CẢNG VỤ ĐƯỜNG THỦY NỘI ĐỊA

*** * ***

PHỤ LỤC
YÊU CẦU KỸ THUẬT

Gói thầu:	Gói thầu số 01: Thuê dịch vụ hạ tầng CNTT phục vụ triển khai hệ thống thu phí hạ tầng tại khu vực cảng biển.
Kế hoạch thuê:	Kế hoạch Thuê dịch vụ phục vụ hệ thống 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 trên địa bàn Thành phố Hồ Chí Minh giai đoạn năm 2025 – 2031.
Chủ trì thuê:	Cảng vụ đường thủy nội địa thành phố Hồ Chí Minh.
Đơn vị tư vấn lập HSMT:	Công ty cổ phần Thiết kế Xây dựng Thương mại Hoàn Quân

Năm 2026

MỤC LỤC

GIẢI THÍCH ĐỊNH NGHĨA VÀ TỪ VIẾT TẮT

STT	Định nghĩa/ Từ viết tắt	Giải thích
1	CNTT	Công nghệ thông tin
2	NSD	Người sử dụng
3	CĐT	Chủ đầu tư (Bên thuê)
4	NT	Nhà thầu (Bên cung cấp dịch vụ)
4	THDL	Tích hợp dữ liệu
5	UBND	Ủy ban nhân dân
6	Cảng vụ	Cảng vụ đường thủy nội địa
7	Hệ thống thu phí	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 cảng biển trên địa bàn thành phố Hồ Chí Minh

PHẦN I: CÁC YÊU CẦU THUÊ DỊCH VỤ

1. Yêu cầu về chất lượng dịch vụ hạ tầng CNTT phục vụ triển khai 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 cảng biển trên địa bàn thành phố Hồ Chí Minh.

1.1. Yêu cầu năng lực 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.

Nhà cung cấp dịch vụ phải có chứng chỉ ISO 9001 về hệ thống quản lý chất lượng còn hiệu lực.

Nhà cung cấp dịch vụ phải có chứng chỉ ISO 27001 về tiêu chuẩn quản lý an toàn thông tin còn hiệu lực.

Nhà cung cấp dịch vụ phải có chứng chỉ ISO 27017 về kiểm soát bảo mật an toàn thông tin cho các dịch vụ đám mây còn hiệu lực.

Nhà cung cấp dịch vụ phải có chứng chỉ ISO 27018 về bảo vệ thông tin định danh cá nhân trong môi trường đám mây công cộng còn hiệu lực.

Nhà cung cấp dịch vụ phải có giấy phép cung cấp dịch vụ viễn thông (ISP).

Hạ tầng nhà cung cấp dịch vụ phải đạt tối thiểu cấp độ 3 về an toàn hệ thống thông tin đối với hệ thống điện toán đám mây và phương án bảo đảm an toàn thông tin phù hợp với theo tiêu chuẩn quốc gia TCVN 11930:2017 hoặc Tiêu chuẩn quốc tế ISO/IEC 27001 hoặc tương đương.

Hạ tầng nhà cung cấp dịch vụ phải đạt tối thiểu cấp độ 3 về an toàn hệ thống thông tin đối với trung tâm dữ liệu và phương án bảo đảm an toàn thông tin phù hợp với theo tiêu chuẩn quốc gia TCVN 11930:2017 hoặc Tiêu chuẩn quốc tế ISO/IEC 27001 hoặc tương đương.

Nhà cung cấp dịch vụ có sẵn trung tâm dữ liệu được thiết kế đáp ứng Hạng 3 theo tiêu chuẩn quốc gia TCVN 9250:2021 (hoặc Rate-3 theo tiêu chuẩn ANSI/TIA-942-B:2017), hoặc Tier 3 theo tiêu chuẩn của Uptime Institute.

Nhà cung cấp dịch vụ phải có chứng nhận kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng theo quy định.

Trong trường hợp liên danh: Nhà cung cấp dịch vụ thực hiện phạm vi công việc nào thì cung cấp tài liệu chứng minh đủ điều kiện thực hiện nội dung liên quan do Nhà thầu đảm nhận.

1.2. Yêu cầu về chất lượng dịch vụ

1.2.1. Năng lực kỹ thuật hệ thống

Thiết bị: Sử dụng hệ thống thiết bị cài đặt các ứng dụng, phần mềm đạt tiêu chuẩn chất lượng tốt, ổn định, được cung cấp chuyên nghiệp. Các thiết bị luôn được dự phòng đôi.

Về quản lý cấu hình:

- Nhân sự quản trị hệ thống của nhà cung cấp dịch vụ sẽ trực tiếp quản lý khai báo cấu hình thiết bị.

- Bên sử dụng dịch vụ sẽ thực hiện giám sát hoạt động từ xa thông qua công cụ quản lý, giám sát hoạt động của toàn quyền đối với hệ thống thuê.

Thiết kế trên cơ sở tổng quát, có tính dự phòng các thiết bị quan trong, dự phòng các thành phần ngay trong các thiết bị hệ thống, đảm bảo độ tin cậy cho hệ thống, thông tin dữ liệu và cho việc mở rộng sau này.

Khả năng mở rộng: Năng lực của hệ thống phải có khả năng đáp ứng các yêu cầu mở rộng khi dữ liệu, số lượng giao dịch, số lượng người dùng tăng lên.

Có khả năng quản trị hệ thống và khắc phục sự cố một cách dễ dàng.

Hệ thống lưu trữ có khả năng quản lý chặt chẽ, thống nhất, bảo đảm cho hoạt động ổn định, giảm thiểu khả năng xảy ra lỗi.

Hệ thống có tính dự phòng cao, hạn chế xảy ra tình trạng "lỗi đơn điểm" (SPOF – Single point Of Failure) cho một số thành phần.

