với tần suất cao, đột ngột; + Tấn công qua phân tích hành vi người dùng:HTTP page flood, DNS flood, brute force;	M	10	10
3.11	Có khả năng đếm số request theo các thông tin nâng cao, ít nhất phải hỗ trợ các trường sau: IP nguồn, quốc gia, user agent, HTTP methods, cookies, URI path, …	M	5	5
3.12	Có tính năng cho phép người dùng lựa chọn chủ động các nguồn lưu lượng để ngăn chặn khi lượng request rate gần tới ngưỡng cấu hình và hỗ trợ cấu hình bảo vệ rate limiting đến từng path trên URL hoặc API endpoint.	M	5	5
4	Yêu cầu tính năng lường lửa ứng dụng web (WAF)			
4.1	Cho phép tạo mới, chỉnh sửa các chính sách bảo vệ và hỗ trợ bộ lọc để tìm kiếm. Ngoài ra có thể bật, tắt, xóa, nhân bản các chính sách bảo vệ	M	5	5
4.2	Cho phép người dùng tự viết Rule phục vụ việc phát hiện và ngăn chặn các cuộc tấn công theo các tham số: - Request method - Request URI - Query string - Protocol (name and version) - Header name - Header value - Request body - Cookie name - Cookie value Các thuộc tính tùy chỉnh trong rule có thể được thiết lập bằng: - Value - Range value - Regular expression.	M	5	10
4.3	Hỗ trợ việc giải mã các truy cập Web qua SSL/TLS (HTTPS)	M	5	5
4.4	Hỗ trợ giao thức HTTP/2 và HTTP/3, QUIC	M	5	5
4.5	Hỗ trợ SSL/TLS version 1.2, version 1.3	M	5	5
4.6	Cho phép cấu hình tính năng rewrite hoặc redirect trong các request và respond (Ví dụ: Khi phản hồi ra chèn thêm cookie vào bản tin respond).	M	5	5

STT	NỘI DUNG YÊU CẦU	M/O	ĐIỂM TỐI THIỂU	ĐIỂM TỐI ĐA
4.7	Có khả năng phát hiện và bảo vệ ứng dụng khỏi các cuộc tấn công khai thác lỗ hổng bảo mật ứng dụng web thuộc Top 10 OWASP: - A01: Broken Access Control: + Cross-Site Request Forgery (CSRF) + URL Redirection to Untrusted Site ('Open Redirect') + Missing Authentication for Critical Function + Missing Authorization, Incorrect Authorization + Incorrect Permission Assignment for Critical Resource + Unvalidated Redirects and Forwards - A02: Cryptographic Failures (Sensitive Data Exposure) - A03: Injection: bao gồm nhưng không giới hạn: SQL injection, Command injection, Shell injection, LDAP injection, XPath injection, XML injection, XXE, Expression language injection, Code injection, NoSQL injection, SSTI, HTML injection, CRLF injection, Remote File Inclusion (RFI), Xquery Injection, Cross-Site Scripting (XSS). Uncontrolled Format String. - A04: Insecure Design: + Insecure Direct Object References + Use of Potentially Dangerous Function + Incorrect Calculation of Buffer Size + Integer Overflow or Wraparound + Reliance on Untrusted Inputs in a Security Decision + Use of a Broken or Risky Cryptographic Algorithm + Use of Hard-coded Credentials - A05: Security Misconfiguration: + WSDL Enumeration + Unrestricted Upload of File with Dangerous Type + Inclusion of Functionality from Untrusted Control Sphere + Execution with Unnecessary Privileges + Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') - A06: Vulnerable and Outdated Componentes: Using Known Vulnerable Components - A07: Identification and Authentication Failures - A08: Software and Data integrity failures - A09: Security logging and Monitoring failures - A10: Server-side request forgery (SSRF)	M	10	10
4.8	Có khả năng chặn lọc các loại file không được cho phép	M	5	5
4.9	Giải pháp đi kèm nguồn thông tin tình báo về các mối nguy hại được cập nhật thường xuyên giúp nâng cao khả năng bảo vệ với các mối nguy hại mới	M	5	5
4.10	Có chức năng phát hiện và ngăn chặn, giảm thiểu mức độ ảnh hưởng của các hình thức tấn công từ chối dịch vụ lớp ứng dụng (Layer-7 DoS attack), bao gồm: - Buffer Overflow attack - HTTP flood - Slowloris	M	5	5
4.11	Giải pháp có tính năng tự động cập nhật các chính sách WAF mới nhất	M	5	5

