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

Mục 1. Yêu cầu về kỹ thuật

I. Giới thiệu chung về dự toán mua sắm, gói thầu

- Tên dự toán mua sắm: Đảm bảo An toàn thông tin Hệ thống thu phí hạ tầng cảng biển Hải Phòng.

- Tên gói thầu: Gói thầu số 01: Cung cấp thiết bị, dịch vụ Đảm bảo An toàn thông tin Hệ thống thu phí hạ tầng cảng biển Hải Phòng.

- Giá gói thầu: **2.641.804.000** đồng.

- Chủ đầu tư: Cảng vụ Đường thủy nội địa Hải Phòng.

- Nguồn vốn: Kinh phí phục vụ công tác thu phí sử dụng công trình kết cấu hạ tầng, công trình dịch vụ, tiện ích công cộng trong khu vực cửa khẩu cảng biển Hải Phòng năm 2025 tại Quyết định số 257/QĐ-SXD ngày 07/5/2025.

- Thời gian thực hiện: Năm 2025 - 2026.

- Địa điểm thực hiện: Phòng máy chủ Chi cục Hải Quan Khu vực III - Số 159 đường Lê Hồng Phong, Phường Đông Hải, thành phố Hải Phòng.

- Quy mô dự toán mua sắm: Triển khai các phương án đảm bảo an toàn thông tin cho hệ thống thu phí hạ tầng cảng biển bao gồm:

+ Dịch vụ quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập.

+ Dịch vụ chặn lọc phần mềm độc hại trên môi trường mạng.

+ Thiết bị chữ ký số.

+ Dịch vụ cân bằng tải và dự phòng nóng cho các thiết bị mạng chính.

+ Dịch vụ phòng chống tấn công từ chối dịch vụ.

+ Dịch vụ giám sát an toàn hệ thống thông tin tập trung.

+ Dịch vụ phòng, chống thất thoát dữ liệu.

+ Dịch vụ phòng chống tấn công mạng cho ứng dụng web; sử dụng Sản phẩm Tường lửa ứng dụng web.

II. Yêu cầu về kỹ thuật

1. Yêu cầu về kỹ thuật chung

1.1. Yêu cầu đối với hàng hóa

Nhà thầu phải chào thầu hạng mục hàng hóa của gói thầu đáp ứng các thông số kỹ thuật theo danh mục liệt kê dưới đây, trong trường hợp bất kỳ thông số kỹ thuật nào có chỉ dẫn liên quan đến nhãn hiệu hàng hóa hoặc ký hiệu/quy định

riêng khác kèm theo thì chỉ mang tính chất tham khảo, nhà thầu có thể chào thầu các loại hàng hóa có tính năng kỹ thuật "tương đương" hoặc "ưu việt hơn" so với các yêu cầu tối thiểu.

Nhà thầu phải có bảng so sánh chứng minh tính đáp ứng của các thông số kỹ thuật giữa hàng hóa, thiết bị chào thầu và yêu cầu kỹ thuật của E-HSMT đầy đủ các nội dung sau:

- Thông số kỹ thuật hàng hóa theo E-HSMT

- Thông số kỹ thuật hàng hóa theo E-HSDT (model, ký mã hiệu, hãng sản xuất)

- Hàng hóa, thiết bị thuộc gói thầu phải mới 100%, chưa qua sử dụng, sản xuất năm 2024 trở lại đây cho đến thời điểm đóng thầu, có nguồn gốc xuất xứ rõ ràng, có Catalogue hoặc tài liệu kỹ thuật với đầy đủ các thông số kỹ thuật kèm theo. Đã bao gồm đầy đủ các vật tư, phụ kiện kèm theo để lắp đặt hoàn chỉnh, vận hành theo yêu cầu của chủ đầu tư.

- Cung cấp Catalogue hoặc tài liệu kỹ thuật để chứng minh hàng hóa chào thầu đáp ứng yêu cầu kỹ thuật của E-HSMT. Trường hợp, trong catalogue hoặc tài liệu kỹ thuật không đầy đủ thông số theo yêu cầu của E-HSMT thì nhà thầu phải có xác nhận thông số kỹ thuật của nhà sản xuất hoặc đại lý phân phối chính thức tại Việt Nam.

- Tham chiếu thông số kỹ thuật hàng hóa theo E-HSDT với hồ sơ, tài liệu kỹ thuật, catalogue của nhà sản xuất. Yêu cầu tham chiếu từng mục thông số kỹ thuật được thể hiện tại trang..., dòng... của hồ sơ, tài liệu kỹ thuật, catalogue.

- Thời gian bảo hành theo tiêu chuẩn của nhà sản xuất.

- Đối với hàng hóa nhập khẩu:

+ Hàng hóa phải được phân phối tại Việt Nam.

+ Nhà thầu phải có bản cam kết cung cấp các loại giấy tờ trong quá trình thực hiện hợp đồng, cụ thể: Chứng nhận xuất xứ (Certificate of Origin - CO), Chứng nhận chất lượng (Certificate of Quality - CQ) do Hãng sản xuất cấp (bản chính hoặc bản sao chứng thực hợp lệ).

- Tài liệu tiếng nước ngoài nhà thầu dịch sang Tiếng Việt.

- Đối với các loại thiết bị, vật tư sản xuất trong nước

+ Nhà thầu phải có bản cam kết cung cấp các loại giấy tờ trong quá trình thực hiện hợp đồng, cụ thể: Cung cấp giấy chứng nhận xuất xưởng vào thời điểm giao hàng, cung cấp giấy Chứng nhận chất lượng do hãng sản xuất cấp (bản chính hoặc bản sao chứng thực hợp lệ).

- Cam kết trong trường hợp trúng thầu nhà thầu phải cung cấp đúng chủng loại hàng hóa đề xuất trong E-HSDT.

- Nhà thầu phải có bảng tuyên bố đáp ứng về kỹ thuật của hàng hóa chào thầu

theo mẫu sau:

TT	Tên hàng hóa	Ký mã hiệu/ Nhãn mác sản phẩm, Tên nhà sản xuất, Xuất xứ	Yêu cầu kỹ thuật theo E-HSMT	Thông số kĩ thuật, tiêu chuẩn chất lượng, đặc tính kỹ thuật chào thầu	Tài liệu kỹ thuật tham chiếu trong E-HSDT
(1)	**(2)**	**(3)**	**(4)**	**(5)**	**6**
1					*Trang ... của Catalog ... thuộc E-HSDT*
…					*Trang ... của Catalog ... thuộc E-HSDT*
n					*Trang ... của Catalog ... thuộc E-HSDT*

(Ghi chú:

- Cột 1, 2, 4: Nhà thầu ghi thông tin theo yêu cầu của E-HSMT;

- Cột 3, 5, 6 : Nhà thầu ghi các thông tin của hàng hóa dự thầu;

- Cột 3, 5, 6: Nhà thầu cung cấp tài liệu chứng minh cho các thông tin kê khai.)

1.2. Yêu cầu đối với dịch vụ

- Nhà thầu phải tích hợp dịch vụ trong gói thầu này với những thiết bị đang sử dụng tại các địa điểm lắp đặt sao cho đồng bộ, phù hợp đảm bảo sự liên kết, thống nhất hoạt động dịch vụ phải tương thích với hạ tầng hiện có của đơn vị sử dụng. Trong trường hợp Nhà thầu cần nghiên cứu hiện trường để có cơ sở chuẩn bị E-HSDT nhà thầu cần đề xuất đến Bên mời thầu bằng văn bản trước thời điểm đóng thầu tối thiểu 03 ngày làm việc. Toàn bộ chi phí đi nghiên cứu hiện trường do nhà thầu tự chi trả.

- Bên mời thầu sẽ cho phép nhà thầu và các bên liên quan của nhà thầu tiếp cận hiện trường để phục vụ mục đích nghiên cứu hiện trường với điều kiện nhà thầu và các bên liên quan của nhà thầu cam kết rằng Bên mời thầu và các bên liên quan của Bên mời thầu không phải chịu bất kỳ trách nhiệm nào đối với nhà thầu và các bên liên quan của nhà thầu liên quan đến việc nghiên cứu hiện trường này. Nhà thầu và các bên liên quan của nhà thầu sẽ tự chịu trách nhiệm cho những rủi ro của mình như tai nạn, mất mát hoặc thiệt hại tài sản và bất kỳ các mất mát, thiệt hại và chi phí nào khác phát sinh từ việc nghiên cứu hiện trường.

2. Các yêu cầu kỹ thuật chi tiết

2.1. Yêu cầu về Dịch vụ quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập

a) Với dịch vụ quản lý truy cập giữa các vùng mạng

Quản lý truy cập giữa các vùng mạng đóng vai trò như một rào cản giữa mạng nội bộ (LAN) và mạng bên ngoài (Internet) để bảo vệ hệ thống khỏi các mối đe dọa mạng. Tường lửa hoạt động bằng cách kiểm soát lưu lượng mạng vào và ra dựa trên các quy tắc bảo mật được định nghĩa trước, cho phép hoặc chặn các gói tin theo các tiêu chí như địa chỉ IP, giao thức, cổng, hoặc ứng dụng. Tường lửa giúp ngăn chặn các cuộc tấn công mạng như truy cập trái phép, mã độc, hoặc khai thác lỗ hổng.

Tính năng hệ thống

- Trung tâm điều khiển: Cung cấp mức độ hiển thị đa dạng về các hoạt động, rủi ro và mối đe dọa trong hệ thống với nhiều tiện ích nhằm bổ sung thông tin cho người quản trị, dễ dàng truy cập.

- Tính năng Firewall:

+ Thiết lập chính sách truy cập mạng.

+ Thiết lập chính sách truy cập ứng dụng mạng.

+ Thiết lập chính sách truy cập mạng theo lịch có sẵn.

- Tính năng IPSec VPN:

+ Kết nối VPN giữa 2 site.

+ Gửi báo cáo các loại tấn công tự động.

+ Có giao diện web để giám sát băng thông sử dụng.

+ Hỗ trợ giữ nguyên giao thức định tuyến tĩnh/động.

+ Kết nối VPN giữa nhiều site (hơn 2 site).

- Static/dynamic routing:

+ Hỗ trợ RIP/OSPF/BGP Routing.

+ Hỗ trợ Static route.

- Cấu hình NAT: Cung cấp tính năng NAT.

- VPN – Kết nối an toàn và bảo mật từ xa: Hỗ trợ đầy đủ các công nghệ kết nối VPN site-to-site, client-to-site.

- Reporting and Logging: Báo cáo và ghi log các hoạt động: cung cấp khả năng lưu trữ log cả trên cloud lẫn trên thiết bị linh hoạt với mức độ tùy chỉnh cao mà không

phải trả thêm khoản phí nào. Báo cáo về các mối đe doạ theo từng người dùng.

Thông lượng của thiết bị tường lửa ≥ 18 Gbps.

Yêu cầu tính dự phòng: hỗ trợ triển khai mô hình active-active hoặc active-passive.

b) Với dịch vụ phòng chống xâm nhập

- Dịch vụ phòng chống, ngăn chặn xâm nhập (IPS) cung cấp khả năng quét lưu lượng mạng hiệu suất cao để phát hiện và ngăn chặn các mối đe dọa mạng trong thời gian thực. IPS hoạt động bằng cách phân tích lưu lượng mạng để xác định các mẫu hành vi độc hại, chẳng hạn như các cuộc tấn công khai thác lỗ hổng, mã độc hoặc các nỗ lực xâm nhập. Với khả năng xử lý tối thiểu 5 Gbps cho IPS đảm bảo hiệu suất ngay cả trong môi trường mạng có lưu lượng cao.

- Tính năng IPS được hỗ trợ bởi trí tuệ nhân tạo (AI) và công nghệ máy học, giúp nhận diện các mối đe dọa chưa từng biết (zero-day threats) trước khi chúng xâm nhập vào mạng. Dữ liệu mối đe dọa được cập nhật liên tục, đảm bảo phản ứng nhanh chóng. Dịch vụ này cũng tích hợp với tường lửa, từ đó tự động cô lập các thiết bị bị nhiễm để ngăn chặn lây lan.