1.2.2. Cơ sở hạ tầng phục vụ

Vị trí địa lý của trung tâm dữ liệu: xa khu dân cư, toàn nhà đặt hệ thống hạ tầng thiết bị biệt lập… đảm bảo an ninh, an toàn phù hợp theo tiêu chuẩn tương đương TCVN 9250 (Tiêu chuẩn Trung tâm dữ liệu - Yêu cầu về hạ tầng kỹ thuật viễn thông) hoặc tương đương.

Hạ tầng mạng viễn thông: triển khai trên hạ tầng mạng tích hợp với các thiết bị được trang bị đôi dự phòng, năng lực xử lý cao, đồng bộ được hỗ trợ chính hãng như Cisco, Netapp, Checkpoint, … ở cấp độ nhà khai thác dịch vụ.

Hạ tầng trung tâm dữ liệu: Sử dụng hạ tầng trung tâm dữ liệu ở cấp độ nhà khai thác dịch vụ được đầu tư đồng bộ, dự phòng cao, cụ thể:

- Nguồn điện lưới trung thế được thiết kế theo mạch vòng trung thế có khả năng vận hành, chuyển tải linh hoạt trong mọi trường hợp, có dự phòng đầy đủ. Từ mạch vòng cấp 2 ngõ vào trung thế khác nhau đến 2 trạm biến áp đặt tại 02 vị trí riêng biệt, độc lập nằm ngoài trung dữ liệu;

- Nguồn điện từ hai trạm biến áp này đi vào hệ thống UPS dự phòng N+1(đặt tại phòng nguồn độc lập), cấp điện cho toàn bộ thiết bị công nghệ thông tin trong Trung tâm dữ liệu với ngõ ra 220V± 1%, phân phối trên 2 thanh nguồn PDU khác nhau cho mỗi tủ rack, thời gian lưu điện dự phòng tối thiểu 30 phút/ 100% tải.

- Đảm bảo nguồn điện liên tục trong trường hợp mất điện trên cả 2 ngõ điện vào, Trung tâm dữ liệu phải trang bị máy phát điện dự phòng 1+1, thời gian mất điện lưới và máy phát hoà tải <= 17 giây;

- Hệ thống điều hoà chính xác dự phòng N+1: đảm bảo nhiệt độ 21oC ± 1oC; độ ẩm RH 55% ± 5%. Hệ thống điều hoà chính xác sử dụng hệ thống động lực học chất lỏng

bên trong, nhằm phân tích và làm mát hiệu quả hơn và sử dụng công nghệ quạt EC (Electronically Commutated) hoặc tương đương nhằm giúp tiết kiệm năng lượng.

- Vị trí lắp tủ rack phù hợp với thiết kế theo tiêu chuẩn tương đương TCVN 9250 hoặc tương đương.

- Hệ thống PCCC sử dụng khí an toàn cho thiết bị và các thiết bị chữa cháy bằng tay dành cho khu vực hành lang bên ngoài Trung tâm dữ liệu.

- Tiếp đất cho hệ thống CNTT < 2Ω, có cắt lọc sét đường nguồn và cắt lọc sét lan truyền.

- Sàn nâng với tải tập trung 4.5 KN/điểm, tải phân bổ đều 12KN/m2, tải va đập 50Kgs, điện trở bề mặt 105 Ω - 108 Ω (chống tĩnh điện), kích thước sàn 600x600mm, chiều cao chân sàn 400mm.

- Hạ tầng được quản lý tập trung qua các công cụ quản lý giám sát chuyên dùng

- Đội ngũ kỹ thuật trực vận hành, giám sát hệ thống 24/7.

- Camera IP giám sát an ninh; kiểm soát ra/vào bằng khoá số, thẻ từ.

- Nhân viên bảo vệ toà nhà Trung tâm dữ liệu trực 24/24.

Hạ tầng cáp quang kết nối đa hướng đến các ISP:

- Trung tâm dữ liệu phải có kết nối cáp quang đa hướng tới hầu hết các nhà cung cấp đường truyền ISP lớn ở Việt Nam như VNPT, FPT, Viettel, CMC,Mobifone Global, … thông qua PoP đặt tại phòng cáp của trung tâm dữ liệu. Hướng cáp quang đi từ các nhà cung cấp đường truyền đến Trung tâm dữ liệu của TP theo ít nhất 2 hướng cáp khác nhau, đấu nối theo kiểu vòng ring hoặc dự phòng 1+1 nhằm đảm bảo chất lượng dịch vụ đường truyền tốt nhất.

- Việc cung cấp đường truyền kết nối theo yêu cầu phải được thực hiện nhanh chóng. Trung tâm dữ liệu phải có PoP kết nối của các nhà cung cấp dịch vụ đường truyền ISP tạo thuận lợi cho việc cấu hình khai báo mở kênh sử dụng dịch vụ.

- Dịch vụ kết nối Internet của Trung tâm dữ liệu phải có cổng kết nối với nhiều nhà cung cấp dịch vụ Internet lớn ở Việt Nam, được thực hiện phân tải đều trên các hướng kết nối để trách nghẽn và được định tuyến tự động chuyển hướng khi có sự cố đường truyền xảy ra.

- Hệ thống Internet Gateway: Hệ thống Internet Gateway của Trung tâm dữ liệu phải gồm ít nhất 2 Router Gateway kết nối Internet quốc tế và 2 Router Gateway kết nối Internet trong nước được cấu hình dự phòng chia tải với nhiều kết nối đến các ISP khác nhau qua các kênh truyền dẫn cáp quang theo mạch vòng Ring hoặc dự phòng 1+1.

