

PHẦN 2. YÊU CẦU VỀ KỸ THUẬT
CHƯƠNG V. YÊU CẦU VỀ KỸ THUẬT

I. Yêu cầu chung

- Hạng mục mua sắm:

STT	Hạng mục/cấu phần mua sắm	Số lượng	Đơn vị tính	Mô tả, Ghi chú
1	Thiết bị bảo mật email kèm bảo hành và dịch vụ hỗ trợ kỹ thuật 12 tháng	02	Thiết bị	Thiết bị bảo mật email bao gồm thiết bị và bản quyền tính năng bảo mật email kèm bảo hành và dịch vụ hỗ trợ kỹ thuật 12 tháng.
2	Thiết bị phòng chống tấn công có chủ đích cho email kèm bản quyền tính năng bảo mật và dịch vụ bảo hành, hỗ trợ kỹ thuật 12 tháng	01	Thiết bị	Thiết bị phòng chống tấn công có chủ đích cho email bao gồm thiết bị và bản quyền tính năng phòng chống tấn công có chủ đích kèm bảo hành và dịch vụ hỗ trợ kỹ thuật 12 tháng.

- Thời gian triển khai: 15 tháng kể từ ngày hợp đồng có hiệu lực, bao gồm:

- Thời gian bàn giao, nghiệm thu hàng hóa, triển khai cài đặt, kích hoạt bản quyền là 02 tháng kể từ ngày hợp đồng có hiệu lực.
- Thời gian hiệu lực bản quyền phần mềm, bảo hành và hỗ trợ kỹ thuật là 12 tháng (kể từ ngày nghiệm thu hoàn thành triển khai và kích hoạt bản quyền phần mềm).
- Thời gian nghiệm thu và thanh lý hợp đồng là 01 tháng.

- Địa điểm triển khai: Trung tâm xử lý của BIDV tại Phường Cầu Giấy, Thành phố Hà Nội

II. Yêu cầu đối với thiết bị email gateway

1. Yêu cầu chung

- Có khả năng hoạt động ở các chế độ:

- Gateway
- Mail Server

2. Yêu cầu về tính năng

- Các yêu cầu về hệ thống:

- Quản lý theo 2 chiều In/Out
- Có tính năng Multi Domain
- Có tính năng SMTP Authen qua LDAP, RADIUS
- Email Routing dựa trên LDAP
- Có tính năng bảo mật với các cơ chế: SPF, DKIM

- Các yêu cầu về AntiSpam

- Có tính năng chống Spam
- Phát hiện spam dựa trên danh tiếng của người gửi (Global Sender Reputation)
- Phát hiện email spam và phishing URIs
- Phân tích Bayesian
- Có tính năng Greylisting (kiểm soát các email được gửi tự động, 1 lần từ nguồn gửi)

là spam)

- Phát hiện spam với thuật toán Heuristic
- Tích hợp với third-party spam URI and real-time blacklists (SURBL/RBL)
- PDF Scanning và Image Analysis
- Black/Safe Lists at Global, Domain, và User levels
- Cung cấp tính năng ngăn chặn kẻ tấn công lấy được tài khoản email hợp lệ đang tồn tại trên hệ thống thư điện tử
- Có tính năng nhận diện, ngăn chặn các email kiểu Newsletter
- Các yêu cầu đối với Antivirus
 - Cập nhật database antivirus trên cloud
 - Phát hiện virus dựa trên hành vi Heuristic-based
 - Có tính năng Virus Outbreak
 - Tích hợp được với Cloud và On-premise sandbox
- Các yêu cầu về tính sẵn sàng
 - Có tính năng High Availability (HA): Active-Active/Active-Passive
 - Có tính năng đồng bộ về cấu hình
 - Có tính năng đồng bộ mail queue
 - Cảnh báo và phát hiện thiết bị lỗi
- Các yêu cầu nâng cao
 - Có tính năng mã hóa email (identity-based encryption)
 - Có tính năng URL Click Protect (Rewrite URL để phát hiện các URL độc hại khi gửi vào hệ thống)
 - Có tính năng Impersonation Analysis
 - Có tính năng ngăn chặn tấn công APT thông qua URL hoặc file đính kèm bằng cách tích hợp với thiết bị sandbox.
 - Có tính năng lựa chọn định dạng tệp tin và giới hạn dung lượng tệp tin để gửi đến hệ thống Sandbox để phân tích.
 - Có cơ chế queue mail trong một khoảng thời gian để chờ kết quả phân tích mã độc từ thành phần sandbox.
- Quản trị, báo cáo, ghi nhật ký
 - Cho phép quản trị thông qua: HTTPS, SSH
 - Event Logging
 - Hỗ trợ SNMP
 - Tích hợp được với các hệ thống lưu log tập trung, hệ thống SIEM thông qua Syslog
 - Tích hợp tính năng báo cáo (Reporting)

3. ***Yêu cầu về hiệu năng***

- Tối thiểu 1,8 triệu email/giờ đối với email routing hoặc tối thiểu 26000 user.