- IPS hỗ trợ kiểm tra TLS 1.3 với hiệu suất cao, loại bỏ các điểm mù bảo mật trong lưu lượng mã hóa. Người dùng có thể tùy chỉnh các mẫu IPS theo từng quy tắc tường lửa, tối ưu hóa hiệu suất mà không làm giảm mức độ bảo vệ. Ngoài ra, các báo cáo chi tiết về lưu lượng mạng, mối đe dọa và hoạt động IPS được cung cấp qua giao diện web, giúp quản trị viên dễ dàng theo dõi và điều chỉnh chính sách bảo mật.

Công nghệ nền tảng: IPS sử dụng nhiều công nghệ và phương pháp để phát hiện và ngăn chặn các mối đe dọa.

Phân tích mẫu chữ ký (Signature-based Detection):

- Dựa vào cơ sở dữ liệu chứa các mẫu chữ ký của các loại tấn công đã biết, IPS so sánh lưu lượng mạng với các mẫu này để phát hiện tấn công.

- Hiệu quả cao đối với các mối đe dọa đã biết.

Phân tích hành vi bất thường (Anomaly-based Detection):

- Xây dựng mô hình hành vi bình thường của hệ thống; bất kỳ hành vi nào vượt quá giới hạn bình thường sẽ bị coi là đáng ngờ.

- Hữu ích trong việc phát hiện các mối đe dọa mới.

Yêu cầu năng lực của dịch vụ IPS ≥ 5 Gbps

2.2. Yêu cầu kỹ thuật dịch vụ chặn lọc phần mềm độc hại trên môi trường mạng

- Giải pháp chặn lọc phần mềm độc hại trên môi trường mạng (Network

Antivirus) cung cấp khả năng bảo vệ chống lại các mối đe dọa phần mềm độc hại, bao gồm ransomware, phần mềm gián điệp, trojan và các mối đe dọa zero-day, ngay tại lớp mạng. Giải pháp quét và theo dõi lưu lượng mạng trong thời gian thực với hiệu suất cao, cho bảo vệ mối đe dọa, đảm bảo hiệu quả ngay cả trong các môi trường mạng có lưu lượng lớn.

- Network Antivirus sử dụng công nghệ quét sâu các gói tin (deep packet inspection) để kiểm tra tất cả lưu lượng vào và ra, bao gồm các tệp được truyền tải qua các giao thức phổ biến như HTTP, HTTPS, FTP, SMTP và POP3. Tính năng này có thể phát hiện và chặn các tệp độc hại ở nhiều định dạng, chẳng hạn như .exe, .docx, .pdf, và các tệp nén như ZIP, RAR, hoặc 7Z. Công nghệ phân tích hành vi và học sâu (deep learning) cho phép nhận diện các mối đe dọa chưa từng biết trước, dựa trên các mẫu hành vi bất thường thay vì chỉ dựa vào chữ ký (signature-based detection).

- Thông lượng giải pháp cần đáp ứng khi bật tính năng

Threat Protecion ≥ 4.5 Gbps.

2.3. Yêu cầu kỹ thuật thiết bị chữ ký số

Thiết bị ký số HSM (Hardware Security Module) là một thiết bị phần cứng chuyên dụng, được thiết kế để quản lý, lưu trữ và xử lý các khóa mã hóa một cách an toàn, đảm bảo bảo mật cho các giao dịch số, dữ liệu nhạy cảm, và quy trình xác thực. HSM cung cấp môi trường bảo mật vật lý và logic để bảo vệ khóa mã hóa khỏi các cuộc tấn công, bao gồm cả xâm nhập vật lý và phần mềm.

HSM thực hiện các chức năng mã hóa chính như tạo khóa, mã hóa/giải mã, ký số, và xác thực chữ ký số. Chúng hỗ trợ các thuật toán mã hóa đối xứng (như AES) và không đối xứng (như RSA, ECC), đáp ứng các tiêu chuẩn bảo mật nghiêm ngặt như FIPS 140-2/140-3, Common Criteria, và NITES.

Hệ thống hiện tại hiện sử dụng một thiết bị ký số HSM Utimaco Security Server Se12 LAN V4 chạy độc lập, không có thiết bị dự phòng và đã hết vòng đời sản phẩm, không có dịch vụ bảo hành và hỗ trợ kỹ thuật từ hãng. Để đảm bảo tương thích về mặt công nghệ đề xuất trang bị thiết bị HSM của hãng Utimaco:

HSM cung cấp các tính năng chính như:

STT	Yêu cầu	Thông số kỹ thuật và các tiêu chuẩn
1	Hiệu năng thiết bị	- Thuật toán RSA có độ dài khoá: ≥ 2048 bit. - Signature Creation RSA-2048: ≥ 101 Signatures/s - Key Generation RSA-2048: ≥ 2.53 (Key/s) - Key Generation ECDSA P-256 bit: ≥ 267 (Key/s)

STT	Yêu cầu	Thông số kỹ thuật và các tiêu chuẩn
		- Encryption/Decryption AES 256 – GCM: ≥ 37.00 (Mbytes/s) - Encryption/Decryption AES 256 – ECB: ≥ 67.90 (Mbytes/s) - Containers: ≥ 1
2	Các giao diện lập trình ứng dụng (APIs)	Tối thiểu có: - PKCS#11. - Java Cryptography Extension (JCE). - Microsoft Crypto API (CAPI) and Cryptography Next Generation (CNG) - Extensible Key Management (SQLEKM) - OpenSSL. - CXI
3	Thuật toán mã hoá	Tối thiểu có: - RSA, DSA, ECDSA with NIST, Brainpool and FRP256v1 curves, EdDSA - DH, ECDH with NIST, Brainpool, FRP256v1 and Montgomery curves - AES, Triple-DES, DES. - MAC, CMAC, HMAC. - 5G, Block-chain and PQC ready - SHA-1, SHA2-Family, SHA3, RIPEMD. - Bộ tạo số ngẫu nhiên dựa trên hàm băm (DRG.4 acc. AIS 31). - Thuật toán sinh số ngẫu nhiên dựa trên nền tảng phần cứng (PTG.2 acc AIS 31).
4	Tiêu chuẩn an ninh	Tối thiểu có: - FIPS 140-2 Level 3 - Operation in FIPS Mode is possible. - CC / NITES - PCI PTS HSM v3
5	Tính năng thiết bị	- Tối thiểu hỗ trợ hệ điều hành: Windows, Linux - Có chức năng lưu trữ và quản lý khóa an toàn.

STT	Yêu cầu	Thông số kỹ thuật và các tiêu chuẩn
		- Có tối thiểu 2 chế độ: lưu khóa bên trong thiết bị HSM và bên ngoài dưới dạng file mã hoá. - Cho phép xác thực quyền admin bằng thẻ thông minh. - Cho phép quản lý truy cập dựa trên yếu tố phân định vai trò và phân tách chức năng (role-based access control and separation of functions). - Cho phép triển khai nhiều HSM mới theo cụm với HSM cũ (Utimaco) để đảm bảo tính sẵn sàng (high available) và tự động phân phối tải (load balancing). - Có cơ chế quản lý HSM từ xa. - Dung lượng lưu (cặp khóa, chứng thư số): ≥ 3000 với thuật toán RSA có độ dài khóa: ≥ 2048bit. - Phân vùng quản trị: Hỗ trợ lên tới 1.000 partitions/slots. - Số lượng kết nối từ server ứng dụng tới thiết bị HSM: ≥ 3000.
6	Thiết kế	- Dạng thiết bị lắp lên tủ rack, kích thước 1U, 19 inch - Cổng kết nối RJ45 loại 1Gb/s: ≥ 02. - Nguồn điện của thiết bị: 2 nguồn x 100~240 VAC, 50~60Hz, có khả năng thay thế nóng (hot-swap)
7	Bảo hành và hỗ trợ kỹ thuật	12 tháng

2.4. Yêu cầu dịch vụ cân bằng tải và dự phòng nóng cho các thiết bị mạng chính – Tường lửa cơ sở dữ liệu DBF

Do cần ngăn chặn theo thời gian thực các tấn công vào database nên hệ thống được thiết kế cặp thiết bị Tường lửa CSDL hoạt động theo cơ chế Inline layer 2 bridge và Active-Active Failover. Khi một thiết bị gặp sự cố, dữ liệu được failover sang thiết bị còn lại xử lý tiếp, không gây gián đoạn hệ thống. Ngoài ra thiết bị còn hỗ trợ chế độ Fail-Open cho phép mở thông mạng nếu lỗi thiết bị. Tường lửa CSDL được đặt trước các máy chủ CSDL, kiểm soát các truy cập từ ứng dụng, người dùng qua mạng vào máy chủ CSDL. Tường lửa CSDL bảo vệ CSDL trước những loại tấn công khai thác lỗ hổng CSDL (SQL injection…) và hành vi bất thường đồng thời ghi lại log toàn bộ thao tác với CSDL để làm báo cáo, điều tra.

- Nhật ký sự kiện quan trọng: cho phép ghi lại các sự kiện quan trọng liên quan đến truy cập dữ liệu và quản lý cơ sở dữ liệu, bao gồm việc truy cập bảng, cột, thực hiện truy vấn, thay đổi dữ liệu, tạo và xóa người dùng, cấp quyền, và nhiều hoạt động khác.

- Thu thập thông tin audit: cho phép thu thập thông tin chi tiết về người dùng, thời gian, địa chỉ IP, chương trình ứng dụng, và hành động thực hiện trong hệ thống cơ sở dữ liệu.

- Tích hợp với giám sát và nhật ký ngoại vi: cho phép tích hợp với các công cụ giám sát và giám sát bảo mật bên ngoài để cung cấp cái nhìn toàn diện hơn về hoạt động cơ sở dữ liệu và an ninh.

2.5. Yêu cầu về dịch vụ phòng, chống tấn công từ chối dịch vụ (anti- DDOS)

- Giải pháp Anti-DDoS được thiết kế để phát hiện và giảm thiểu các cuộc tấn công từ chối dịch vụ (DoS) và phân tán (DDoS), vốn nhằm làm quá tải và gián đoạn các dịch vụ mạng.

- Anti-DDoS phân tích lưu lượng mạng trong thời gian thực, phát hiện các mẫu lưu lượng bất thường liên quan đến các cuộc tấn công như ICMP flood, SYN flood, UDP flood, hoặc HTTP flood. Tính năng này cho phép cấu hình các giới hạn tốc độ gói tin (packet rate) và tốc độ bùng nổ (burst rate) để kiểm soát lưu lượng từ các nguồn đáng ngờ. Ví dụ, quản trị viên có thể đặt giới hạn 1200 gói/phút cho ICMP/ICMPv6 flood, giúp ngăn chặn các cuộc tấn công làm ngập băng thông.

- Khi phát hiện một cuộc tấn công DDoS, giải pháp tự động áp dụng các biện pháp giảm thiểu, bao gồm giới hạn lưu lượng từ một địa chỉ IP cụ thể, chặn các gói tin bất thường, hoặc chuyển hướng lưu lượng để bảo vệ tài nguyên mạng. Tính năng này được cập nhật liên tục để nhận diện các mẫu tấn công mới. Ngoài ra, giải pháp hỗ trợ bảo vệ cả lưu lượng IPv4 và IPv6, đảm bảo khả năng tương thích với các môi trường mạng hiện đại.

- Quản trị viên có thể thiết lập các quy tắc DoS dựa trên loại tấn công, giao thức, hoặc nguồn lưu lượng, với các tùy chọn như giới hạn tốc độ gói tin hoặc chặn hoàn toàn các nguồn tấn công. Báo cáo chi tiết về các cuộc tấn công DDoS, bao gồm thông tin về lưu lượng bất thường và hành động giảm thiểu.