Hệ thống chuyển mạch lõi trung tâm (Core Switch)

- Hệ thống chuyển mạch lõi trung tâm phải được triển khai cài đặt, cấu hình dựa trên nền tảng công nghệ mạng được định nghĩa bằng phần mềm, hỗ trợ linh hoạt tích hợp ứng dụng và tự động hóa chuyển mạch, linh hoạt di chuyển ứng dụng trong môi trường điện toán đám mây mà vẫn duy trì được an ninh bảo mật và độ sẵn sàng cao.

- Hệ thống chuyển mạch lõi trung tâm được cấu hình dự phòng, có khả năng chia tải cung cấp kết nối các khu vực dịch vụ (truy cập Internet pubic, private, DMZ…) và cung cấp kết nối, liên thông với các hệ thống khác như Tường lửa Internet, Tường lửa ứng dụng Web, IPS, APT, Cân bằng tải, SIEM, …. Năng lực của Hệ thống chuyển mạch lõi trung tâm phải có khả năng hỗ trợ chuyển mạch cho các kết nối.

Hạ tầng bảo mật, an ninh thông tin của Trung tâm dữ liệu:

Hạ tầng bảo mật, an ninh thông tin được thiết kế và triển khai tích hợp đáp ứng đầy đủ các quy định yêu cầu về Hệ thống thông tin cấp độ 3 theo Nghị định 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ và Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông theo cấp độ theo Quyết định số 401/QĐ-STTTT ngày 12 tháng 12 năm 2022 của Sở Thông tin và truyền thông về việc phê duyệt cấp độ an toàn hệ thống thông tin đối với Hệ thống thu phí sử dụng kết cấu hạ tầng, công trình dịch vụ tiện ích công cộng trong khu vực cửa khẩu cảng biển khu vực Thành phố Hồ Chí Minh.

Các giải pháp thuê dịch vụ an ninh đáp ứng tiêu chí của hệ thống như sau:

STT	Căn cứ	Nội Dung	Tham chiếu dịch vụ tương ứng
1	Đáp ứng phương án đảm bảo an toàn hệ thống thông tin cấp độ 3 quy định tại Khoản 2, Điều 9, Nghị định 85/2016/NĐ-CP. Đáp ứng yêu cầu quy định tại điểm i, khoản b, mục 1, phần II, phụ lục III, Thông tư 12/2022/TT-BTTTT ngày 12/8/2022.	Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương; sử dụng Sản phẩm Mạng riêng ảo	Tính năng ttuy cập kết nối từ xa VPN trong dịch vụ máy chủ ảo.
2	Đáp ứng phương án đảm bảo an toàn hệ thống thông tin cấp độ 3 quy định tại Khoản 2, Điều 9, Nghị định 85/2016/NĐ-CP. Đáp ứng yêu cầu quy định tại điểm ii, khoản b, mục 1, phần II, phụ lục III, Thông tư 12/2022/TT-BTTTT ngày 12/8/2022.	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập sử dụng Sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc Sản phẩm Phòng, chống xâm nhập lớp mạng	Dịch vụ tường lửa đa lớp (Internal Firewall + External Firewall)

3	Đáp ứng phương án đảm bảo an toàn hệ thống thông tin cấp độ 3 quy định tại Khoản 2, Điều 9, Nghị định 85/2016/NĐ-CP. Đáp ứng yêu cầu quy định tại điểm iii, khoản b, mục 1, phần II, phụ lục III, Thông tư 12/2022/TT-BTTTT ngày 12/8/2022.	Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng chính, tối thiểu bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm, tường lửa ứng dụng web, hệ thống lưu trữ tập trung, tường lửa cơ sở dữ liệu (nếu có)	Dịch vụ cân bằng tải
4	Đáp ứng phương án đảm bảo an toàn hệ thống thông tin cấp độ 3 quy định tại Khoản 2, Điều 9, Nghị định 85/2016/NĐ-CP. Đáp ứng yêu cầu quy định tại điểm v, khoản b, mục 1, phần II, phụ lục II, Thông tư 12/2022/TT-BTTTT ngày 12/8/2022.	Có phương án chặn lọc phần mềm độc hại trên môi trường mạng sử dụng Tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc phương án tương đương	Dịch vụ phát hiện và ngăn chặn xâm nhập IPS
5	Đáp ứng phương án đảm bảo an toàn hệ thống thông tin cấp độ 3 quy định tại Khoản 2, Điều 9, Nghị định 85/2016/NĐ-CP. Đáp ứng yêu cầu quy định tại điểm vi, khoản b, mục 1, phần II, phụ lục III, Thông tư 12/2022/TT-BTTTT ngày 12/8/2022.	Có phương án phòng chống tấn công từ chối dịch vụ; sử dụng dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống tấn công từ chối dịch vụ đối với các hệ thống Trung tâm dữ liệu, điện toán đám mây, hệ thống Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số và hệ thống Kết nối tích hợp, chia sẻ dữ liệu	Dịch vụ phòng chống tấn công từ chối dịch vụ (DDoS)
6	Đáp ứng phương án đảm bảo an toàn hệ thống thông tin cấp độ 3 quy định tại Khoản 2, Điều 9, Nghị định 85/2016/NĐ-CP. Đáp ứng yêu cầu quy định tại điểm vii, khoản b, mục 1, phần II, phụ lục III, Thông	Có phương án 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