STT	NỘI DUNG YÊU CẦU	M/O	ĐIỂM TỐI THIỂU	ĐIỂM TỐI ĐA
4.12	Cung cấp khả năng tự động phân tích và đưa ra khuyến cáo WAF rule cho quản trị viên	M	5	10
4.13	Các bộ quy tắc được cập nhật tự động và thường xuyên để đối phó với các cuộc tấn công mới.	M	5	10
4.14	Có tính năng chặn/cho phép IP, dải mạng, hoặc vùng miền địa lý	M	5	5
4.15	Có chức năng tự động phát hiện và ngăn chặn các hình thức tấn công dò tìm mật khẩu (brute-force, credential stuffing) các trang đăng nhập của ứng dụng.	M	5	5
4.16	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).	M	5	5
4.17	Cho phép mã hoá các trường thông tin nhạy cảm (sensitive fields) ở phía Client Side (Browser), hỗ trợ HTML Field Obfuscation, Identify Stolen Credentials, và Full AJAX Encryption	M	5	10
4.18	Cung cấp các phương pháp bảo vệ cookie và session: - cookie injection - cookie tampering - session hijacking - session fixation	M	5	5
4.19	Giải pháp phải có khả năng bảo vệ chống lại các bot thực hiện các hành động sau: - Site Scraping - Vulnerability scanning - Comment spamming	M	5	5
4.20	Có chức năng tự động yêu cầu xác thực challenge-response (như CAPTCHA) để ngăn chặn các công cụ duyệt web tự động và xác thực người dùng khi nghi ngờ.	M	5	5
5	Yêu cầu về tính năng API Security			
5.1	Có khả năng tự động phát hiện và phân loại các kết nối API đang hoạt động trên hệ thống (API Discovery)	M	10	10
5.2	Có khả năng ngăn chặn lại các tấn công DoS vào các kết nối API	M	10	10
5.3	Có khả năng tạo các chính sách Rate limiting cho các request API	M	5	10
5.4	Có chức năng xác thực 2 chiều giữa client và server (Mutual TLS) và quản lý xác thực chứng chỉ số	M	5	10
5.5	Có cơ chế kiểm tra và xác thực dữ liệu của URL và tham số truyền vào API nhằm đảm bảo dữ liệu hợp lệ, đúng định dạng và không chứa nội dung độc hại trước khi API xử lý	M	5	10
5.6	Có cơ chế xác minh tính hợp lệ của JSON Web Tokens (JWT) nhằm đảm bảo rằng các yêu cầu API hoặc phiên làm việc được xác thực và bảo mật	M	5	10
5.7	Có chức năng phân tích request để phát hiện và ngăn chặn các hành vi bất thường sử dụng Machine learning - Sequence Analytics, Sequence Mitigation	M	5	10
5.8	Hỗ trợ API Schema Validation (kiểm tra định dạng dữ liệu theo OpenAPI/Swagger) để kiểm tra các API hợp lệ	M	5	10
6	Yêu cầu về quản trị, giám sát			