Nội dung	Yêu cầu
Khả năng chặn lọc lưu lượng tấn công	a) Anti-DDoS đảm bảo khả năng phát hiện và chặn lọc lưu lượng tấn công tối thiểu 80%.
	b) Anti-DDoS đảm bảo khả năng bảo vệ lưu lượng sạch tối thiểu 85%.
Khả năng bảo vệ	Anti-DDoS đảm bảo dịch vụ vẫn hoạt động bình thường trước tối thiểu các loại tấn công DDoS sau bao gồm: a) 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;

Nội dung	Yêu cầu
	b) 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; c) Tấn công sử dụng gói tin không hợp lệ: malformed, invalid packet; d) Tấn công gửi gói tin/yêu cầu với tần suất cao, đột ngột; đ) Tấn công qua phân tích hành vi người dùng: HTTP page flood, DNS flood, brute force; e) Khả năng chặn lọc gói tin theo chính sách sử dụng ALC.
Cảnh báo theo thời gian thực	Anti-DDoS cho phép tự động cảnh báo tới người dùng theo thời gian thực đối với các loại sự kiện sau. a) Cảnh báo khi có tấn công DDoS xảy ra; b) Cảnh báo về tự động xử lý tấn công DDoS; c) Cảnh báo khi tấn công DDoS kết thúc.
Yêu cầu về giám sát	Anti-DDoS cho phép giám sát và phân tích sự cố tấn công DDoS: a) 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; b) Cho phép giám sát băng thông theo địa chỉ IP và dải mạng phục vụ phân tích tấn công; c) Cho phép giám sát theo dõi hiệu quả chặn lọc thông qua lưu lượng băng thông trước và sau khi đi qua bộ lọc.

2.6. Yêu cầu về dịch vụ giám sát an toàn hệ thống thông tin tập trung

- Công nghệ giám sát (SIEM) phải được các tổ chức quốc tế đánh giá và công nhận về tính năng hiệu năng.

- Công nghệ giám sát phải nằm trong top Leader của Gartner trong 10 năm liên tiếp.

- Đơn vị cung cấp dịch vụ cần có đội ngũ ứng cứu xử lý sự cố thường trực 24/7 tại địa bàn thành phố Hải Phòng sẵn sàng hỗ trợ, ứng cứu các sự cố An toàn thông tin trong toàn bộ quá trình cung cấp dịch vụ.

- Giám sát sự kiện an toàn thông tin giúp kịp thời phát hiện, xử lý, ứng cứu các rủi ro gây mất an toàn thông tin, lộ lọt dữ liệu, trước các cuộc tấn công từ trong và ngoài tổ chức. dịch vụ giám sát sự kiện an toàn thông tin phải đáp ứng các tính năng sau:

+ Dữ liệu đa dạng và toàn diện: Thu thập dữ liệu an toàn thông tin từ nhiều thiết bị cần quản lý thông qua cơ chế lấy Syslog hoặc bằng các giao thức như:

JDBC, SNMP, SDEE, OPSEC… Hệ thống tương thích tốt với các giải pháp khác như Antivirus, Firewall, VPN, WAF.

+ Chuẩn hoá và loại bỏ dữ liệu dư thừa: Dữ liệu thu thập về sẽ được hệ thống sắp xếp, chuẩn hoá và phân loại lại theo một định dạng chung, tối ưu hoá cho việc phân tích và điều tra xử lý sự cố. Đồng thời dữ liệu cũng được lọc bớt các thành phần dư thừa, đảm bảo cho người vận hành có thể điều tra và nhận diện nhanh chóng các vi phạm, tấn công đang xảy ra trong hệ thống, từ đó đưa ra các quyết định hiệu quả và kịp thời.

+ Phát hiện tấn công thời gian thực dựa trên Killchain và IOC: Thành phần phân tích và phát hiện tấn công của giải pháp có khả năng xử lý đến 5000EPS/1 thiết bị và có khả năng mở rộng theo quy mô của hệ thống. Công nghệ phân tích tương quan nhiều chiều theo thời gian thực, nhiều pha trên dữ liệu, sử dụng các mô hình mới trên thế giới như Killchain và IOC. Hệ thống tập luật mềm dẻo, tương thích dễ dàng với môi trường hạ tầng khác nhau. Bộ phân tích có khả năng phát hiện ra các dấu hiệu khả nghi, những hành vi bất thường bên trong hệ thống cần phải điều tra, xử lý; loại bỏ các cảnh báo giả, không chính xác.

+ Tối ưu lưu trữ và tìm kiếm phục vụ cho điều tra: Lưu trữ dữ liệu được sắp xếp, sao lưu, tinh chỉnh để phục vụ tối đa cho việc điều tra và xử lý sự cố, cũng có thể mở rộng dễ dàng theo quy mô, yêu cầu của hệ thống.

+ Giao diện giám sát trực quan, đa dạng: Giao diện trực quan, thân thiện, cung cấp sẵn hàng chục loại định dạng giao diện giám sát theo nhiều tiêu chí đa dạng, theo các use case vận hành thường gặp.

+ Quản lý Workflow: Quản lý ticket và workflow giúp quản lý vận hành khai thác an toàn thông tin, lưu trữ và truy vết lịch sử, xử lý sự cố dễ dàng, quản lý được vòng đời của các sự cố từ khi bắt đầu đến khi kết thúc

2.7. Yêu cầu về dịch vụ phòng, chống thất thoát dữ liệu

- Giải pháp phòng chống thất thoát dữ liệu (Data Loss Prevention - DLP) là một hệ thống công nghệ và quy trình được thiết kế để ngăn chặn dữ liệu nhạy cảm bị rò rỉ, mất mát hoặc truy cập trái phép.

- Tính năng cần có của dịch vụ chống thất thoát dữ liệu (DLP):

+ Kiểm soát toàn bộ dữ liệu gửi ra ngoài qua Internet, bao gồm: Email / Webmail /Mạng xã hội /Messenger /Cloud (gồm Office 365 & Google Docs).

+ Phân tích luồng dữ liệu mã hóa dạng SSL ở 2 mức: Endpoint / Gateway.

+ Phân tích hành vi người dùng /Tạo hồ sơ /Cảnh báo mối đe dọa/ Ngăn chặn sự vi phạm dữ liệu.

+ Tạo biểu đồ kết nối liên lạc người dùng.

+ Kiểm soát thiết bị ngoại vi & thiết bị tại tổ chức / Ngăn chặn chép ảnh ra bên ngoài /qua in ấn.

+ Mã khóa file khi sao chép ra ngoài.

2.8. Yêu cầu về dịch vụ phòng chống tấn công mạng cho ứng dụng web; sử dụng Sản phẩm Tường lửa ứng dụng web

Dịch vụ tường lửa ứng dụng Web có những tính năng như sau:

- Ngăn chặn các tấn công khai thác điểm yếu đã biết tới các hệ thống website như cross-site-scripting (XSS), SQL injection, Local File Inclusion (LFI), XML External Entity,...

- Phòng chống các cuộc tấn công từ chối dịch vụ tại layer 7.

- Khi triển khai Giải pháp tường lửa ứng dụng Web đứng trước web application, lớp bảo vệ sẽ đứng giữa web application và internet do đó các ứng dụng web sẽ được bảo vệ bằng các bộ lọc, giám sát và chặn các traffic HTTP/S độc hại tới dịch vụ.

- Ngăn tất cả các dữ liệu không được phép từ client đến trực tiếp server backend. WAF sẽ đóng vai trò như một reverse proxy để bảo vệ máy chủ web.

- Giải pháp có thể giám sát, phân tích và thống kê truy cập của người dùng theo thời gian thực từ đó hỗ trợ ngăn chặn, cảnh báo các bất thường trong truy cập.

- Khả năng chống tấn công, thâm nhập từ bên ngoài có thể ngăn chặn ngay lập tức với các cuộc tấn công ứng dụng Web nằm trong Top 10 OWASP bao gồm:

+ Injection.

+ Broken Authentication.

+ Sensitive Data Exposure.

+ XML External Entities.

+ Broken Access Control.

+ Security Misconfiguration.

+ Cross-Site-Scripting(XSS).

+ Insecure Deserialization.

+ Using Components with Know Vulnerabilities.

+ Insufficient Logging & Monitoring.

Giải pháp có khả năng theo dõi các luồng traffic inbound, từ đó theo dõi được hành vi của các cuộc tấn công DOS vào ứng dụng web và đưa ra cảnh báo, ngăn chặn các cuộc tấn công này. Tính năng này có thể được cấu hình trên Portal và có thể điều chỉnh rate-limit cho từng website ứng dụng khác nhau.

- Giải pháp có thể thêm, sửa, xóa certificate một cách dễ dàng trên Portal quản trị của WAF cho các website được WAF bảo vệ.

- Khi hệ thống phát hiện được có hành vi thay đổi cấu hình, dữ liệu sẽ có cảnh báo kịp thời cho quản trị viên qua alert và email để phòng chống đánh cắp dữ liệu, cấu hình hệ thống.

Giải pháp thông báo các thông tin về lưu lượng truy cập trang web cũng như các sự kiện an toàn thông tin, WAF thống kê thông tin về mức độ sử dụng CPU, lưu lượng truy cập website (IP, Protocol, dạng tấn công,..), WAF cũng cung cấp thông tin địa lý từ các địa chỉ IP có hành vi tấn công.

2.9. Yêu cầu về quản lý, vận hành dịch vụ

STT	Dịch vụ	Mô tả công việc
1	Dịch vụ quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Cấu hình và triển khai: Thiết lập cấu hình các luật và chính sách bảo mật trên để kiểm soát lưu lượng mạng vào ra. Cập nhật phiên bản mới hoặc các dữ liệu bảo vệ mới cho tường lửa khi có yêu cầu. Hỗ trợ đội ngũ vận hành thiết lập, cấu hình chính sách truy cập giữa các vùng mạng
2	Dịch vụ chặn lọc phần mềm trên môi trường mạng	Kích hoạt tính năng ngăn chặn phần mềm độc hại và cập nhật dữ liệu thường xuyên khi có phiên bản cập nhật mới của hãng cung cấp
3	Dịch vụ phòng, chống tấn công từ chối dịch vụ	Thiết lập ngưỡng, tần suất truy cập phòng chống tấn công từ chối dịch vụ
4	Dịch vụ phòng, chống thất thoát dữ liệu	Cấu hình các chính sách ngăn chặn các hành vi gửi tập tin mã hóa/đặt mật khẩu, nén ra ngoài
5	Dịch vụ tường lửa CSDL (DBF)	Hỗ trợ thiết lập, cấu hình dịch vụ tường lửa CSLD tích hợp với hệ thống CSDL hiện tại.
6	Dịch vụ tường lửa ứng dụng WEB	Thêm/xóa các domain mới vào hệ thống bảo vệ Cấu hình và triển khai WAF: - Thiết lập và cấu hình WAF theo các yêu cầu bảo mật của ứng dụng web cụ thể. Cập nhật và nâng cấp: - Theo dõi các bản cập nhật và phiên bản mới của WAF để đảm bảo tính bảo mật và hiệu suất tốt nhất.

STT	Dịch vụ	Mô tả công việc
		- Thực hiện quá trình nâng cấp phiên bản WAF một cách cẩn thận để tránh gặp lỗi hoặc gián đoạn hoạt động của ứng dụng. Kiểm tra và thử nghiệm: - Tiến hành kiểm tra thử nghiệm để đảm bảo rằng WAF hoạt động đúng cách và có khả năng ngăn chặn các loại tấn công mạng như mong đợi. - Kiểm tra cẩn thận trước khi triển khai các quy tắc bảo mật mới để tránh gây rối hoặc gián đoạn không mong muốn đến ứng dụng web.

2.10. Yêu cầu về sẵn sàng với Ipv6

Các sản phẩm, dịch vụ phải có tính sẵn sàng hỗ trợ địa chỉ Internet thế hệ mới IPv6, DNSSEC. Triển khai HTTPS sử dụng giao thức TLS v1.2 trở lên với các bộ mã hóa an toàn trong xác thực người dùng và truyền nhận các thông tin nhạy cảm (thông tin cá nhân, thông tin thanh toán). Cụ thể:

STT	Yêu cầu
1	Đảm bảo phần mềm hỗ trợ IPv6
2	Đảm bảo đường truyền kết nối Internet cho Webserver hỗ trợ IPv6
3	Khai báo Webserver lắng nghe được các kết nối qua mạng IPv6
4	Khai báo bản ghi AAAA cho tên miền trên hệ thống DNS Hosting
5	Đảm bảo máy chủ DNS Hosting hỗ trợ IPv6
6	Sẵn sàng hỗ trợ địa chỉ Internet thế hệ mới IPv6, DNSSEC. Triển khai HTTPS sử dụng giao thức TLS v1.2 trở lên với các bộ mã hóa an toàn trong xác thực người dùng và truyền nhận các thông tin nhạy cảm (thông tin cá nhân, thông tin thanh toán).