	tư 12/2022/TT-BTTTT ngày 12/8/2022.		
7	Đáp ứng phương án đảm bảo an toàn hệ thống thông tin cấp độ 3 quy định tại Khoản 2, Điều 9, Nghị định 85/2016/NĐ-CP. Đáp ứng yêu cầu quy định tại điểm x, khoản b, mục 1, phần II, phụ lục III, Thông tư 12/2022/TT-BTTTT ngày 12/8/2022.	Có phương án giám sát hệ thống thông tin tập trung	Yêu cầu dịch vụ giám sát máy chủ trong dịch vụ máy chủ ảo.
8	Đáp ứng phương án đảm bảo an toàn hệ thống thông tin cấp độ 3 quy định tại Khoản 2, Điều 9, Nghị định 85/2016/NĐ-CP. Đáp ứng yêu cầu quy định tại điểm xi, khoản b, mục 1, phần II, phụ lục III, Thông tư 12/2022/TT-BTTTT ngày 12/8/2022.	Có phương án giám sát an toàn hệ thống thông tin tập trung sử dụng Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin hoặc Sản phẩm tương đương	Dịch vụ dịch vụ Phát hiện, cảnh báo sớm các vấn đề nguy cơ liên quan đến an toàn thông tin (SIEM)
9	Đáp ứng phương án đảm bảo an toàn hệ thống thông tin cấp độ 3 quy định tại Khoản 2, Điều 9, Nghị định 85/2016/NĐ-CP. Đáp ứng yêu cầu quy định tại điểm xi, khoản b, mục 1, phần II, phụ lục III, Thông tư 12/2022/TT-BTTTT ngày 12/8/2022.	Có phương án quản lý sao lưu dự phòng tập trung sử dụng hệ thống lưu trữ tập trung và Sản phẩm quản lý lưu trữ tập trung	Dịch vụ sao lưu và phục hồi dữ liệu
10	Đáp ứng phương án đảm bảo an toàn hệ thống thông tin cấp độ 3 quy định tại Khoản 2, Điều 9, Nghị định 85/2016/NĐ-CP. Đáp ứng yêu cầu quy định tại điểm xiii, khoản b, mục 1, phần II, phụ lục III,	Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng, sử dụng Sản phẩm Phòng, chống mã độc và/hoặc Sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu	Dịch vụ phòng chống mã độc trên máy chủ

	Thông tư 12/2022/TT-BTTTT ngày 12/8/2022.	cuối, có chức năng quản lý tập trung	

1.3. Yêu cầu về kỹ thuật, công nghệ để đáp ứng yêu cầu chất lượng dịch vụ

Đảm bảo đáp ứng tiêu chí về Chất lượng dịch vụ đáp ứng theo Phụ Lục I, Thông tư 16/2024/TT-BTTTT ngày 30 ngày 12 năm 2024 của Bộ Thông tin và Truyền thông quy định 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.

Các dịch vụ, giải pháp phải tuân thủ các quy định hoạt động giám sát an toàn hệ thống thông tin tại Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Thông tin và Truyền thông.

Thông tư số 39/2017/TT-BTTTT ngày 15 tháng 12 năm 2017 của Bộ Thông tin và Truyền thông về Ban hành danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước.

Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước:

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1	Tiêu chuẩn về kết nối			
1.1	Truyền siêu văn bản	HTTP v1.1	Hypertext Transfer Protocol version 1.1	Bắt buộc áp dụng
		HTTP v2.0	Hypertext Transfer Protocol version 2.0	Khuyến nghị áp dụng
1.2	Truyền tệp tin	FTP	File Transfer Protocol	Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn
		HTTP v1.1	Hypertext Transfer Protocol version 1.1	
		HTTP v2.0	Hypertext Transfer Protocol version 2.0	Khuyến nghị áp dụng
		WebDAV	Web-based Distributed Authoring and Versioning	Khuyến nghị áp dụng
1.3	Truyền, phát luồng âm thanh/ hình ảnh	RTSP	Real-time Streaming Protocol	Khuyến nghị áp dụng
		RTP	Real-time Transport Protocol	Khuyến nghị áp dụng
		RTCP	Real-time Control Protocol	Khuyến nghị áp dụng
1.4	Truy cập và chia sẻ dữ liệu	OData v4	Open Data Protocol version 4.0	Khuyến nghị áp dụng

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1.5	Truyền thư điện tử	SMTP/ MIME	Simple Mail Transfer Protocol/Multipurpose Internet Mail Extensions	Bắt buộc áp dụng
1.6	Cung cấp dịch vụ truy cập hộp thư điện tử	POP3	Post Office Protocol version 3	Bắt buộc áp dụng cả hai tiêu chuẩn đối với máy chủ
		IMAP 4rev1	Internet Message Access Protocol version 4 revision 1	
1.7	Truy cập thư mục	LDAP v3	Lightweight Directory Access Protocol version 3	Bắt buộc áp dụng
1.8	Dịch vụ tên miền	DNS	Domain Name System	Bắt buộc áp dụng
1.9	Giao vận mạng có kết nối	TCP	Transmission Control Protocol	Bắt buộc áp dụng
1.10	Giao vận mạng không kết nối	UDP	User Datagram Protocol	Bắt buộc áp dụng
1.11	Liên mạng LAN/WAN	IPv4	Internet Protocol version 4	Bắt buộc áp dụng
		IPv6	Internet Protocol version 6	Bắt buộc áp dụng đối với các thiết bị có kết nối Internet
1.12	Mạng cục bộ không dây	IEEE 802.11g	Institute of Electrical and Electronics Engineers Standard (IEEE) 802.11g	Bắt buộc áp dụng
		IEEE 802.11n	Institute of Electrical and Electronics Engineers Standard (IEEE) 802.11n	Khuyến nghị áp dụng
1.13	Truy cập Internet với thiết bị không dây	WAP v2.0	Wireless Application Protocol version 2.0	Bắt buộc áp dụng
1.14	Dịch vụ Web dạng SOAP	SOAP v1.2	Simple Object Access Protocol version 1.2	Bắt buộc áp dụng một, hai hoặc cả ba tiêu chuẩn
		WSDL V2.0	Web Services Description Language version 2.0	

