Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu

1.1. Giới thiệu chung

- Tên kế hoạch thuê dịch vụ Công nghệ thông tin: Dịch vụ bảo vệ tên miền và phòng chống DDOS giai đoạn 2025-2026;

- Chủ đầu tư: Cục Công nghệ thông tin;

- Tên gói thầu: Kế hoạch thuê dịch vụ CNTT Dịch vụ bảo vệ tên miền và phòng chống tấn công DDOS giai đoạn 2025-2026.

- Nguồn vốn: Kinh phí thường xuyên của Kiểm toán nhà nước.

- Hình thức lựa chọn nhà thầu: Chào hàng cạnh tranh, qua mạng.

- Phương thức đấu thầu: Một giai đoạn, một túi hồ sơ.

- Thời gian bắt đầu tổ chức lựa chọn nhà thầu: Quý IV năm 2025.

- Loại hợp đồng: Trọn gói

- Thời gian thực hiện gói thầu: 12 tháng.

1.2. Phạm vi và quy mô cung cấp dịch vụ của gói thầu

- Cung cấp dịch vụ bảo vệ tên miền và phòng chống Ddos cho 09 phần mềm ứng dụng của Kiểm toán nhà nước trong thời gian 12 tháng với tổng dung lượng 5Tb/ tháng, gồm các dịch vụ sau:

+ Dịch vụ DDoS Protection: Chống lại SYN flood, ACK flood, UDP flood; Chống lại HTTP/HTTPS flood, tấn công low-and-slow; có 3 chế độ bảo vệ để tùy chọn; Giới hạn số lượng và tần suất yêu cầu HTTP; Cấu hình blacklist/whitelist dựa trên IP, HTTP header.

+ Dịch vụ Bot Protection: Phân loại và xử lý bot (bypass bot SEO, chặn bot độc hại); Phát hiện bot qua cookie, JavaScript, hành vi người dùng; Xác minh tính hợp lệ của yêu cầu; Phát hiện bot không xác định và ngăn chặn tấn công bot; Ngăn chặn chiếm đoạt tài khoản qua credential stuffing; Giảm thiểu rủi ro gian lận tài chính.

+ Dịch vụ báo cáo an ninh mạng chuyên sâu: Phân tích log từ WAF, DDoS Protection, Bot Protection bằng cách đẩy log tấn công (Syslog, Splunk) đến SIEM của Kiểm toán nhà nước; cho phép hiển thị thời gian thực thông tin tấn công (xu hướng, chi tiết, loại hình, nguồn); xuất báo cáo bảo mật (tổng quan, phân tích sự cố); cung cấp log chi tiết (IP, tên miền, chính sách kích hoạt) và hỗ trợ KQL để phân tích; báo cáo phân tích bảo mật và đề xuất tối ưu hóa chính sách; hỗ trợ tải log sự cố từ console

- Phạm vi các tên miền cần bảo vệ của Kiểm toán nhà nước

TT	Tên miền	Mô tả
1	sav.gov.vn	Trang Cổng thông tin Kiểm toán nhà nước
2	mail.sav.gov.vn	Trang Thư điện tử
3	sso.sav.gov.vn	Trang đăng nhập tập trung của Kiểm toán nhà nước
4	hoatdongkiemtoan.sav.gov.vn	Trang thông tin hoạt động kiểm toán
5	savic.sav.gov.vn	Trang thông tin của Cục Công nghệ thông tin
6	dangdoanthe.sav.gov.vn	Trang thông tin của Đảng đoàn thể
7	tongkiemtoan.sav.gov.vn	Trang thông tin của Tổng Kiểm toán.
8	congkhaibckt.sav.gov.vn	Trang thông tin công khi báo cáo kiểm toán.
9	ati.sav.gov.vn	Trang thông tin của Trường Đào tạo và Bồi dưỡng nghiệp vụ kiểm toán.

- Địa điểm thực hiện: Trung tâm dữ liệu của Kiểm toán nhà nước.