2.11. Mô hình triển khai

Nhà thầu có bản vẽ logic mô hình triển khai tương ứng với các giải pháp kỹ thuật chi tiết của các dịch vụ, phù hợp với hiện trạng và đáp ứng được quy định của pháp luật về an toàn thông tin cấp độ 3. Nhà thầu diễn giải các vùng mạng được thiết kế theo bản vẽ mô hình logic.

3. Yêu cầu, điều kiện về khả năng kết nối, liên thông với ứng dụng, hệ thống thông tin khác

Hệ thống phải đảm bảo tuân thủ đúng theo Quyết định số 292/QĐ-BKHCN ngày 25/3/2025 về việc ban hành khung kiến trúc Chính phủ số Việt Nam, phiên bản 4.0 và Nghị định số 47/2020/NĐ-CP ngày 09/4/2020 của Chính phủ về quản

lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước, trong đó có các kết nối chính như sau:

- Sẵn sàng kết nối liên thông dữ liệu với các hệ thống ứng dụng công nghệ thông tin khác của các Sở ban ngành, cơ quan, doanh nghiệp trong thành phố thông qua nền tảng chia sẻ tích hợp LGSP.

- Đảm bảo hỗ trợ phần mềm kết nối liên thông dữ liệu với các hệ thống thông tin hiện tại đang kết nối: Phần mềm khai báo Hải Quan, Hệ thống thanh toán 24/7 của Cục Hải quan, đối tác thanh toán, hóa đơn điện tử.

- Sẵn sàng hỗ trợ kết nối liên thông dữ liệu với các hệ thống thông tin, cơ sở dữ liệu của Bộ ngành Trung ương thông qua nền tảng chia sẻ tích hợp LGSP – NGSP.

Các kết nối này có thể được thực hiện thông qua mạng internet, mạng số liệu chuyên dùng, mạng VPN.

4. Yêu cầu về đảm bảo an toàn bảo mật thông tin

Hệ thống được Ủy ban nhân dân thành phố Hải Phòng phê duyệt là hệ thống thông tin cấp độ 3 tại quyết định số 2331/QĐ-UBND ngày 19/7/2022 về việc phê duyệt cấp độ an toàn hệ thống thông tin.

Nhà thầu thuyết minh chi tiết, đầy đủ yêu cầu cơ bản bảo đảm an toàn hệ thống thông tin đối với hệ thống thông tin cấp độ 3 quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông.

5. Yêu cầu về kỹ thuật hạ tầng, điều kiện triển khai

Các giải pháp cung cấp dịch vụ sẽ được cấu hình, cài đặt, tích hợp trên máy chủ, thiết bị, phù hợp với môi trường triển khai tại Phòng máy chủ Chi cục Hải quan Khu vực III.

Đảm bảo các điều kiện triển khai về hạ tầng máy chủ, thiết bị, môi trường để cài đặt, vận hành dịch vụ.

- Sử dụng các máy chủ vật lý hoặc máy chủ ảo tùy thuộc vào yêu cầu của giải pháp: đảm bảo máy chủ có đủ tài nguyên (*CPU, RAM, Lưu trữ*), hiệu năng để đáp ứng yêu cầu của giải pháp.

- Hệ thống phải có khả năng mở rộng dễ dàng khi cần thiết để đáp ứng nhu cầu trong suốt thời gian cung cấp dịch vụ.

- Các hệ điều hành phổ biến bao gồm: Linux, Windows Server.

- Hệ cơ sở dữ liệu: MySQL, PostgreSQL, SQLServer, MongoDB….

- Đảm bảo cung cấp cơ sở vật chất cần thiết để triển khai và cung cấp dịch vụ: mặt bằng, không gian lắp đặt, điện, mạng…

6. Yêu cầu về năng lực, kinh nghiệm

6.1. Yêu cầu về năng lực của nhà cung cấp dịch vụ

Nhà cung cấp dịch vụ có kinh nghiệm trong việc vận hành, quản trị hệ thống và cung cấp dịch vụ an ninh thông tin cho chính phủ điện tử.

- Có chứng nhận đảm bảo Phát triển, vận hành, bảo đảm an ninh mạng, an toàn thông tin; Giám sát và xử lý sự cố an toàn thông tin; Cung cấp sản phẩm, giải pháp và dịch vụ về an ninh mạng, an toàn thông tin ISO 27001:2022.

- Có kinh nghiệm tìm ra các lỗ hổng phổ biến được tiết lộ (CVE - Common Vulnerabilities and Exposures) liên quan các ứng dụng web và thiết bị mạng trong thời hạn là các năm gần đây (có tài liệu hoặc danh sách được công bố trên website của tổ chức. Có >250 CVE (Nhà thầu cung cấp đầy đủ list CVE đã được xác nhận

6.2. Yêu cầu về năng lực nhân sự

Nhà cung cấp dịch vụ phải có đội ngũ nhân sự chuyên môn phù hợp với trách nhiệm quản lý, quản trị dịch vụ đang được bố trí đảm nhận công việc.

Cơ cấu tổ chức về nhân sự chuyên môn của nhà cung cấp dịch vụ cần đáp ứng những yêu cầu tối thiểu như sau:

- *Nhân sự Quản lý kỹ thuật*

+ Số lượng nhân sự: 01 người.

+ Mô tả công việc: Phân tích nâng cao các giải pháp an toàn thông tin bảo mật cho hệ thống đáp ứng các yêu cầu của dịch vụ ứng dụng (Thu thập, xử lý, phân tích log, Phân tích phát hiện tấn công dựa vào phân tích lưu lượng mạng, Phân tích phát hiện tấn công Endpoints Server, Phát hiện, ngăn chặn tấn công lớp ứng dụng, Quản lý, phân tích, cảnh báo).

- *Nhân sự Quản trị, vận hành An toàn thông tin, khai thác hệ thống:*

+ Số lượng nhân sự: 01 người.

+ Mô tả công việc: Thực hiện công việc trực tiếp các giải pháp an toàn thông tin bảo mật cho hệ thống (Thu thập, xử lý, phân tích log: (thiết bị mạng Router, Switch), thiết bị bảo mật (Firewall, NIDS, Endpoint server), hệ điều hành (Linux, Windows), ứng dụng (Web, Mail, DNS, DHCP); Phân tích phát hiện tấn công dựa vào phân tích lưu lượng mạng: Phát hiện tấn công cơ bản lớp mạng, phát hiện kết nối đến máy chủ điều khiển của mã độc; Phân tích phát hiện tấn công Endpoints Server: Phát hiện các hành vi bất thường như Tập tin bị thay đổi, thêm mới trên đường dẫn, Chạy các lệnh nguy hiểm, hành vi như: thay đổi Registry, tự động khởi chạy; Phát hiện, ngăn chặn tấn công lớp ứng dụng: bảo vệ Web hoặc tích hợp với giải pháp có sẵn).

7. Yêu cầu về hỗ trợ kỹ thuật, bảo trì và xử lý sự cố gián đoạn dịch vụ

7.1. Yêu cầu quy trình quản lý sự cố của nhà cung cấp

- Phát hiện sự cố

+ Nhà cung cấp dịch vụ cần bố trí nhân sự liên tục giám sát hệ thống và phát hiện các dấu hiệu bất thường.

+ Sử dụng giải pháp, công cụ để giám sát để nhận cảnh báo về các sự cố tiềm năng.

- Phản ứng sự cố

+ Cam kết thời gian phản ứng không quá 01 giờ từ khi nhận được thông tin về sự cố.

+ Sử dụng quy trình phản ứng nhanh được xác định trước để bắt đầu xử lý sự cố.

- Xử lý sự cố

+ Có biện pháp khắc phục tạm thời để bảo đảm hệ thống không bị gián đoạn.

+ Xác định nguyên nhân của sự cố, tiến hành sửa chữa, khắc phục sự cố đảm bảo chất lượng đã cam kết.

- Báo cáo sự cố

+ Ghi chép chi tiết về sự cố bao gồm: thời gian xảy ra, nguyên nhân, biện pháp khắc phục và thời gian hoàn thành.

+ Cung cấp báo cáo sự cố cho các bên liên quan sau khi vấn đề đã được xử lý.

- Kiểm tra và xác nhận

+ Sau khi sự cố được khắc phục, tiến hành kiểm tra lại toàn bộ hệ thống để bảo đảm sự cố đã được giải quyết triệt để.

+ Xác nhận với chủ đầu tư hoặc các bộ phận liên quan về tình trạng của hệ thống sau khi xử lý.

7.2. Yêu cầu về bảo trì, hỗ trợ kỹ thuật

Nhà cung cấp dịch vụ bảo đảm thực hiện công tác bảo trì định kỳ trong thời gian cung cấp dịch vụ, bao gồm các bản vá lỗi, cập nhập bảo mật và hỗ trợ kỹ thuật bao gồm:

- Cập nhật: Nhà cung cấp dịch vụ có kế hoạch, phương án cập nhập các bản vá lỗi, tính năng kỹ thuật và bảo mật.

- Nâng cấp: Nâng cấp các phiên bản mới của phần mềm, dịch vụ với các chức năng cải tiến hơn trong thời gian cung cấp dịch vụ.

- Việc cập nhật, năng cấp, cải thiện chất lượng tính năng của dịch vụ phải có thông báo bằng văn bản hoặc email đến chủ đầu tư trước 48h.

- Yêu cầu về hỗ trợ kỹ thuật: Cung cấp cả hai hình thức hỗ trợ là online và trực tiếp.

- Hỗ trợ qua online: Qua email, điện thoạt, chát, bảo đảm hỗ trợ 24/7 trong thời gian cung cấp dịch vụ.

- Hỗ trợ trực tiếp: Có kỹ thuật trực tiếp tại địa chỉ cài đặt hệ thống trong thời gian 2h từ khi nhận được phát sinh yêu cầu hỗ trợ.

8. Yêu cầu về tập huấn hướng dẫn, sử dụng

- Thành phần tham gia: Cán bộ, chuyên viên khai thác, sử dụng, quản trị vận hành.

- Hình thức: Tổ chức lớp tập huấn tập trung, hướng dẫn sử dụng trực tiếp với sự hướng dẫn của giảng viên.

- Nội dung tập huấn: Hướng dẫn sử dụng và khai thác quy trình thực hiện xử lý thông tin, khắc phục sự cố và hỗ trợ công tác quản trị, vận hành hệ thống.

- Địa điểm tập huấn: theo yêu cầu của chủ đầu tư.

- Giảng viên, trợ giảng của nhà cung cấp trực tiếp giảng dạy.

III. Các yêu cầu khác

1. Yêu cầu về phòng chống cháy nổ, an toàn triển khai

Trong quá trình thiết lập hạ tầng cung cấp dịch vụ, đơn vị cung cấp dịch vụ phải tuân thủ các điều kiện về phòng chống cháy nổ, cụ thể như sau:

- Về an toàn lao động: có phương án ngăn ngừa hoặc giảm thiểu tác động của các yếu tố nguy hiểm và có hại trong quá trình thi công.

- Trang bị các phương tiện bảo vệ để tạo ra những điều kiện thuận lợi tiện nhất cho cơ thể con người thích ứng với môi trường xung quanh, bảo đảm điều kiện lao động.

- Các phương tiện bảo vệ không gây ra các yếu tố nguy hiểm và có hại trong quá trình thi công.

- Phương tiện bảo vệ cần đáp ứng yêu cầu thẩm mỹ công nghiệp.

- Trong trường hợp khi kết cấu của thiết bị, tổ chức quá trình thi công và phương tiện bảo vệ tập thể chưa đảm bảo an toàn lao động sẽ phải sử dụng các phương tiện bảo vệ cá nhân.

- Về an toàn khi lắp đặt hệ thống: đảm bảo chống cháy nổ, điện, giật, sét, tránh rơi hỏng, rơi rớt thiết bị xuống mặt đất làm hư hại thiết bị, tránh các kết nối gây chạm, chập điện…

- Bảo đảm tuân thủ các điều kiện an ninh quốc phòng cho các hệ thống CNTT theo quy định.

- Về vấn đề bảo đảm an toàn điện, an toàn thiết bị.

+ Việc tháo gỡ dây dẫn, sữa chữa hiệu chỉnh thiết bị điện phải do công nhân có trình độ kỹ thuật về an toàn điện thích hợp vơi từng loại công việc tiến hành.

+ Các thiết bị điện di động, máy điện cầm tay và đèn điện xách tay khi nối vào lưới điện phải qua ổ cắm. Việc đấu nối phải thỏa mãn các yêu cầu về kỹ thật an toàn điện.