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		UDDI v3	Universal Description, Discovery and Integration version 3	
1.15	Dịch vụ Web dạng RESTful	RESTful web service	Representational state transfer	Khuyến nghị áp dụng
1.16	Dịch vụ đặc tả Web	WS BPEL v2.0	Web Services Business Process Execution Language Version 2.0	Khuyến nghị áp dụng
		WS-I Simple SOAP Binding Profile Version 1.0	Simple SOAP Binding Profile Version 1.0	Khuyến nghị áp dụng
		WS-Federation v1.2	Web Services Federation Language Version 1.2	Khuyến nghị áp dụng
		WS-Addressing v1.0	Web Services Addressing 1.0	Khuyến nghị áp dụng
		WS-Coordination Version 1.2	Web Services Coordination Version 1.2	Khuyến nghị áp dụng
		WS-Policy v1.2	Web Services Coordination Version 1.2	Khuyến nghị áp dụng
		OASIS Web Services Business Activity Version 1.2	Web Services Business Activity Version 1.2	Khuyến nghị áp dụng
		WS-Discovery Version 1.1	Web Services Dynamic Discovery Version 1.1	Khuyến nghị áp dụng
		WS-MetadataExchange	Web Services Metadata Exchange	Khuyến nghị áp dụng
1.17	Dịch vụ đồng bộ thời gian	NTPv3	Network Time Protocol version 3	Bắt buộc áp dụng một trong hai tiêu chuẩn
		NTPv4	Network Time Protocol version 4	
2	Tiêu chuẩn về tích hợp dữ liệu			

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
2.1	Ngôn ngữ định dạng văn bản	XML v1.0 (5th Edition)	Extensible Markup Language version 1.0 (5th Edition)	Bắt buộc áp dụng một trong hai tiêu chuẩn
		XML v1.1 (2nd Edition)	Extensible Markup Language version 1.1	
2.2	Ngôn ngữ định dạng văn bản cho giao dịch điện tử	ISO/TS 15000:2014	Electronic Business Extensible Markup Language (ebXML)	Bắt buộc áp dụng
2.3	Định nghĩa các lược đồ trong tài liệu XML	XML Schema V1.1	XML Schema version 1.1	Bắt buộc áp dụng
2.4	Biến đổi dữ liệu	XSL	Extensible Stylesheet Language	Bắt buộc áp dụng phiên bản mới nhất.
2.5	Mô hình hóa đối tượng	UML v2.5	Unified Modelling Language version 2.5	Khuyến nghị áp dụng
2.6	Mô tả tài nguyên dữ liệu	RDF	Resource Description Framework	Khuyến nghị áp dụng
		OWL	Web Ontology Language	Khuyến nghị áp dụng
2.7	Trình diễn bộ kí tự	UTF-8	8-bit Universal Character Set (UES)/Unicode Transformation Format	Bắt buộc áp dụng
2.8	Khuôn thức trao đổi thông tin địa lý	GML v3.3	Geography Markup Language version 3.3	Bắt buộc áp dụng
2.9	Truy cập và cập nhật các thông tin địa lý	WMS v1.3.0	OpenGIS Web Map Service version 1.3.0	Bắt buộc áp dụng
		WFS v1.1.0	Web Feature Service version 1.1.0	Bắt buộc áp dụng
2.10	Trao đổi dữ liệu đặc tả tài liệu XML	XMI v2.4.2	XML Metadata Interchange version 2.4.2	Khuyến nghị áp dụng
2.11	Sổ đăng ký siêu dữ liệu (MDR)	ISO/IEC 11179:2015	Sổ đăng ký siêu dữ liệu (Metadata registries - MDR)	Khuyến nghị áp dụng
2.12	Bộ phần tử siêu dữ liệu Dublin Core	ISO 15836-1:2017	Bộ phần tử siêu dữ liệu Dublin Core	*Khuyến nghị áp dụng(*)*

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
2.13	Định dạng trao đổi dữ liệu mô tả đối tượng dạng kịch bản JavaScript	JSON RFC 7159	JavaScript Object Notation	Khuyến nghị áp dụng
2.14	Ngôn ngữ mô hình quy trình nghiệp vụ	BPMN 2.0	Business Process Model and Notation version 2.0	Khuyến nghị áp dụng
3	Tiêu chuẩn về truy cập thông tin			
3.1	Chuẩn nội dung Web	HTML v4.01	Hypertext Markup Language version 4.01	Bắt buộc, áp dụng
		WCAG 2.0	W3C Web Content Accessibility Guidelines (WCAG) 2.0	Khuyến nghị áp dụng
		HTML 5	Hypertext Markup Language version 5	Khuyến nghị áp dụng
3.2	Chuẩn nội dung Web mở rộng	XHTML v1.1	Extensible Hypertext Markup Language version 1.1	Bắt buộc áp dụng
3.3	Giao diện người dùng	CSS2	Cascading Style Sheets Language Level 2	Bắt buộc áp dụng một trong ba tiêu chuẩn
		CSS3	Cascading Style Sheets Language Level 3	
		XSL	Extensible Stylesheet Language version	
3.4	Văn bản	(.txt)	Định dạng Plain Text (.txt): Dành cho các tài liệu cơ bản không có cấu trúc	Bắt buộc áp dụng
		(.rtf) v1.8, v1.9.1	Định dạng Rich Text (.rtf) phiên bản 1.8, 1.9.1: Dành cho các tài liệu có thể trao đổi giữa các nền khác nhau	Bắt buộc áp dụng
		(.docx)	Định dạng văn bản Word mở rộng của Microsoft (.docx)	Khuyến nghị áp dụng
		(.pdf) v1.4, v1.5, v1.6, v1.7	Định dạng Portable Document (.pdf) phiên bản 1.4, 1.5, 1.6, 1.7:	Bắt buộc áp dụng một, hai hoặc cả ba tiêu chuẩn