2. Mục tiêu công việc

Mục tiêu thuê dịch vụ:

- Bảo vệ các tên miền của Kiểm toán nhà nước đang public ra internet khỏi các mối đe dọa, tấn công trên môi trường mạng.

- Đảm bảo tính sẵn sàng và an toàn của các phần mềm ứng dụng thuộc hệ thống thông tin của Kiểm toán nhà nước.

- Cung cấp thông tin phân tích chuyên sâu để hỗ trợ ra quyết định bảo mật cho Kiểm toán nhà nước.

- Đảm bảo việc tuân thủ các quy định pháp luật về an toàn thông tin.

3. Yêu cầu kỹ thuật của gói thầu

3.1. Yêu cầu kỹ thuật, công nghệ:

3.1.1. Dịch vụ DDoS Protection

a. Giảm thiểu DDoS tầng L3/L4

Phạm vi bảo vệ: Ngăn chặn các cuộc tấn công dựa trên lưu lượng lớn và giao thức, bao gồm:

+ **SYN Flood**: Gây quá tải máy chủ bằng các yêu cầu TCP SYN để làm cạn kiệt bảng kết nối.

+ **ACK Flood**: Gửi lượng lớn gói ACK để tiêu tốn tài nguyên máy chủ.

+ **UDP Flood**: Làm bão hòa băng thông bằng các gói UDP.

+ **Tấn công Phản chiếu/Khuếch đại**: Lợi dụng các giao thức như DNS, NTP hoặc SSDP để khuếch đại lưu lượng.

Cơ chế:

+ **Lọc lưu lượng**: Các trung tâm lọc toàn cầu của dịch vụ loại bỏ lưu lượng độc hại trước khi nó đến hạ tầng của KTNN tại 116 Nguyễn Chánh, Hà Nội.

+ **Phân tích hành vi**: Sử dụng AI/ML để phát hiện các bất thường trong mô hình lưu lượng, như đột biến về tốc độ gói tin hoặc lạm dụng giao thức.

+ **Chặn theo địa lý**: Lọc lưu lượng từ các khu vực có nguy cơ cao dựa trên thông tin tình báo về mối đe dọa theo thời gian thực, giảm thiểu rủi ro từ các nguồn tấn công quốc tế.

+ **Giới hạn tốc độ**: Giới hạn số lượng gói tin theo IP hoặc giao thức để ngăn cạn kiệt tài nguyên.

+ **Hiệu suất**: Đảm bảo tính sẵn sàng của hệ thống >99,99%, với lưu lượng độc hại được chặn tại biên mạng để giảm thiểu độ trễ cho người dùng hợp pháp.

b. Giảm thiểu DDoS tầng L7

Phạm vi bảo vệ: Xử lý các cuộc tấn công tầng ứng dụng nhắm vào giao thức HTTP/HTTPS, bao gồm:

+ **HTTP/HTTPS Flood**: Gây quá tải máy chủ web bằng các yêu cầu dường như hợp lệ.

+ **Tấn công Low-and-Slow**: Tiêu tốn tài nguyên máy chủ dần dần bằng các kết nối kéo dài (ví dụ: Slowloris, RUDY).

Cơ chế:

+ **Bộ quy tắc được quản lý**: Sử dụng các quy tắc được định nghĩa trước, cập nhật thường xuyên dựa trên danh sách OWASP Top.

+ **Chính sách thách thức**: Áp dụng các kỹ thuật xác minh client (ví dụ: thách thức JavaScript, xác thực cookie) để phân biệt người dùng hợp pháp với bot.

+ **Giới hạn tốc độ**: Thiết lập ngưỡng tùy chỉnh cho tần suất yêu cầu HTTP theo IP, phiên hoặc URL, ngăn chặn quá tải máy chủ.

+ **Kiểm soát truy cập**: Hỗ trợ cấu hình danh sách đen/danh sách trắng dựa trên địa chỉ IP, tiêu đề HTTP hoặc tác nhân người dùng để chặn các nguồn độc hại đã biết.