STT	NỘI DUNG YÊU CẦU	M/O	ĐIỂM TỐI THIỂU	ĐIỂM TỐI ĐA
6.1	Cho phép quản trị thông qua giao diện Web User Interface, API	M	5	5
6.2	Cho phép cấu hình cảnh báo qua email	M	5	5
6.3	Cho phép thực hiện tạo báo cáo có khả năng tùy chỉnh nội dung theo nhu cầu, có sẵn các báo cáo mẫu và có thể trích xuất	M	5	5
6.4	Cho phép xem và tải về các báo cáo về tuân thủ OWASP, PCI-DSS cùng với chi tiết các bước cần thực hiện trong trường hợp chưa tuân thủ.	O	0	5
6.5	Có thể đặt lịch gửi báo cáo tự động qua email	M	5	5
6.6	Có chức năng phân quyền quản trị theo chức năng nhiệm vụ của nhân viên (role-based access control). xác thực 2 lớp (2FA)	M	5	5
6.7	Các log, cảnh báo của hệ thống được thu thập đầy đủ về hệ thống SIEM của SHB (Sử dụng IBM Qradar).	M	5	5
6.8	Hỗ trợ tạo báo cáo giám sát theo các thông số:Time range, IP address, Attack type, Location…	M	5	5
6.9	Có chức năng sao lưu, phục hồi cấu hình hệ thống.	M	5	5
6.10	Có sẵn các mẫu chính sách bảo mật (policy templates) giúp quản trị viên tạo các chính sách bảo mật dễ dàng, nhanh chóng.	M	5	5
6.11	Có chức năng ghi nhật ký và trích xuất nhật ký các hành động của người dùng theo thời gian.	M	5	5
6.12	Có khả năng phát hiện các sự kiện bảo mật và cảnh báo theo thời gian thực.	M	5	5
6.13	Cho phép ẩn các dữ liệu nhạy cảm như số tài khoản, mã PIN, mật khẩu, số thẻ, … trong phần nhật ký log để tránh lộ lọt thông tin.	M	5	5
6.14	Ghi log đầy đủ request/response, headers (phục vụ điều tra sự cố, phân tích hành vi)	M	5	5
6.15	Hỗ trợ lưu trữ log với thời gian tối thiểu 30 ngày	M	5	5
C. YÊU CẦU VỀ TRIỂN KHAI				
1	Hệ thống được triển khai và bàn giao theo phương thức trọn gói. Vì vậy, nhà thầu đóng vai trò tích hợp hệ thống, chủ trì và phối hợp với các hãng sản xuất liên quan tới các sản phẩm trong gói thầu để thực hiện cài đặt, cấu hình, thiết lập tham số, tinh chỉnh theo đúng kiến trúc hệ thống đảm bảo đáp ứng các yêu cầu của SHB đưa ra. Đề nghị Nhà thầu cung cấp thư Cam kết đáp ứng yêu cầu này trong trường hợp có đáp ứng.	M	10	10
2	Thời gian triển khai: 04 tháng kể từ khi ký hợp đồng.	M	10	10
3	Nhà thầu cần nêu rõ về sự tham gia của nhân sự mỗi bên (nhân sự của Hãng cung cấp giải pháp, nhân sự của nhà phân phối giải pháp, nhân sự đối tác của Hãng tại Việt Nam, nhân sự kỹ thuật của SHB, trong bản kế hoạch đệ trình trong HSDT. Trong đó, Nhà thầu làm rõ kế hoạch và hình thức làm việc của nhân sự tại các giai đoạn.	M	10	10
4	Trong HSDT, Nhà thầu cung cấp chi tiết phương pháp luận triển khai, kế hoạch triển khai tổng thể và chi tiết theo từng giai đoạn (giai đoạn thiết kế, giai đoạn triển khai, cài đặt, tích hợp). Kế hoạch của Nhà thầu phải bao gồm tối thiểu các hạng mục sau: kế hoạch đặt hàng, cấu hình, tích hợp, thử nghiệm, tối ưu hóa hệ thống, triển khai, nghiệm thu đáp ứng đúng các tiến độ do SHB đưa ra. Việc triển khai có thể tiến hành theo từng cấu phần để đảm bảo đáp ứng yêu cầu về tiến độ và chất lượng triển khai dự án. Khuyến khích Nhà thầu trình bầy chi tiết và mở rộng các yêu cầu, khuyến cáo về triển khai để chứng minh kinh nghiệm và năng lực của Nhà thầu.	M	10	10