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
			Dành cho các tài liệu chỉ đọc	
		(.doc)	Định dạng văn bản Word của Microsoft (.doc)	
		(.odt) v1.2	Định dạng Open Document Text (.odt) phiên bản 1.2	
3.5	Bảng tính	(.csv)	Định dạng Comma eparated Variable/Delimited (.csv): Dành cho các bảng tính cần trao đổi giữa các ứng dụng khác nhau.	Bắt buộc áp dụng
		(.xlsx)	Định dạng bảng tính Excel mở rộng của Microsoft (.xlsx)	Khuyến nghị áp dụng
		(.xls)	Định dạng bảng tính Excel của Microsoft (.xls)	Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn
		(.ods) v1.2	Định dạng Open Document Spreadsheets (.ods) phiên bản 1.2	
3.6	Trình diễn	(.htm)	Định dạng Hypertext Document (.htm): cho các trình bày được trao đổi thông qua các loại trình duyệt khác nhau	Bắt buộc áp dụng
		(.pptx)	Định dạng PowerPoint mở rộng của Microsoft (.pptx)	Khuyến nghị áp dụng
		(.pdf)	Định dạng Portable Document (.pdf): cho các trình bày lưu dưới dạng chỉ đọc	Bắt buộc áp dụng một, hai hoặc cả ba tiêu chuẩn
		(.ppt)	Định dạng PowerPoint (.ppt) của Microsoft	
		(.odp) v1.2	Định dạng Open Document Presentation (.odp) phiên bản 1.2	
3.7	Ảnh đồ họa	JPEG	Joint Photographic Expert Group (.jpg)	

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		GIF v89a	Graphic Interchange (.gif) version 89a	Bắt buộc áp dụng một, hai, ba hoặc cả bốn tiêu chuẩn
		TIFF	Tag Image File (.tif)	
		PNG	Portable Network Graphics (.png)	
3.8	Ảnh gắn với tọa độ địa lý	GEO TIFF	Tagged Image File Format for GIS applications	Bắt buộc áp dụng
3.9	Phim ảnh, âm thanh	MPEG-1	Moving Picture Experts Group-1	Khuyến nghị áp dụng
		MPEG-2	Moving Picture Experts Group-2	Khuyến nghị áp dụng
		MPEG-4	Moving Picture Experts Group-4	Khuyến nghị áp dụng
		MP3	MPEG-1 Audio Layer 3	Khuyến nghị áp dụng
		AAC	Advanced Audio Coding	Khuyến nghị áp dụng
3.10	Luồng phim ảnh, âm thanh	(.asf), (.wma), (.wmv)	Các định dạng của Microsoft Windows Media Player (.asf), (.wma), (.wmv)	Khuyến nghị áp dụng
		(.ra), (.rm), (.ram), (.rmm)	Các định dạng Real Audio/Real Video (.ra), (.rm), (.ram), (.rmm)	Khuyến nghị áp dụng
		(.avi), (.mov), (.qt)	Các định dạng Apple Quicktime (.avi), (.mov), (.qt)	Khuyến nghị áp dụng
3.11	Hoạt họa	GIF v89a	Graphic Interchange (.gif) version 89a	Khuyến nghị áp dụng
		(.swf)	Định dạng Macromedia Flash (.swf)	Khuyến nghị áp dụng
		(.swf)	Định dạng Macromedia Shockwave (.swf)	Khuyến nghị áp dụng
		(.avi), (.qt), (.mov)	Các định dạng Apple Quicktime (.avi),(.qt),(.mov)	Khuyến nghị áp dụng
3.12	Chuẩn nội dung cho thiết bị di động	WML v2.0	Wireless Markup Language version 2.0	Bắt buộc áp dụng

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
3.13	Bộ ký tự và mã hóa	ASCII	American Standard Code for Information Interchange	Bắt buộc áp dụng
3.14	Bộ ký tự và mã hóa cho tiếng Việt	TCVN 6909:2001	TCVN 6909:2001 "Công nghệ thông tin - Bộ mã ký tự tiếng Việt 16-bit"	Bắt buộc áp dụng
3.15	Nén dữ liệu	Zip	Zip (.zip)	Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn
		.gz v4.3	GNU Zip (.gz) version 4.3	
3.16	Ngôn ngữ kịch bản phía trình khách	ECMA 262	ECMAScript version 6 (6th Edition)	Bắt buộc áp dụng
3.17	Chia sẻ nội dung Web	RSS v1.0	RDF Site Summary version 1.0	Bắt buộc áp dụng một trong hai tiêu chuẩn
		RSS v2.0	Really Simple Syndication version 2.0	
		ATOM v1.0	ATOM version 1.0	Khuyến nghị áp dụng
3.18	Chuẩn kết nối ứng dụng cổng thông tin điện tử	JSR 168	Java Specification Requests 168 (Portlet Specification)	Bắt buộc áp dụng
		JSR286	Java Specification Requests 286 (Portlet Specification)	Khuyến nghị áp dụng
		WSRP v1.0	Web Services for Remote Portlets version 1.0	Bắt buộc áp dụng
		WSRP v2.0	Web Services for Remote Portlets version 2.0	Khuyến nghị áp dụng
4	Tiêu chuẩn về an toàn thông tin			
4.1	An toàn thư điện tử	S/MIME v3.2	Secure Multi-purpose Internet Mail Extensions version 3.2	Bắt buộc áp dụng
		OpenPGP	OpenPGP	Khuyến nghị áp dụng
4.2	An toàn tầng giao vận	SSH v2.0	Secure Shell version 2.0	Bắt buộc áp dụng
		TLS v1.2	Transport Layer Security version 1.2	Bắt buộc áp dụng
4.3	An toàn truyền tệp tin	HTTPS	Hypertext Transfer Protocol Secure	Bắt buộc áp dụng