4. ***Yêu cầu cấu hình phần cứng***

- Số cổng RJ45: ≥ 4 cổng.
- Số cổng SFP: Tối thiểu 2 x 10GE SFP+ (bao gồm module SFP+ đi kèm).
- Triển khai được ở IPv4 và IPv6.
- Lưu trữ: ≥ 2 TB. Hỗ trợ tối thiểu RAID 1, RAID 5.
- Nguồn: 2 Nguồn.

III. Yêu cầu đối với thiết bị phòng chống tấn công có chủ đích cho email

1. Yêu cầu về cấu hình và năng lực xử lý

- Năng lực xử lý:
 - + Hiệu năng phân tích tập tin đính kèm đáp ứng tối thiểu 1900 tập tin đính kèm/giờ (1.400.000 tập tin/tháng) hoặc đáp ứng tổng lượng email gửi vào tối thiểu 25000 email/giờ (600.000 email/ngày)
 - + Yêu cầu về cấu hình
 - Số cổng RJ45: tối thiểu 4 cổng 10/100/1000 RJ45.
 - Số cổng SFP: Tối thiểu 2 x 10GE SFP+ (bao gồm module SFP+ đi kèm).
 - Nguồn điện: Tối thiểu 2 nguồn redundant.

2. Yêu cầu về bản quyền tính năng bảo mật

- Hình thức bản quyền: bản quyền theo thiết bị (per Device) hoặc theo user (đáp ứng tối thiểu 12.000 user)
- Bản quyền tính năng phòng chống tấn công có chủ đích thời hạn 12 tháng kể từ ngày nghiệm thu hoàn thành triển khai và kích hoạt bản quyền.

3. Yêu cầu về tính năng

- Giải pháp có tính năng phân tích và ngăn chặn các dạng tấn công phishing, mã độc nâng cao, zeroday, mã độc có chủ đích có trong các tập tin / đường link URL đính kèm trong thư điện tử.
- Giải pháp có tính năng phát hiện mã độc dựa theo nhiều môi trường khác nhau, với nhiều phiên bản khác nhau, tối thiểu hỗ trợ nền tảng hệ điều hành Windows.
- Giải pháp có tính năng phát hiện mã độc trong các đường dẫn, file đính kèm được gửi qua email cho người dùng.
- Giải pháp có tính năng phân tích các mối đe dọa trong các tập tin được đặt mật khẩu nhúng trong thư điện tử.
- Giải pháp có chế độ phân tích live mode để tải về các tập tin hoặc các thành phần từ Internet trong quá trình phân tích mã độc (Cho phép xem lại quá trình hoạt động của mã độc, tải gói tin và chụp lại màn hình phân tích).
- Giải pháp tích hợp sẵn các sandbox trên thiết bị để phân tích (on-premise).
- Máy ảo phân tích mã độc được cài đặt hệ điều hành windows 11 hoặc mới hơn, tích hợp sẵn Microsoft Office.
- Giải pháp cung cấp giao diện quản trị Dashboard hiển thị các thông tin tổng hợp số lượng email đã bị chặn, số lượng email có đính kèm mã độc được phát hiện theo thời gian.
- Giải pháp có tính năng phân tích các tập tin đính kèm email như file thực thi, file văn bản, file nén.
- Giải pháp được triển khai ở các chế độ:
 - + Chế độ MTA hoặc tương đương (blocking)
 - + Chế độ BCC (monitor)
 - + Chế độ SPAN/TAP
- Giải pháp có tính năng quản trị trên giao diện Web.
- Giải pháp có tính năng ghi lại nhật ký (log) theo chuẩn syslog.

IV. Yêu cầu triển khai, tích hợp hệ thống và bảo hành

1. Yêu cầu triển khai tích hợp hệ thống

Lắp đặt, triển khai tích hợp và xây dựng cấu hình chính sách bảo mật hệ thống, cụ thể như sau:

- Nhà thầu hỗ trợ triển khai các thiết bị phần cứng do nhà thầu cung cấp theo đúng yêu cầu tính năng kỹ thuật của sản phẩm.
- Nhà thầu chịu trách nhiệm tích hợp giải pháp của nhà thầu với các phần tử tương tác khác trong mạng như Switch, Router, các hệ thống bảo mật khác và với hệ thống email tại BIDV, đảm bảo không phá vỡ cấu trúc hạ tầng mạng LAN, hệ thống kết nối Internet, ứng dụng, với các nội dung:
 - + Khảo sát hiện trạng hệ thống.
 - + Hoàn thành thiết kế kỹ thuật, phương án triển khai chi tiết.
 - + Cài đặt và tích hợp hệ thống.
 - + Thiết lập, tối ưu các chính sách theo yêu cầu của BIDV.
 - + Cập nhật các phiên bản mới nhất của hệ thống
- Địa điểm triển khai, tích hợp hệ thống: Trung tâm xử lý của BIDV tại Phường Cầu Giấy, Thành phố Hà Nội.
- Hướng dẫn vận hành và sử dụng thiết bị trong quá trình cài đặt và tích hợp hệ thống.