+ Trước khi lắp ráp và sửa chữa điện hay thiết bị, phải ngắt điện cho khu vực thao tác, tại cầu dao đó cần có bảng thông báo.

2. Sở hữu thông tin, dữ liệu hình thành trong quá trình cung cấp dịch vụ và phương án quản lý, chuyển giao

2.1. Việc sở hữu thông tin, dữ liệu hình thành trong quá trình cung cấp dịch vụ

Sở hữu các thông tin, dữ liệu hình thành trong quá trình cung cấp dịch vụ tuân thủ quy định tại khoản 4 điều 52 của Nghị định số 73/2019/NĐ-CP (được sửa đổi, bổ sung tại Khoản 30, Điều 1 của Nghị định số 82/2024/NĐ-CP ngày 10/07/2024) cụ thể như sau:

"*Thông tin, dữ liệu hình thành trong quá trình thuê dịch vụ công nghệ thông tin thuộc sở hữu của cơ quan, đơn vị thuê. Nhà cung cấp dịch vụ có trách nhiệm bảo đảm an ninh, an toàn thông tin, chuyển giao đầy đủ cho cơ quan, đơn vị thuê các thông tin, dữ liệu khi kết thúc hợp đồng thuê dịch vụ công nghệ thông tin*".

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

- Thông tin, dữ liệu hình thành trong quá trình thuê dịch vụ CNTT thuộc sở hữu của Bên thuê. Đơn vị cung cấp dịch vụ có trách nhiệm bảo đảm an toàn, bảo mật và tính riêng tư về thông tin, dữ liệu của cơ quan nhà nước; tuân thủ quy định của pháp luật về an toàn, an ninh thông tin, cơ yếu và Luật bảo vệ bí mật nhà nước.

- Đơn vị cung cấp dịch vụ có trách nhiệm chuyển giao đầy đủ các thông tin, dữ liệu thuộc sở hữu của Bên thuê và các công cụ cần thiết khi kết thúc hợp đồng để đảm bảo Bên thuê vẫn có thể khai thác sử dụng dịch vụ được liên tục kể cả trong trường hợp thay đổi đơn vị cung cấp dịch vụ.

- Trong quá trình vận hành hệ thống, Bên thuê sẽ được cung cấp các tài khoản hệ thống để truy cập, quản lý các thông tin dữ liệu do mình sở hữu.

3. Yêu cầu phát sinh trong quá trình khai thác, sử dụng dịch vụ

- Đơn vị cung cấp dịch vụ có cam kết khi phát sinh yêu cầu: về kỹ thuật, chức năng, tính năng của hệ thống, về kết nối, chia sẻ dữ liệu khi Chính phủ hoặc Bộ, ngành liên quan hoặc thành phố yêu cầu hoặc khi có văn bản, quy định mới

liên quan được ban hành. Ngoài ra, đơn vị cung cấp dịch vụ phải có trách nhiệm và cam kết cụ thể về thời gian cập nhật, bổ sung, nâng cấp chức năng trong hợp đồng khi đang trong giai đoạn thuê.

- Đối với hoạt động bảo trì và hỗ trợ hệ thống cần tuân thủ các yêu cầu:

+ Trong trường hợp hệ thống bổ sung, nâng cấp, cải thiện chất lượng các tính năng của hệ thống trong giờ làm việc chính thức, phải có thông báo bằng văn bản hoặc email đến khách hàng trước 48 giờ.

+ Yêu cầu lựa chọn thời điểm bảo trì ngoài giờ hành chính. Tổng thời gian bảo trì không ảnh hưởng tới thời gian sử dụng dịch vụ của khách hàng không quá 02 giờ (120 phút).

+ Bố trí nhân lực phụ trách xử lý, giải quyết các vấn đề vướng mắc, hỏi đáp của người dùng cũng như đơn vị thuê dịch vụ trong quá trình tham gia sử dụng dịch vụ.

+ Cam kết hỗ trợ vận hành 24/7 trong suốt thời gian thuê dịch vụ.

Mục 2. Bản vẽ và hiện trạng

Bản vẽ và hiện trạng theo Phụ lục (đính kèm).

Mục 3. Kiểm tra và thử nghiệm

Các kiểm tra và thử nghiệm cần tiến hành gồm có: Kiểm tra ngoại hình và vận hành thử nghiệm hàng hoá.

Trường hợp hàng hóa không phù hợp với đặc tính kỹ thuật theo hợp đồng thì Bên mời thầu có quyền từ chối và nhà thầu phải có trách nhiệm thay thế hoặc tiến hành những điều chỉnh cần thiết để đáp ứng đúng các yêu cầu về đặc tính kỹ thuật. Trường hợp nhà thầu không có khả năng thay thế hay điều chỉnh hàng hóa không phù hợp, Bên mời thầu có quyền tổ chức việc thay thế hay điều chỉnh nếu thấy cần thiết, mọi rủi ro và chi phí liên quan do Nhà thầu chịu. Việc thực hiện kiểm tra, thử nghiệm hàng hóa của Bên mời thầu không dẫn đến miễn trừ nghĩa vụ bảo hành hay các nghĩa vụ khác theo hợp đồng của Nhà thầu.

Tất các dịch vụ trước khi đưa vào vận hành chính thức phải triển khai vận hành thử, nội dung vận hành thử bao gồm: Kiểm tra về chức năng và kiểm tra về hiệu năng:

- Yêu cầu tài liệu phục vụ vận hành thử:

+ Tài liệu mô tả yêu cầu của hệ thống;

+ Tài liệu hướng dẫn người sử dụng, bao gồm cả người sử dụng là cán bộ quản trị hệ thống;

+ Tài liệu mô tả yêu cầu kỹ thuật cần đáp ứng của dịch vụ;

+ Tài liệu mô tả yêu cầu hạ tầng kỹ thuật cần đáp ứng về môi trường vận hành, khai thác dịch vụ;

+ Kế hoạch vận hành thử do nhà thầu triển khai lập đã được chủ đầu tư thông qua;

+ Hồ sơ báo cáo kết quả kiểm thử nội bộ hoặc kết quả kiểm thử dịch vụ mới nhất (nếu có).

- Trình tự, thủ tục vận hành thử:

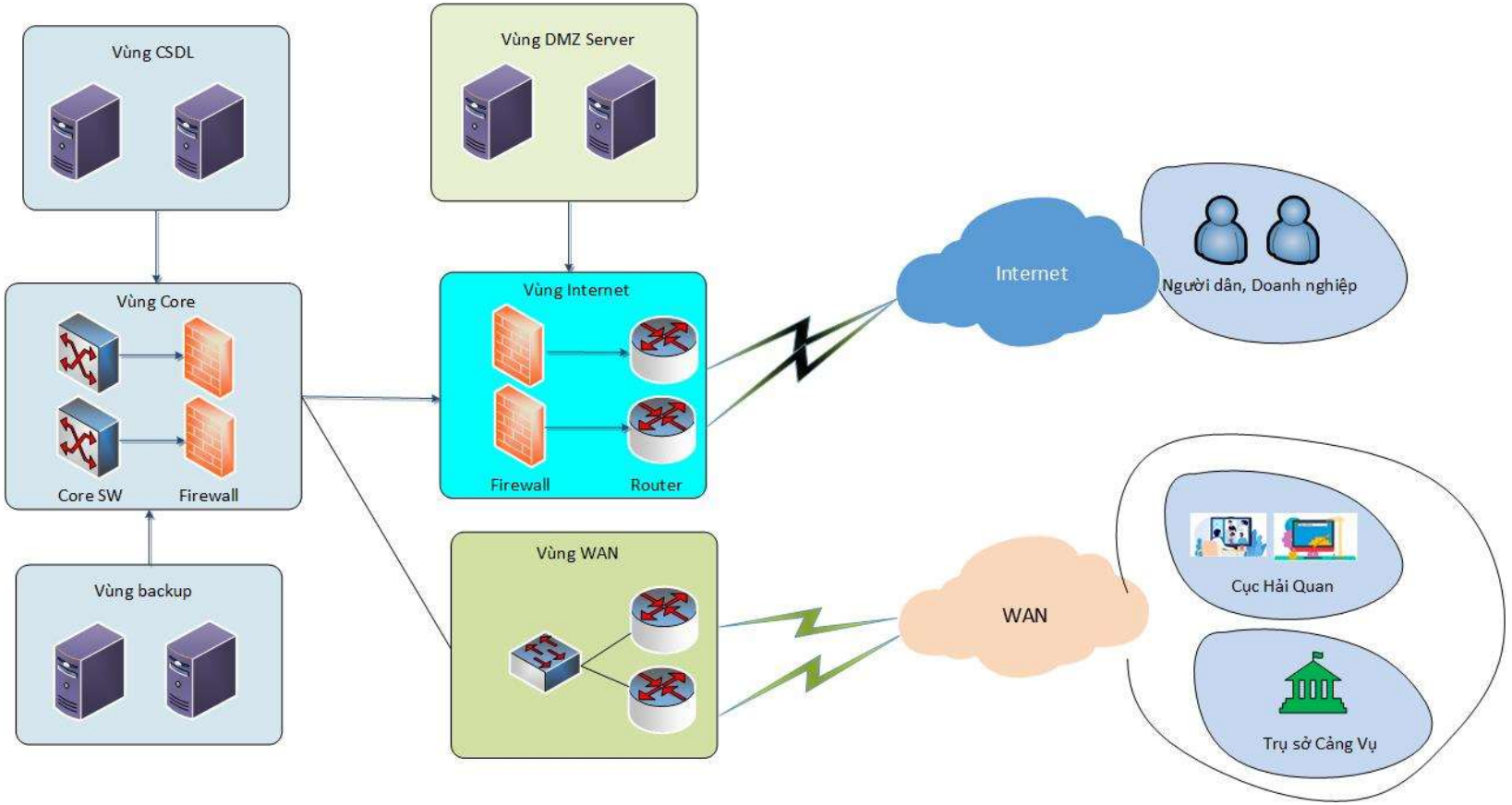
Bao gồm các bước như sau: lập kế hoạch vận hành thử; xây dựng tình huống, kịch bản vận hành thử; thực hiện vận hành thử; lập báo cáo kết quả vận hành thử.

- Chi phí vận hành thử: đã bao gồm trong chi phí thuê dịch vụ.

PHỤ LỤC. HIỆN TRẠNG MÔ HÌNH HỆ THỐNG VÀ CÁC THIẾT BỊ MẠNG

1. Mô hình hệ thống

1.1. Mô hình hạ tầng



Mô tả:

Hệ thống quản lý thu phí sử dụng công trình kết cấu hạ tầng, công trình dịch vụ, tiện ích công cộng trong khu vực cửa khẩu cảng biển Hải Phòng hiện đang đặt tại Phòng máy chủ Chi cục Hải Quan Khu vực III được đưa vào sử dụng vận hành từ năm 2018 và được đầu tư, nâng cấp một lần vào năm 2020. Hệ thống được đầu tư các thiết bị như máy chủ, thiết bị lưu trữ, thiết bị mạng, thiết bị bảo mật, phần mềm hệ thống.

- Về thiết kế các vùng mạng: Các vùng mạng được thiết kế như sau:

+ Vùng Internet (mạng biên): Hệ thống tường lửa (firewall) phục vụ quản lý kết nối giữa Internet với hệ thống.

+ Vùng DMZ server: Đặt các máy chủ cung cấp dịch vụ ra bên ngoài Internet.

+ Vùng Core: Hệ thống Firewall thiết lập cơ chế quản lý, giám sát, điều hướng người dùng và dữ liệu trong hệ thống.

+ Vùng WAN: Quản lý đường truyền số liệu chuyên dùng kết nối thông qua mạng viễn thông (Metronet) đến các điểm thu phí.

+ Vùng CSDL: Đặt các máy chủ cơ sở dữ liệu của hệ thống.

+ Vùng backup (sao lưu): Hệ thống lưu trữ tài nguyên dữ liệu và chia sẻ dữ liệu tự động với vùng ứng dụng.

- Về thiết bị, giải pháp an toàn thông tin: Hệ thống được trang bị các giải pháp, phương án an toàn thông tin bao gồm:

+ Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu: Sử dụng cặp thiết bị tường lửa Firewall Cisco FirePower 2110 NGFW Appliance.