+ **Phát hiện dựa trên AI**: Sử dụng máy học để nhận diện các mẫu tấn công zero-day, thích ứng với các mối đe dọa mới theo thời gian thực.

+ **Hiệu suất**: Xử lý lưu lượng hợp lệ với độ trễ <50ms, đảm bảo trải nghiệm người dùng liền mạch cho các ứng dụng web của KTNN.

c. Chính sách bảo vệ cài sẵn

Ba chế độ bảo vệ:

+ **Chế độ tiêu chuẩn**: Cài đặt mặc định cho bảo vệ cân bằng, phù hợp với hoạt động thông thường.

+ **Chế độ nâng cao**: Độ nhạy cao hơn để phát hiện các cuộc tấn công tinh vi, lý tưởng trong các giai đoạn có nguy cơ cao.

+ **Chế độ tùy chỉnh**: Cho phép KTNN định nghĩa các quy tắc cụ thể (ví dụ: danh sách trắng IP cho kiểm toán viên nội bộ, giới hạn tốc độ cho API công cộng).

+ **Cấu hình**: Các chính sách có thể điều chỉnh qua bảng điều khiển quản lý của nhà cung cấp dịch vụ, với các cập nhật được áp dụng theo thời gian thực trong vòng 60 giây.

d. Hạ tầng giảm thiểu toàn cầu

+ **Trung tâm lọc**: Hạ tầng vận hành hơn 100 Điểm hiện diện (PoP) trên toàn cầu, với các trung tâm lọc có dung lượng cao tại châu Á, châu Âu và Bắc Mỹ, có khả năng xử lý các cuộc tấn công lên đến 10 Tbps.

+ **Gần gũi địa lý**: Lưu lượng đến các tên miền của KTNN được định tuyến đến trung tâm lọc gần nhất, giảm độ trễ và chặn các cuộc tấn công từ xa khỏi hạ tầng cốt lõi.

+ **Dự phòng**: Hệ thống giảm thiểu nhiều lớp đảm bảo không có điểm lỗi duy nhất, với khả năng chuyển đổi dự phòng sang các PoP khác nếu cần.

e. Quy trình vận hành

Giám sát lưu lượng: Nền tảng của dịch vụ liên tục phân tích lưu lượng đến các tên miền của KTNN theo thời gian thực, sử dụng các số liệu cơ bản được thiết lập từ dữ liệu lịch sử.

Phát hiện tấn công:

+ Nhận diện các bất thường qua kiểm tra gói tin, phân tích hành vi và phát hiện dựa trên chữ ký.

+ Phân loại loại tấn công (ví dụ: tấn công lưu lượng lớn, giao thức, tầng ứng dụng) trong vòng 10 giây.

Giảm thiểu:

+ Loại bỏ các gói tin độc hại tại biên mạng bằng ACL, giới hạn tốc độ hoặc cơ chế thách thức.

+ Chuyển tiếp lưu lượng sạch đến tường lửa của KTNN để xử lý tiếp.

Ghi nhật ký và báo cáo:

+ Tạo nhật ký chi tiết (IP, loại tấn công, thời gian, hành động giảm thiểu).

+ Cung cấp bảng điều khiển thời gian thực và báo cáo có thể tải xuống ở định dạng PDF/Excel.

3.1.2. Dịch vụ Bot Protection

- Sử dụng AI và phân tích hành vi để phát hiện bot.
- Tích hợp SDK cho ứng dụng di động (nếu cần).
- Hỗ trợ captcha tùy chỉnh và phân tích fingerprint.

3.1.3. Dịch vụ báo cáo an ninh mạng

- Hỗ trợ KQL để truy vấn log.
- Cung cấp dashboard thời gian thực và báo cáo xuất định dạng PDF/Excel.