STT	NỘI DUNG YÊU CẦU	M/O	ĐIỂM TỐI THIỂU	ĐIỂM TỐI ĐA
5	Nhà thầu đề xuất số lượng ứng dụng sẽ thực hiện triển khai Giải pháp tường lửa ứng dụng web (WAF) và phòng chống tấn công DDOS (Anti DDoS), đảm bảo tối thiểu 05 ứng dụnjg của SHB sẽ được triển khai WAF và Anti DDoS.	M	50	90
D. YÊU CẦU VỀ HỖ TRỢ KỸ THUẬT				
1	Nhà thầu cung cấp cam kết chất lượng dịch vụ hỗ trợ kỹ thuật chính hãng (SLA) bao gồm ngưỡng leo thang và thời gian xử lý.	M	5	5
2	Nhà thầu phải cung cấp dịch vụ hỗ trợ kỹ thuật 24/7 theo đúng tiêu chuẩn chính hãng hiện hành.	M	5	5
3	Trường hợp SHB cần hỗ trợ liên quan đến các tấn công vào hệ thống của SHB, nhà cung cấp dịch vụ (kỹ sư hỗ trợ) phải có phản hồi chậm nhất 01h kể từ khi nhận được yêu cầu hỗ trợ của SHB.	M	5	5
4	Có kênh liên lạc hỗ trợ bằng điện thoại, email. Cung cấp thời gian cam kết phản hồi, xử lý, hỗ trợ thông tin của hãng nếu có giải pháp triển khai thêm mới trên hạ tầng của SHB.	M	5	5
5	Kỹ sư của hãng, hoặc kỹ sư của nhà thầu được chứng thực bởi hãng phải có mặt tại địa điểm của SHB trong vòng 01h (một giờ) sau khi nhận được thông báo và yêu cầu về việc khắc phục, xử ly sự cố. Trong vòng 04h (bốn giờ) từ thời điểm có mặt tại địa điểm của SHB phải đề xuất được giải pháp khả thi để khắc phục sự cố và hoàn thành thực hiện theo giai pháp được sự đồng ý của SHB.	M	10	10
6	Trường hợp có sự cố từ phía nhà cung cấp dịch vụ gây gián đoạn dịch vụ, nhà cung cấp phải đảm bảo chủ động thông báo cho SHB chậm nhất 15 phút sau khi sự cố xảy ra và tham gia xử lý sự cố	M	10	10
7	Hỗ trợ khách hàng tối ưu hóa hệ thống và triển khai cho hệ thống mới khi có yêu cầu.	M	20	20
E. YÊU CẦU VỀ NHÂN SỰ				
1	Quản lý dự án			
1.1	Số lượng: 01 người.	M	5	5
1.2	Tốt nghiệp đại học chuyên ngành Công nghệ thông tin hoặc tương đương.	M	5	5
1.3	Có tối thiểu 03 năm kinh nghiệm làm quản trị dự án.	M	5	5
1.4	Có kinh nghiệm quản trị ít nhất 02 dự án triển khai về bảo mật.	M	5	5
1.5	Có một trong các chứng chỉ về quản trị dự án: PMP® hoặc PRINCE2.	M	5	5
1.6	Cung cấp thông tin về bằng cấp, chứng chỉ liên quan của các cán bộ thực hiện vị trí này.	M	5	5
2	Nhân sự triển khai, tích hợp			
2.1	Số lượng tối thiểu: 02 người.	M	5	5
2.2	Tất cả nhân sự có kinh nghiệm triển khai thành công giải pháp của nhà cung cấp được nhà thầu chào trong gói thầu này.	M	10	10
2.3	Tất cả nhân sự tốt nghiệp đại học chuyên ngành Công nghệ thông tin hoặc tương đương.	M	5	5
2.4	Tất cả nhân sự có chứng chỉ chuyên môn được cấp từ hãng hãng về giải pháp đề xuất triển khai.	M	10	10
2.5	Cung cấp thông tin về bằng cấp, chứng chỉ, kinh nghiệm liên quan của các cán bộ thực hiện vị trí này.	M	5	5
3	Nhân sự hỗ trợ kỹ thuật			

STT	NỘI DUNG YÊU CẦU	M/O	ĐIỂM TỐI THIỂU	ĐIỂM TỐI ĐA
3.1	Số lượng tối thiểu: 02 người.	M	5	5
3.2	Tất cả nhân sự tốt nghiệp đại học chuyên ngành Công nghệ thông tin hoặc tương đương.	M	5	5
3.3	Tất cả nhân sự có chứng chỉ chuyên môn được cấp từ hãng hãng về giải pháp đề xuất triển khai.	M	10	10
3.4	Tất cả nhân sự có kinh nghiệm cung cấp dịch vụ của nhà cung cấp được nhà thầu chào trong gói thầu này với vai trò nhân sự hỗ trợ kỹ thuật.	M	10	10
3.5	Mô tả thành tích, kinh nghiệm, chứng chỉ trong lĩnh vực an toàn thông tin (có cung cấp thông tin chi tiết về bằng cấp, chứng chỉ, kinh nghiệm)	M	5	5
F. YÊU CẦU VỀ TÀI LIỆU				
	Nhà thầu phải xây dựng và cung cấp tối thiểu các loại tài liệu sau:			
1	- Kế hoạch triển khai chi tiết.	M	5	5
2	- Quy trình triển khai.	M	5	5
3	- Tài liệu kiến trúc và thiết kế hệ thống.	M	5	5
4	- Tài liệu kỹ thuật chi tiết về cài đặt, cấu hình hệ thống.	M	5	5
5	- Kịch bản kiểm thử hệ thống.	M	5	5
6	- Tài liệu mô tả các quy trình và hướng dẫn vận hành hệ thống.	M	5	5
7	- Tài liệu phân quyền quản trị và người sử dụng hệ thống.	M	5	5
8	- Các giấy phép chứng nhận.	M	5	5
9	- Các tài liệu khác theo chính sách, quy trình của SHB	M	5	5
	TỔNG CỘNG		**800**	**1000**

Ghi chú:

- M (Mandatory): Đây là các yêu cầu bắt buộc, nhà thầu phải đáp ứng.

- O (Optional): Đây là các yêu cầu không bắt buộc, nhà thầu có thể có hoặc không. Tuy nhiên, nếu đáp ứng được các tiêu chí này sẽ được cộng điểm hoặc đánh giá cao hơn trong quá trình chấm thầu.

Nhà thầu được đánh giá đáp ứng năng lực kỹ thuật khi tổng điểm đánh giá tối thiểu đạt 800 điểm và đáp ứng tất cả các yêu cầu bắt buộc (M).