2. ***Yêu cầu bảo hành, hỗ trợ kỹ thuật***

- Nhà thầu có trách nhiệm bảo hành, hỗ trợ kỹ thuật đối với tất cả các phần mềm (firmware) và phần cứng được lắp đặt thuộc dự án này.
- Thời hạn bảo hành, hỗ trợ kỹ thuật: Theo tiêu chuẩn của hãng bao gồm cả phần cứng và phần mềm (firmware) nhưng tối thiểu 12 tháng sau khi nghiệm thu hoàn thành triển khai và kích hoạt bản quyền.
- Địa điểm bảo hành: Trung tâm xử lý của BIDV tại Phường Cầu Giấy, Thành phố Hà Nội.
- Quy trình bảo hành: Nhà thầu phải cung cấp tài liệu quy trình bảo hành trong đó mô tả cụ thể các mức dịch vụ được đề xuất trong thời gian thực hiện bảo hành.
- Đội ngũ cán bộ bảo hành: Có danh sách cán bộ tham gia bảo hành.
- Hình thức bảo hành: tại chỗ (On-site) và từ xa (Off-site), phụ thuộc vào mức độ cấp thiết và khẩn cấp của sự việc cần hỗ trợ.
- 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 các nội dung bảo hành, hỗ trợ kỹ thuật đáp ứng theo tiêu chuẩn của hãng (tối thiểu bao gồm thời gian phản hồi đối với sự cố nghiêm trọng là trong vòng 01 giờ kể từ khi nhận được thông báo từ BIDV; hình thức hỗ trợ qua điện thoại, website).
Nhà thầu cam kết cung cấp văn bản xác nhận/thư ủy quyền từ chính hãng sản xuất hoặc đại diện hãng tại Việt Nam về việc mua dịch vụ từ chính hãng trước khi ký hợp đồng.
- Yêu cầu cụ thể về bảo hành, hỗ trợ kỹ thuật.
 - + Hỗ trợ nâng cấp phần mềm, cài đặt bản vá, thiết lập chính sách trên hệ thống phù hợp quy định của BIDV.
 - + Đảm bảo tối ưu hoạt động của hệ thống, tránh những lỗi về phần cứng, phần mềm trong quá trình hoạt động, 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.
 - + Thực hiện nâng cấp miễn phí phiên bản phần mềm, firmware theo khuyến nghị từ

hãng cung cấp, đảm bảo hoạt động đáp ứng các yêu cầu chức năng đã nêu ở trên.

- + Đảm bảo được nâng cấp phiên bản phần mềm (firmware) và bản vá theo khuyến nghị từ hãng cung cấp, đảm bảo phần mềm của hệ thống luôn được cập nhật những mẫu nhận diện email spam, email chứa mã độc mới nhất.
 - + Thực hiện 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.
 - + Thời gian tiếp nhận yêu cầu bảo hành từ 8 giờ đến 21 giờ hàng ngày, kể cả ngày lễ, ngày tết. Các yêu cầu bảo hành sau 21 giờ hàng ngày sẽ được đáp ứng ngay vào sáng ngày hôm sau.
- Yêu cầu về khắc phục sự cố: Thời gian phản hồi tối đa cho các yêu cầu xử lý sự cố:

Cấp độ nghiêm trọng	Mô tả	Thời gian đáp ứng (kể từ thời điểm BIDV thông báo tới nhà thầu)	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	01 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 license 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

- Yêu cầu về thay thế linh kiện, thiết bị phần cứng
 - + Trong trường hợp linh kiện/thiết bị hỏng hóc, nhà thầu phối hợp hãng kiểm tra khắc phục. Sau khi hãng chấp thuận thay thế linh kiện/thiết bị, trong vòng 30 ngày nhà thầu tiếp nhận hàng hóa thay thế từ hãng và bàn giao cho BIDV.
 - + Sau khi bàn giao hàng hóa, trong vòng 7 ngày tiếp theo, nhà thầu có trách nhiệm hỗ trợ BIDV thay thế linh kiện/thiết bị hỏng hóc đảm bảo thiết bị hoạt động ổn định, an toàn và nhận bàn giao thiết bị/linh kiện đã hỏng do BIDV bàn giao lại. Trong thời gian thay thế/sửa chữa linh kiện/thiết bị hỏng, nhà thầu có phương án hỗ trợ BIDV đảm bảo Hệ thống hoạt động an toàn, ổn định (nếu cần).
 - + Tất cả chi phí linh kiện, thiết bị phần cứng thay thế, chi phí vận chuyển và các chi phí phát sinh trong quá trình thực hiện do Nhà thầu chịu, BIDV không phải chịu bất kỳ chi phí nào