+ Phương án giám sát hệ thống thông tin tập trung: Hiện đang sử dụng Netdata làm công cụ giám sát toàn bộ hệ thống.

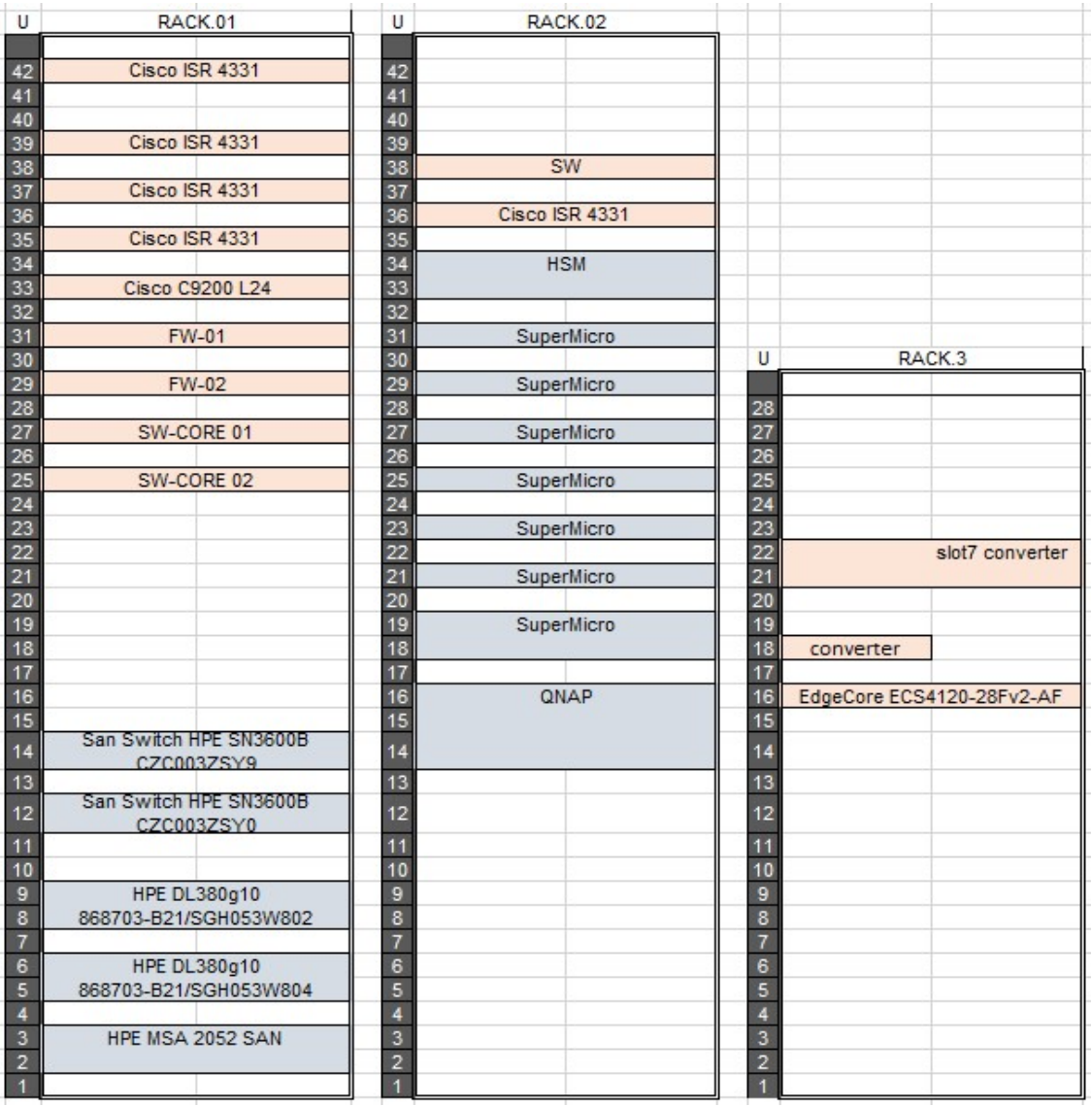
+ Giải pháp phòng chống mã độc cho máy chủ: Sử dụng giải pháp Kaspersky antivirus tập trung.

+ Giải pháp quản lý sao lưu dự phòng tập trung: Sử dụng phần mềm Veeam Backup & Replication để sao lưu dữ liệu thường xuyên (hàng ngày), dữ liệu của hệ thống được lưu trữ cùng mã kiểm tra tính nguyên vẹn sử dụng MD5 và lưu trữ trên hệ thống SAN HPE của hãng HP, có năng lực quản lý và lưu trữ 24TB dữ liệu.

+ Phương án duy trì ít nhất 02 kết nối mạng: Hiện có 02 đường WAN kết nối đến Cổng thanh toán 24/7 của Cục Hải quan (*01 đường chính, 01 dự phòng*); 02 WAN kết nối với Cảng vụ đường thủy nội địa; 02 đường internet IP tĩnh (tiếp nhận thông tin khai báo tờ khai phí của doanh nghiệp và trao đổi thông tin với doanh nghiệp kho, bãi, cảng).

1.2. Mô hình vật lý

- Rack 1



U	RACK.01
42	Cisco ISR 4331
41	
40	
39	Cisco ISR 4331
38	
37	Cisco ISR 4331
36	
35	Cisco ISR 4331
34	
33	Cisco C9200 L24
32	
31	FW-01
30	
29	FW-02
28	
27	SW-CORE 01
26	
25	SW-CORE 02
24	
23	
22	
21	
20	
19	
18	
17	
16	
15	
14	San Switch HPE SN3600B CZC003ZSY9
13	
12	San Switch HPE SN3600B CZC003ZSY0
11	
10	
9	HPE DL380g10
8	868703-B21/SGH053W802
7	
6	HPE DL380g10
5	868703-B21/SGH053W804
4	
3	HPE MSA 2052 SAN
2	
1	

U	RACK.02
42	
41	
40	
39	
38	SW
37	
36	Cisco ISR 4331
35	
34	HSM
33	
32	
31	SuperMicro
30	
29	SuperMicro
28	
27	SuperMicro
26	
25	SuperMicro
24	
23	SuperMicro
22	
21	SuperMicro
20	
19	SuperMicro
18	
17	
16	QNAP
15	
14	
13	
12	
11	
10	
9	
8	
7	
6	
5	
4	
3	
2	
1	

U	RACK.3
28	
27	
26	
25	
24	
23	
22	slot7 converter
21	
20	
19	
18	converter
17	
16	EdgeCore ECS4120-28Fv2-AF
15	
14	
13	
12	
11	
10	
9	
8	
7	
6	
5	
4	
3	
2	
1	

U	RACK.01	Detail on server	Port	card	cable	Label	Thiết bị kết nối tới							note
							Label	RACK	Unit	port	Name	Device	SN	
42	**ROUTER-NB 01** Cisco ISR 4331		mgmt	copper				RACK.01	27	1				
			Ge0/0/0	copper				RACK.01	40	1				
			Ge0/0/1	copper				Rack.10	16	13	Tủ quang	EdgeCore ECS4120-28Fv2-AF	EC2127000719	
			Ge0/0/2	copper				Rack.10	16	12	Tủ quang	EdgeCore ECS4120-28Fv2-AF	EC2127000719	
41														
40	ASA5506 X		mgmt	copper				RACK.01	27	3				
			1	copper				RACK.01	42	Ge0/0/0				
			2	copper				RACK.01	25	24				
			3	copper				RACK.01	27	24				
39	**ROUTER-NB 02**		mgmt	copper				RACK.01	27	2				
38														
37	**ROUTER-WAN 01** Cisco ISR 4331		mgmt	copper				RACK.01	25	1				
			Ge0/0/0	copper				RACK.01	27	21				
			Ge0/0/1	copper				RACK.01	33	20				
36														
35	**ROUTER-WAN 02** Cisco ISR 4331		mgmt	copper				RACK.01	25	2				
			Ge0/0/0	copper				RACK.01	25	21				
			Ge0/0/1	copper				RACK.01	33	22				
34														
33	Cisco C9200 L24 SSI2442046P		3	copper				RACK.10	21-22	slot7 NIC	Tủ quang	converter 3onedata	14 chassis converte	
			7	copper				RACK.10	16	8	Tủ quang	EdgeCore ECS4120-28Fv2-AF	EC2127000719	
			11	copper								user		
			13	copper								user		
			19	copper				RACK.10	18	NIC	Tủ quang	converter 3onedata	VAG1019000902	
			20	copper				RACK.01	37	Ge0/0/1				
			22	copper				RACK.01	35	Ge0/0/1				
			23	copper				RACK.01	25	23				
			24	copper				RACK.01	27	23				
32														
31	**FW-01** Cisco FPR-2100		mgmt	copper				RACK.01	27	5				
			WAN1	copper				RACK.01	27	22				
			WAN2	copper				RACK.01	27	20				
30														
29	**FW-02**		mgmt	copper				RACK.01	27	4				
			WAN1	copper				RACK.01	25	22				
			WAN2	copper				RACK.01	25	20				
28														

U	RACK.01	Detail on server	Port	card	cable	Label	Thiết bị kết nối tới							note
							Label	RACK	Unit	port	Name	Device	SN	
27	**SW-CORE 01** Cisco Catalyst 9300-NM-8X FOC2502L2NT		1	copper				RACK.01	42	mgmt				
			2	copper				RACK.01	39	mgmt				
			3	copper				RACK.01	40	mgmt				
			4	copper				RACK.01	29	mgmt				
			5	copper				RACK.01	31	mgmt				
			7	copper				RACK.01	2-3	Ctrl1 mgmt				
			8	copper				RACK.01	14	mgmt				
			9	copper				RACK.01	8-9	iLO				
			11	copper				RACK.02	39	11				
			12	copper				RACK.02	14-16	4				
			13	copper				RACK.01	5-6	NIC 4				
			14	copper				RACK.01	8-9	NIC 2				
			15	copper				RACK.01	5-6	NIC 2				
			16	copper				RACK.01	8-9	NIC 4				
			17	copper				RACK.02	33-34	NIC 2	HSM			
			20	copper				RACK.01	31	WAN2				
			21	copper				RACK.01	37	Ge0/0/0				
			22	copper				RACK.01	31	WAN1				
			23	copper				RACK.01	33	24				
			24	copper				RACK.01	40	3				
			TE1	fc	SRV-01 LINK2 SW-CORE01 TE.01	SRV-01 LINK2 SW-CORE01 TE.01	RACK.01	8-9	Flex	1	SERVER 01	HPE DL380g10	SGH053W802	0420
			TE2	fc	SRV-02 LINK2 SW-CORE01 TE.02	SRV-02 LINK2 SW-CORE01 TE.02	RACK.01	5-6	Flex	1	SERVER 02	HPE DL380g10	SGH053W804	0199
26														
25	**SW-CORE 02** Cisco Catalyst 9300-NM-8X FOC2503L721		1	copper				RACK.01	37	mgmt				
			2	copper				RACK.01	35	mgmt				
			3	copper				RACK.01	23	mgmt				
			4	copper				RACK.01	12	mgmt				
			5	copper				RACK.01	5-6	iLO				
			12	copper				RACK.02	14-16	3	QNAP			
			13	copper				RACK.01	5-6	NIC 1				
			14	copper				RACK.01	8-9	NIC 1				
			15	copper				RACK.01	5-6	NIC 3				
			16	copper				RACK.01	8-9	NIC 3				
			20	copper										
			21	copper				RACK.02	35		Ge0/0/0			
			22	copper										
			23	copper				RACK.01	33	23				
			24	copper				RACK.01	40	2				
			TE1	fc	SRV-01 LINK1 SW-CORE02 TE.01	SRV-01 LINK1 SW-CORE02 TE.01	RACK.01	8-9	Flex	2	SERVER 01	HPE DL380g10	SGH053W802	0443
			TE2	fc	SRV-02 LINK1 SW-CORE TE.02	SRV-02 LINK1 SW-CORE TE.02	RACK.01	5-6	Flex	2	SERVER 02	HPE DL380g10	SGH053W804	0448