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		FTPS	File Transfer Protocol Secure	Khuyến nghị áp dụng
		SFTP	SSH File Transfer Protocol	Khuyến nghị áp dụng
4.4	An toàn truyền thư điện tử	SMTPS	Simple Mail Transfer Protocol Secure	Bắt buộc áp dụng
4.5	An toàn dịch vụ truy cập hộp thư	POP3S	Post Office Protocol version 3 Secure	Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn
		IMAPS	Internet Message Access Protocol Secure	
4.6	An toàn dịch vụ DNS	DNSSEC	Domain Name System Security Extenssions	Khuyến nghị áp dụng
4.7	An toàn tầng mạng	IPsec - IP ESP	Internet Protocol security với IP ESP	Bắt buộc áp dụng
4.8	An toàn thông tin cho mạng không dây	WPA2	Wi-fi Protected Access 2	Bắt buộc áp dụng
4.9	Giải thuật mã hóa	TCVN 7816:2007	Công nghệ thông tin. Kỹ thuật mật mã thuật toán mã dữ liệu AES	Khuyến nghị áp dụng
		3DES	Triple Data Encryption Standard	Khuyến nghị áp dụng
		PKCS #1 V2.2	RSA Cryptography Standard - version 2.2	Khuyến nghị áp dụng, sử dụng lược đồ RSAES-OAEP để mã hóa
		ECC	Elliptic Curve Cryptography	Khuyến nghị áp dụng
4.10	Giải thuật chữ ký số	PKCS #1 V2.2	RSA Cryptography Standard - version 2.2	Bắt buộc áp dụng, sử dụng lược đồ RSASSA-PSS để ký
		ECDSA	Elliptic Curve Digital Signature Algorithm	Khuyến nghị áp dụng
4.11	Giải thuật băm cho chữ ký số	SHA-2	Secure Hash Algorithms-2	Khuyến nghị áp dụng
4.12	Giải thuật truyền khóa	RSA-KEM	Rivest-Shamir-Adleman - KEM (Key	Bắt buộc áp dụng

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
			Encapsulation Mechanism) Key Transport Algorithm	
		ECDHE	Elliptic Curve Diffie Hellman Ephemeral	Khuyến nghị áp dụng
4.13	Giải pháp xác thực người sử dụng	SAML v2.0	Security Assertion Markup Language version 2.0	Khuyến nghị áp dụng
4.14	An toàn trao đổi bản tin XML	XML Encryption Syntax and Processing	XML Encryption Syntax and Processing	Bắt buộc áp dụng
		XML Signature Syntax and Processing	XML Signature Syntax and Processing	Bắt buộc áp dụng
4.15	Quản lý khóa công khai bản tin XML	XKMS v2.0	XML Key Management Specification version 2.0	Khuyến nghị áp dụng
4.16	Giao thức an toàn thông tin cá nhân	P3P v1.1	Platform for Privacy Preferences Project version 1.1	Khuyến nghị áp dụng
4.17	Hạ tầng khóa công khai			Khuyến nghị áp dụng
	Cú pháp thông điệp mật mã cho ký, mã hóa	PKCS#7 v1.5 (RFC 2315)	Cryptographic message syntax for file-based signing and encrypting version 1.5	
	Cú pháp thông tin thẻ mật mã	PKCS#15 v1.1	Cryptographic token information syntax version 1.1	
	Cú pháp thông tin khóa riêng	PKCS#8 V1.2 (RFC 5958)	Private-Key Information Syntax Standard version 1.2	
	Giao diện thẻ mật mã	PKCS#11 v2.20	Cryptographic token interface standard version 2.20	
	Cú pháp trao đổi thông tin cá nhân	PKCS#12 v1.1	Personal Information Exchange Syntax version 1.1	
	Khuôn dạng danh sách	RFC 5280	Certificate Revocation List Profile	

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
	chứng thư số thu hồi			
	Khuôn dạng chứng thư số	RFC 5280	Public Key Infrastructure Certificate	
	Cú pháp yêu cầu chứng thực	PKCS#10 v1.7 (RFC 2986)	Certification Request Syntax Specification version 1.7	
	Giao thức trạng thái chứng thư trực tuyến	RFC 6960	On-line Certificate status protocol	
	Giao thức gắn tem thời gian	RFC 3161	Time stamping protocol	
	Dịch vụ tem thời gian	ISO/EEC 18014-1:2008	Information technology Security techniques - Time stamping services	
		ISO/EEC 18014-2:2009	Part 1: Framework	
		ISO/EEC 18014-3:2009	Part 2: Mechanisms producing independent tokens	
		ISO/EEC 18014-4:2015	Part 3: Mechanisms producing linked tokens	
			Part 4: Traceability of time sources	
4.18	An toàn cho dịch vụ Web	WS-Security v1.1.1	Web Services Security: SOAP Message Security Version 1.1.1	Khuyến nghị áp dụng
4.19	Khuôn dạng dữ liệu trao đổi sự cố an toàn mạng	RFC 7970	The Incident Object Description Exchange Format version 2 (IODEF)	Khuyến nghị áp dụng

1.4. Cam kết dịch vụ máy chủ ảo nền tảng điện toán đám mây dùng riêng

1.4.1. Trách nhiệm nhà cung cấp dịch vụ trong đảm bảo vận hành

Phải cam kết và đảm bảo cấp phát đầy đủ vùng tài nguyên dành riêng (resource pool) cho hệ thống đám mây dùng riêng (private cloud) theo khối lượng mà bên sử dụng dịch vụ yêu cầu và phải đảm bảo dự phòng tối thiểu 20% tài nguyên để hệ thống vận hành ổn định.

Thông báo về các bản cập nhật, vá lỗi có thể ảnh hưởng tới dịch vụ cung cấp.

Đảm bảo an toàn thông tin, thường xuyên cập nhật các phiên bản phần mềm giải pháp mới nhất đối với dịch vụ cung cấp.