3.2. Yêu cầu về chất lượng dịch vụ

Dịch vụ bảo vệ tên miền và phòng chống DDOS cho 09 tên miền (domain) - Tổng dung lượng 5Tb/ tháng:

3.2.1 Dịch vụ DDoS Protection

- Chặn các cuộc tấn công DDoS L3/L4 và L7 đã xác định.
- Đảm bảo tính sẵn sàng của hệ thống >99.99%.
- Hỗ trợ xử lý sự cố trong vòng 1 giờ kể từ khi phát hiện.

3.2.2 Dịch vụ Bot Protection

- Phát hiện và chặn >95% bot độc hại.
- Không ảnh hưởng đến trải nghiệm người dùng hợp pháp.
- Cập nhật tri thức bot mới trong vòng 24 giờ sau khi phát hiện.

3.2.3 Dịch vụ báo cáo an ninh mạng

- Báo cáo hàng tháng chi tiết về cảnh báo, sự cố, lỗ hổng, và khuyến nghị.
- Báo cáo tổng thể 6 tháng/lần, đánh giá hiệu quả và đề xuất cải thiện.
- Log phân tích đầy đủ, hỗ trợ điều tra sự cố trong vòng 1 giờ.

3.3. Yêu cầu về trách nhiệm nhà cung cấp dịch vụ

Trong thời gian cung cấp dịch vụ Nhà cung cấp dịch vụ phải đảm bảo cung cấp các dịch vụ sau:

- Cung cấp dịch vụ đúng cam kết.
- Cung cấp NDA và giải pháp kỹ thuật theo TCCS 02:2020/VNISA.
- Báo cáo định kỳ (hàng tháng và 6 tháng/lần) và xử lý sự cố kịp thời.
- Xây dựng quy trình xử lý sự cố và đối soát.

3.4. Yêu cầu về sở hữu các thông tin, dữ liệu hình thành trong quá trình cung cấp dịch vụ

- Tất cả thông tin, dữ liệu từ dịch vụ thuộc sở hữu KTNN.
- Đơn vị cung cấp dịch vụ chuyển giao đầy đủ dữ liệu khi kết thúc hợp đồng.
- Đảm bảo an toàn, bảo mật dữ liệu theo quy định pháp luật

3.5. Phương án quản lý, chuyển giao cho bên thuê

- Đơn vị cung cấp dịch vụ lưu trữ và cung cấp báo cáo/log khi KTNN yêu cầu.
- Chuyển giao dữ liệu qua kênh truyền an toàn (SFTP/HTTPS).
- Đảm bảo tính liên tục khi thay đổi nhà cung cấp.

3.6. Yêu cầu về an toàn bảo mật thông tin, dữ liệu

- Tuân thủ Luật An toàn thông tin mạng 86/2015/QH13 và Pháp lệnh bảo vệ bí mật nhà nước.

- Dữ liệu log thuộc sở hữu KTNN, không được chia sẻ với bên thứ ba.

- Mã hóa dữ liệu truyền tải và lưu trữ (AES-256).

- Cam kết bảo mật thông tin qua NDA giữa nhà cung cấp dịch vụ và Kiểm toán nhà nước.

- Không lưu trữ dữ liệu ngoài phạm vi hợp đồng.

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:

- Nhà thầu phải thực hiện và bàn giao đầy đủ các tài liệu, hồ sơ quy định chi tiết tại Nghị định số 73/2019/NĐ-CP ngày 05/9/2019 của Chính phủ quy định về quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước và Nghị định số 82/2024/NĐ-CP ngày 10/7/2024 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 73/2019/NĐ-CP

- Chủ đầu tư sẽ tiến hành kiểm tra, thử nghiệm và nghiệm thu theo các quy định của E-HSMT, quy định của ngành và Thông tư số 16/2024/TT-BTTTT ngày 30/12/2024 của Bộ Thông tin và Truyền thông quy định chi tiết nội dung công tác triển khai, giám sát công tác triển khai, nghiệm thu đối với dự án đầu tư ứng dụng công nghệ thông tin; xác định yêu cầu về chất lượng dịch vụ và các nội dung đặc thù của hợp đồng thuê dịch vụ đối với thuê dịch vụ công nghệ thông tin theo yêu cầu riêng.