U	RACK.01	Detail on server	Port		cable	Label	Thiết bị kết nối tới							note
			serve	card			Label	RACK	Unit	port	Name	Device	SN	
				mgmt	copper	SAN-SW01 MGMT SW-CORE01 P.08		RACK.01	27	8				21
14	**SAN-SW01** HPE SN3600B R4G55A/CZC003ZSY0			0	fc	SAN Port1 SAN-SW01 P.00	SAN PORT1 SAN-SW01 P.00	RACK.01	2-3	Ctrl0 1	MSA	HPE MSA 2052 SAN		0448
				1	fc	SRV-01 FC.02 SAN-SW01 P.01	SRV-01 FC.02 SAN-SW01 P.01	RACK.01	9-10	PCI1 2	SERVER 01	HPE DL380g10	SGH053W802	0010
				4	fc	SAN Port1 SAN-SW01 P.04	SAN PORT1 SAN-SW01 P.04	RACK.01	2-3	Ctrl1 1	MSA	HPE MSA 2052 SAN		0003
				5	fc	SRV-02 FC.02 SAN-SW01 P.05	SRV-02 FC.02 SAN-SW01 P.05	RACK.01	5-6	PCI1 2	SERVER 02	HPE DL380g10	SGH053W804	0268
13														
				mgmt	copper	SAN-SW02 MGMT SW-CORE02 P.04		RACK.01	25	4				19
12	**SAN-SW02** HPE SN3600B CZC003ZSY9			0	fc	SAN Port2 SAN-SW02 P.00	SAN PORT2 SAN-SW02 P.00	RACK.01	2-3	Ctrl0 2	MSA	HPE MSA 2052 SAN		0012
				1	fc	SRV-01 FC.01 SAN-SW01 P.01	SRV-01 FC.01 SAN-SW P.01	RACK.01	8-9	PCI1 1	SERVER 01	HPE DL380g10	SGH053W802	0209
				4	fc	SAN Port2 SAN-SW02 P.04	SAN PORT2 SAN-SW02 P.04	RACK.01	2-3	Ctrl1 2	MSA	HPE MSA 2052 SAN		0038
				5	fc	SRV-02 FC.01 SAN-SW02 P.05	SRV-02 FC.01 SAN-SW02 P.05	RACK.01	5-6	PCI1 1	SERVER 02	HPE DL380g10	SGH053W804	0569
11														
10														
9	**SERVER 01** HPE DL380g10 868703-B21/SGH053W802		PCI 1	1	fc	SRV-01 FC.01 SAN-SW P.01	SRV-01 FC.01 SAN-SW01 P.01	RACK.01	12	1	SAN-SW02	HPE SN3600B	CZC003ZSY9	0209
			PCI 1	2	fc	SRV-01 FC.02 SAN-SW01 P.01	SRV-01 FC.02 SAN-SW01 P.01	RACK.01	14	1	SAN-SW01	HPE SN3600B	CZC003ZSY0	0010
			Flex	2	fc	SRV-01 LINK1 SW-CORE02 TE.01	SRV-01 LINK1 SW-CORE02 TE.01	RACK.01	25	TE1	SW-CORE 02	Cisco Catalyst 9300-NM-8X	FOC2503L721	0443
			Flex	1	fc	SRV-01 LINK2 SW-CORE01 TE.01	SRV-01 LINK2 SW-CORE01 TE.01	RACK.01	27	TE1	SW-CORE 01	Cisco Catalyst 9300-NM-8X	FOC2502L2NT	0420
				iLO	copper	SRV-01 ILO SW-CORE01 P.09		RACK.01	27	9				20
			NIC	1	copper	SRV-01 P.01 SW-CORE02 P.14		RACK.01	25	14				8
			NIC	2	copper	SRV-01 P.02 SW-CORE01 P.14		RACK.01	27	14				7
			NIC	3	copper	SRV-01 P.03 SW-CORE02 P.16		RACK.01	25	16				9
8			NIC	4	copper	SRV-01 P.04 SW-CORE01 P.16		RACK.01	27	16				16

U	RACK.01	Detail on server	Port		cable	Label	Thiết bị kết nối tới							note	
			serve	card			Label	RACK	Unit	port	Name	Device	SN		
8			NIC	4	copper	SRV-01 P.04 SW-CORE01 P.16		RACK.01	27	16				16	v
7															
6	**SERVER 02** HPE DL380g10 868703-B21/SGH053W804		PCI 1	1	fc	SRV-02 FC.01 SAN-SW02 P.05	SRV-02 FC.01 SAN-SW02 P.05	RACK.01	12	5	SAN-SW02	HPE SN3600B	CZC003ZSY9	0569	
			PCI 1	2	fc	SRV-02 FC.02 SAN-SW01 P.05	SRV-02 FC.02 SAN-SW01 P.05	RACK.01	14	5	SAN-SW01	HPE SN3600B	CZC003ZSY0	0268	
			Flex	2	fc	SRV-02 LINK1 SW-CORE TE.02	SRV-02 LINK1 SW-CORE TE.02	RACK.01	25	TE2	SW-CORE 02	Cisco Catalyst 9300-NM-8X	FOC2503L721	0448	
			Flex	1	fc	SRV-02 LINK2 SW-CORE01 TE.02	SRV-02 LINK2 SW-CORE01 TE.02	RACK.01	27	TE2	SW-CORE 01	Cisco Catalyst 9300-NM-8X	FOC2502L2NT	0199	
				iLO	copper	SRV-02 ILO SW-CORE02 P.05		RACK.01	25	5				24	v
			NIC	1	copper	SRV-02 P.01 SW-CORE02 P.13		RACK.01	25	13				22	v
			NIC	2	copper	SRV-02 P.02 SW-CORE01		RACK.01	27	15				10	v
			NIC	3	copper	SRV-02 P.03 SW-CORE02		RACK.01	25	15				12	v
5			NIC	4	copper	SRV-02 P.04 SW-CORE01		RACK.01	27	13				11	v
4															
3	**MSA** HPE MSA 2052 SAN Q1J01B/ACM102T1ZW	Controller-A	Ctrl 1	1	fc	SAN PORT1 SAN-SW01 P.04	SAN Port1 SAN-SW01 P.04	RACK.01	14	4	SAN-SW01	HPE SN3600B	CZC003ZSY0	0003	
		Controller-A	Ctrl 1	2	fc	SAN PORT2 SAN-SW02 P.04	SAN Port2 SAN-SW02 P.04	RACK.01	12	4	SAN-SW02	HPE SN3600B	CZC003ZSY9	0038	
		Controller-A	Ctrl 1	mgmt	copper	SAN P.01 SW-CORE01		RACK.01	27	7				25	SW-Core01-P7
		Controller-B	Ctrl 0	1	fc	SAN PORT1 SAN-SW01 P.00	SAN Port1 SAN-SW01 P.00	RACK.01	14	0	SAN-SW01	HPE SN3600B	CZC003ZSY0	0448	
		Controller-B	Ctrl 0	2	fc	SAN PORT2 SAN-SW02 P.00	SAN Port2 SAN-SW02 P.00	RACK.01	12	0	SAN-SW02	HPE SN3600B	CZC003ZSY9	0012	
2		Controller-B	Ctrl 0	mgmt	copper	SAN P.02 SW-CORE01		RACK.01	25	3				23	SW-Core02-P3

- Rack 2

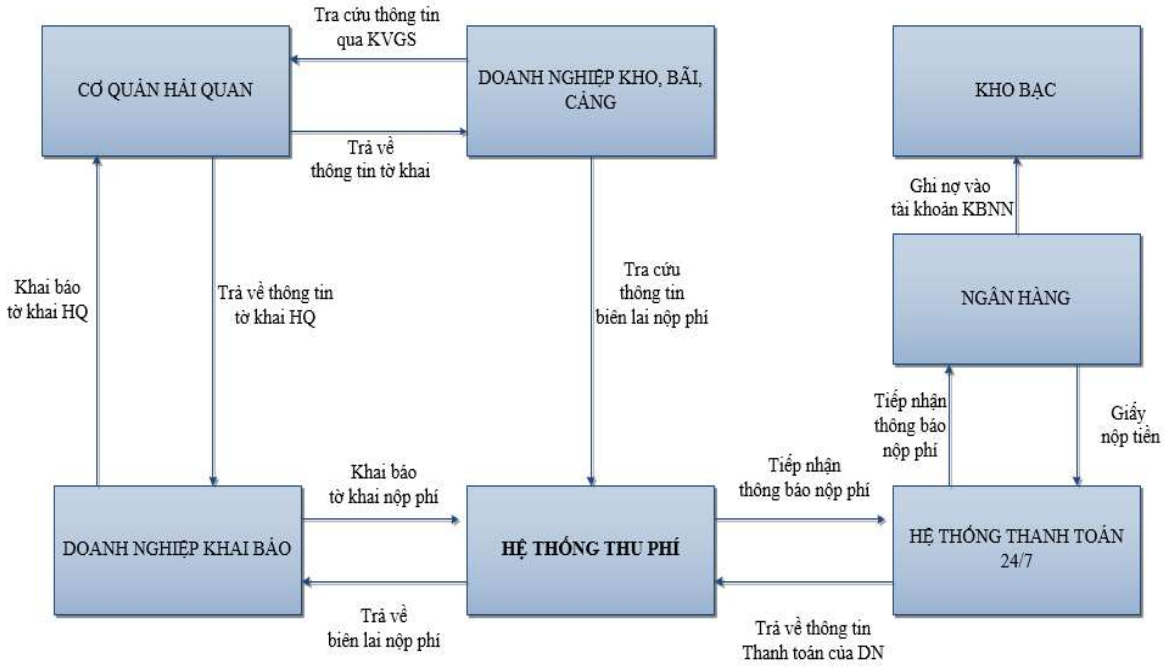
U	RACK.02	Detail on server	Port server	Port card	cable	Label	Thiết bị kết nối tới Label	RACK	Unit	port	Name	Device	SN
42													
41													
40													
39	SW-Thuphi Cisco 2960-X			3	copper			RACK.02	29	NIC 1			
				4	copper			RACK.02	31	NIC 1			
				11	copper	SW-THUPHI old SW-CORE01 P11	SW-THUPHI old SW-CORE01 P11	RACK.01	27	11	SW-CORE 01	Cisco Catalyst 9300-N	FOC2502L2NT
				13	copper			RACK.02	23	NIC 1			
				14	copper			RACK.02	18-19	NIC 1			
				15	copper			RACK.02	21	NIC 1			
				16	copper			RACK.02	18-19	NIC 4			
				17	copper								
				18	copper			RACK.02	14-16	NIC 1			
				19	copper			RACK.02	18-19	NIC 3			
				20	copper			RACK.02	14-16	NIC 2			
				21	copper			RACK.02	25	NIC 1			
				22	copper			RACK.02	27	NIC 1			
				23	copper			RACK.02	35	3			
				24	copper			RACK.02	35	4			
38													
37	Cisco 4300 Series												
36													
35	FW-Thuphi ASA5506-X			3	copper	19		RACK.02	39	23	SW-Thuphi	Cisco 2960-X	
				4	copper			RACK.02	39	24	SW-Thuphi	Cisco 2960-X	
34	HSM utimaco			NIC 2	copper	HSM1		RACK.01	27	17	SW-CORE 01	Cisco Catalyst 9300-N	FOC2502L2NT
33													
32													
31	HA-Server-02 SuperMicro			NIC 1	copper	HA-Server-02-Port1 SW-Thuphi-Port Gi0/2		RACK.02	39	4	SW-Thuphi	Cisco 2960-X	
30													
29	HA-Server-01 SuperMicro			NIC 1	copper	HA-Server-01-Port1 SW-Thuphi-Port Gi0/1		RACK.02	39	3	SW-Thuphi	Cisco 2960-X	
28													
27	Web-Server-01 SuperMicro			NIC 1	copper	Web-Server-01 SW-Thuphi-Port F0/22		RACK.02	39	22	SW-Thuphi	Cisco 2960-X	
26													
25	Web-Server-02 SuperMicro			NIC 1	copper	Web-Server-02 SW-Thuphi-Port F0/21		RACK.02	39	21	SW-Thuphi	Cisco 2960-X	

U	RACK.02	Detail on server	Port server	Port card	cable	Label	Thiết bị kết nối tới Label	RACK	Unit	port	Name	Device	SN
25	Web-Server-02 SuperMicro			NIC 1	copper	Web-Server-02 SW-Thuphi-Port F0/21		RACK.02	39	21	SW-Thuphi	Cisco 2960-X	
24													
23	DB-Server-02 SuperMicro			NIC 1	copper	SW-Thuphi-Port F0/13 DB-Server-02		RACK.02	39	13	SW-Thuphi	Cisco 2960-X	
22													
21	DB-Server-01 SuperMicro			NIC 1	copper	DB-Server-01 SW-Thuphi-Port F0/15		RACK.02	39	15	SW-Thuphi	Cisco 2960-X	
20													
19	DC-Server SuperMicro			NIC1	copper	DB-Server-02 SW-Thuphi-Port F0/14		RACK.02	39	14	SW-Thuphi	Cisco 2960-X	
				NIC 3	copper	DC-Server SW-Thuphi-Port F0/19		RACK.02	39	19	SW-Thuphi	Cisco 2960-X	
18				NIC 4	copper	DB-Server-01 SW-Thuphi-Port F0/16		RACK.02	39	16	SW-Thuphi	Cisco 2960-X	
17													
16	QNAP-Server QNAP			NIC 3	copper	QNAP P0/3 SW-CORE02 P/12		RACK.01	25	12	SW-CORE 02	Cisco Catalyst 9300-N	FOC2503L721
				NIC 1	copper			RACK.02	39	18	SW-Thuphi	Cisco 2960-X	
15				NIC 4	copper	QNAP P0/4 SW-CORE01 P/12		RACK.10	27	12	SW-CORE 01	Cisco Catalyst 9300-N	FOC2502L2NT
14				NIC 2	copper	16		RACK.02	39	20	SW-Thuphi	Cisco 2960-X	

- Rack 3

U	RACK.3	Detail on server	Port server	Port card	cable	Label	Thiết bị kết nối tới Label	RACK	Unit	port	Name	Device	SN	note
#														
#														
#														
#														
#														
#														
#	slot7 converter			NIC	copper			RACK.01	33	3		Cisco C9200 L24		VNNET
#														
#														
#	converter 3onedata VAG10190009			NIC	copper			RACK.01	33	19		Cisco C9200 L24		VNNET
#														
#	EdgeCore ECS4120-28Fv2-AF EC2127000719			8	copper			RACK.01	33	7		Cisco C9200 L24		VNPT xuống Cảng Vụ
				12	copper			RACK.01	42	Ge0/0/2	ROUTER-NB 01	Cisco ISR 4331		
				13	copper			RACK.01	42	Ge0/0/1	ROUTER-NB 01	Cisco ISR 4331		
#				19	copper			RACK.01	33	21		Cisco C9200 L24		VNPT (chưa đấu nối trên tổng cục)

1.3. Mô hình triển khai phần mềm



Mô tả:

- Doanh nghiệp xuất nhập khẩu (XNK)

+ Thực hiện khai báo tờ khai XNK, danh sách container của tờ khai đến hệ thống VNACCS/VCIS của Hải quan. Nhận kết quả chấp nhận thông quan hàng hóa từ hệ thống của Hải quan.

+ Thực hiện khai báo tờ khai nộp phí cơ sở hạ tầng đến hệ thống thu phí. Nhận kết quả thu phí được trả về từ hệ thống thu phí.

+ Thực hiện nộp phí bằng các kênh thanh toán.

+ Quản lý thông tin tờ khai XNK, tờ khai nộp phí, biên lai phí của Doanh nghiệp.

- Cơ quan Hải quan

+ Tiếp nhận tờ khai XNK và danh sách Container của tờ khai, thực hiện kiểm tra, giám sát thông quan hàng hóa trên hệ thống VNACCS/VCIS.

+ Cung cấp hệ thống tra cứu phục vụ việc tra cứu thông tin tờ khai đủ điều kiện qua khu vực giám sát.

+ Đồng bộ dữ liệu tờ khai Hải quan đến hệ thống Thu phí để thực hiện đối soát dữ liệu.

- Hệ thống thu phí

+ Tiếp nhận tờ khai nộp phí từ Doanh nghiệp, trả kết quả xử lý.

+ Thực hiện tạo lập biên lai thu lệ phí từ thông tin tờ khai nộp phí của doanh nghiệp, trả thông tin biên lai về cho doanh nghiệp.

+ Gửi thông báo nộp phí đến Hệ thống thanh toán 24/7 của Cục Hải quan.

+ Cung cấp hệ thống tra cứu biên lai phục vụ việc tra cứu thông tin biên lai từ Doanh nghiệp kinh doanh Cảng.

+ Hệ thống tiếp nhận dữ liệu tờ khai gửi sang cơ quan Hải quan để phục vụ việc đối soát dữ liệu.

+ Hệ thống quản lý dữ liệu thu phí tự động.

+ Quản lý đối soát dữ liệu với cơ quan Hải quan.

- Doanh nghiệp kinh doanh Cảng

+ Tra cứu thông tin tờ khai đủ điều kiện qua khu vực giám sát.

+ Tra cứu thông tin biên lai nộp lệ phí của tờ khai.

- Hệ thống thanh toán 24/7

+ Tiếp nhận thông báo nộp phí từ hệ thống thu phí.

+ Chuyển thông tin nộp phí của doanh nghiệp cho Ngân hàng.

+ Trả thông tin thanh toán của doanh nghiệp về cho hệ thống thu phí.

- Đối tác thanh toán - ngân hàng, kho bạc.

+ Tiếp nhận thông tin giấy báo nộp tiền.

+ Trích tiền từ tài khoản doanh nghiệp gửi về kho bạc nhà nước.

+ Trả kết quả trích nộp tiền về Hệ thống thanh toán 24/7.

- Danh sách tên miền hệ thống và cổng dịch vụ:

STT	TÊN MIỀN	MỤC ĐÍCH SỬ DỤNG
1	thuphi.haiphong.gov.vn:8220	GetIn/GetOut Cảng trả về cho hệ thống thu phí; Kết nối với phần mềm khai báo hải quan
2	thuphi.haiphong.gov.vn:8221	Giao diện cho đơn vị thu phí
3	thuphi.haiphong.gov.vn:8222	Giao diện cho người dân, doanh nghiệp
4	thuphi.haiphong.gov.vn:8223	Giao diện đối soát biên lai với Hải quan
5	thuphi.haiphong.gov.vn:8224	Giao diện kết nối hóa đơn điện tử
6	thuphi.haiphong.gov.vn:8225	Giao diện kết nối hóa đơn điện tử

STT	TÊN MIỀN	MỤC ĐÍCH SỬ DỤNG
7	thuphi.haiphong.gov.vn:8522	Cung cấp giao diện cho đơn vị Kho, Bãi, Cảng

2. Danh sách thiết bị mạng trong hệ thống

STT	Tên thiết bị/Chủng loại	Số lượng	Mục đích sử dụng
1	Máy chủ HPE ProLiant DL380 Gen10 8SFF	02	Máy chủ quản lý ảo hóa
2	Thiết bị lưu trữ HPE MSA 2052 SAN Dual Controller SFF Storage	01	Storage (Lưu trữ CSDL và file ảo hóa các máy chủ)
3	SAN Switch HPE SN3600B 16Gb 24/8 8-port Short Wave SFP+ Fibre Chanel Switch	02	SAN Switch
4	Switch Cisco Cat9300 24-port data only	02	Thiết bị chuyển mạch lõi (Core Switch)
5	Firewall Cisco ASA5506-X w/FirePower Services	02	Firewall vào/ra Internet
6	Thiết bị tường lửa Firewall Cisco FirePower 2110 NGFW Appliance, 1U	02	Firewall cơ sở dữ liệu
7	Router Cisco ISR 4331 Sec bundle w/SEC license	02	Định tuyến Internet : 02 đường internet VNPT public dịch vụ (400Mbps/Kênh)
8	Router WAN Cisco ISR 4331 Sec bundle w/SEC license	02	Định tuyến WAN - 02 Kênh Metronet giữa Phòng máy chủ Hệ thống thu phí và Cảng Vụ (Số 1 Cù Chính Lan Hải Phòng) - 02 Kênh metronet giữa Phòng máy chủ Hệ thống thu phí và Cục Hải quan (đặt tại Hà Nội)
9	Máy chủ CSE-813MTQ-600CB	02	Quản trị các hệ thống VCenter (ảo hóa), VeeamSRV-BK (Backup), Kaspersky Server, Firewall mềm
10	Router WAN Switch Cisco Cat9200L 24-port data	01	Thiết bị chuyển mạch WAN (WAN Switch) - Tập trung các

STT	Tên thiết bị/Chủng loại	Số lượng	Mục đích sử dụng
			kênh truyền của nhà cung cấp dịch vụ
11	Thiết bị lưu trữ QNAP	01	Backup CSDL SQL và các máy ảo hóa
12	Thiết bị ký số HSM Security Server Se12 LAN V4	01	Thiết bị phục vụ giải pháp ký số nội bộ
13	Máy chủ CSE-826BE1C-R920LPB	07	Máy chủ dạng Supermicro- hiện dùng để dự phòng và thử nghiệm

3. Đánh giá về các giải pháp, phương án an toàn thông tin hiện tại so với yêu cầu kỹ thuật hệ thống thông tin cấp độ 3

STT	Yêu cầu	Ghi chú/Mô tả	Đáp ứng/chưa đáp ứng
1	Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Hiện chỉ cho phép truy cập, quản trị hệ thống từ mạng nội bộ, không cho phép quản trị hệ thống từ ngoài internet). Tuy nhiên việc quản trị hệ thống từ mạng nội bộ đang sử dụng giải pháp Remote Desktop Protocol (gọi tắt là RDP) không thiết lập các cơ chế mã hóa để bảo đảm kênh truyền an toàn khi sử dụng kết nối	**Chưa đáp ứng**
2	Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Các thiết bị firewall chỉ có tính năng firewall cơ bản, license IPS/IDS đã hết hạn.	**Chưa đáp ứng**
3	Phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính	Các thiết bị mạng chính, server đều có dự phòng nóng Tuy nhiên chỉ có một thiết bị ký số HSM	**Chưa đáp ứng**
4	Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu	Sử dụng cặp thiết bị tường lửa Firewall Cisco FirePower 2110 NGFW Appliance, tuy nhiên thiết bị đã hết license và chỉ là tường lửa lớp mạng, không có những tính năng chuyên biệt cho việc bảo vệ cơ sở dữ liệu	**Chưa đáp ứng**

STT	Yêu cầu	Ghi chú/Mô tả	Đáp ứng/chưa đáp ứng
5	Phương án chặn lọc phần mềm độc hại trên môi trường mạng	Các thiết bị firewall chỉ có tính năng firewall cơ bản, license antivirus trên môi trường mạng đã hết hạn.	**Chưa đáp ứng**
6	Phương án phòng chống tấn công từ chối dịch vụ	Hệ thống chưa được trang bị giải pháp này	**Chưa đáp ứng**
7	Phương án giám sát hệ thống thông tin tập trung	Hiện đang sử dụng Netdata làm công cụ giám sát toàn bộ hệ thống	Đáp ứng
8	Phương án giám sát an toàn hệ thống thông tin tập trung	Hệ thống chưa được trang bị giải pháp này	**Chưa đáp ứng**
9	Phương án quản lý sao lưu dự phòng tập trung	Sử dụng phần mềm Veeam Backup & Replication để sao lưu dữ liệu thường xuyên (hàng ngày), dữ liệu của hệ thống được lưu trữ cùng mã kiểm tra tính nguyên vẹn sử dụng MD5 và lưu trữ trên hệ thống SAN HPE của hãng HP, có năng lực quản lý và lưu trữ 24TB dữ liệu.	Đáp ứng
10	Có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung	Sử dụng giải pháp của Kaspersky tập trung	Đáp ứng
11	Có phương án phòng, chống thất thoát dữ liệu	Hệ thống chưa được trang bị giải pháp này	**Chưa đáp ứng**
12	Có phương án dự phòng kết nối mạng Internet cho hệ thống	Sử dụng đồng thời 2 kết nối Internet và Metronet của 2 nhà cung cấp dịch vụ khác nhau.	Đáp ứng
13	Có phương án bảo đảm an toàn cho mạng không dây	Hệ thống không thiết lập phân hệ này.	Đáp ứng
14	Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng Sản phẩm Tường lửa ứng dụng web	Hệ thống chưa được trang bị giải pháp này	**Chưa đáp ứng**