Giám sát tài nguyên sử dụng và cảnh báo qua email/SMS/Phone Call khi:

CPU/RAM/ Lưu trữ (GB) sử dụng vượt quá 70%.

Server không thể truy cập được.

Dịch vụ cài đặt ứng dụng không thể kết nối được.

Theo dõi ngưỡng sử dụng tài nguyên CPU/RAM/ Lưu trữ (GB)và báo cáo khách hàng xem xét nâng cấp khi tài nguyên CPU/RAM/ Lưu trữ (GB) sử dụng thường xuyên trên 70%.

Đảm bảo quá trình sao lưu backup dữ liệu, kiểm tra và đảm bảo dữ liệu backup có thể khôi phục được toàn vẹn.

Hỗ trợ kỹ thuật:

Thay đổi cấu hình bảo mật OS theo yêu cầu

Cập nhật bản vá và nâng cấp OS theo yêu cầu

Hỗ trợ cài đặt Database, Web Server theo yêu cầu

Hỗ trợ kiểm tra phát hiện lỗi Database, Web Server theo yêu cầu.

Restart dịch vụ Database, Web Server theo yêu cầu

Thiết lập cơ chế sao lưu backup dữ liệu định kỳ.

Khôi phục từ bản backup theo yêu cầu.

Cài đặt các dịch vụ và phần mềm theo yêu cầu, đảm bảo các phần mềm có license (hệ điều hành), tương thích với hệ điều hành server và được hỗ trợ đầy đủ.

Cập nhật và cài đặt bản vá các dịch vụ và phần mềm theo yêu cầu khi đảm bảo phần mềm được hỗ trợ đầy đủ và tương thích.

Cài đặt bảo mật server, chỉnh sửa rule firewall của server theo yêu cầu.

Hỗ trợ cài đặt tối ưu chống tấn công botnet quy mô vừa và nhỏ, với các cuộc tấn công quy mô lớn hoặc cách tấn công tinh vi hơn nhà cung cấp dịch vụ sẽ tư vấn phương án cho khách hàng.

Tư vấn cấu hình cần nâng cấp khi cấu hình không đáp ứng được tải.

1.4.2. Tiêu chuẩn hạ tầng kỹ thuật đặt hệ thống cung cấp dịch vụ điện toán đám mây dùng riêng (Private cloud)

Các máy chủ vật lý và hệ thống lưu trữ phục vụ cung cấp dịch vụ điện toán đám mây dùng riêng (Private cloud) được đặt trong TTDL (Datacenter) phải đạt cấp độ 3 về an toàn hệ thống thông tin đối với Trung tâm dữ liệu theo tiêu chuẩn quốc gia TCVN 11930:2017 và được thiết kế theo tiêu chuẩn phù hợp với mức đảm bảo kỹ thuật: Hạng 3 theo tiêu chuẩn quốc gia TCVN 9250:2021 (hoặc Rate-3 theo tiêu chuẩn ANSI/TIA-942-B:2017), hoặc Tier 3 theo tiêu chuẩn của Uptime Institute, cụ thể:

TT	Thông số kỹ thuật	Yêu cầu
1	Hạ tầng đảm bảo hoạt động 99,98%	Có
1	Nguồn điện lưới có 2 ngõ vào khác nhau đấu nối với 2 trạm biến áp khác nhau, công suất được thiết kế phù hợp và đảm bảo hoạt động của Trung tâm dữ liệu.	Có
2	2 Hệ thống UPS N+1 hoạt động độc lập, phân phối trên 2 thanh nguồn PDU khác nhau trong cùng tủ rack	Có
3	Máy phát điện (dự phòng N+1)	Có
4	Cấp nguồn điện lưới cho trung tâm dữ liệu từ 2 trạm biến áp tại hai vị trí khác nhau	Có
5	Điều hoà nhiệt độ sử dụng công nghệ máy lạnh chính xác (nhiệt độ :21oC ± 1oC; độ ẩm: RH 55% ± 5%, tốc độ gió: 20.000m3/h)	Có
6	Hệ thống camera, khoá số, thẻ từ kiểm soát ra/vào khu vực TTDL	Có
7	Hệ thống chữa cháy tự động bằng khí	Có
8	Hệ thống cắt lóc sét nguồn đầu vào, sét lan truyền	Có
9	Hệ thống tiếp đất đảm bảo điện trở <2Ω	Có

1.4.3. Tiêu chuẩn về dịch vụ máy chủ ảo dùng riêng (dịch vụ Private cloud)

STT	Các thông số SLA	Chỉ tiêu
1	Độ khả dụng dich vụ hạ tầng điện toán đám mây trung bình trên tháng	99,9%
2	Cảnh báo (email, SMS) khi tài nguyên hệ thống (CPU, RAM, Lưu trữ) vượt 70% so với cấu hình đã cấp phát	Gửi ngay
3	Cam kết thời gian đáp ứng và giải quyết sự cố của chủ trì thuê dịch vụ trong vòng 30 phút kể từ khi phát sinh yêu cầu	100%
4	Resource pool cho hệ thống private cloud cung cấp máy chủ ảo (VM) không giới hạn VCPU, RAM và Storage	100%
5	Toàn bộ máy chủ vật lý của hệ thống điện toán đám mây dùng riêng đều được trang bị 2 card mạng port 10Gbps	Có

STT	Các thông số SLA	Chỉ tiêu
	hoạt động dự phòng, được kết nối vào hệ thống mạng có giao tiếp 10Gbps	
6	Công nghệ RAM cho máy chủ ảo (VM) sử dụng RAM thật (KHÔNG lấy HDD làm RAM) và set đúng dung lượng thực vào thẳng VPS, KHÔNG SHARE với VM khác để đạt tốc độ cao nhất	Có
7	Hạ tầng điện toán đám mây dùng riêng đảm bảo hệ thống server vật lý được tổ chức dự phòng, phân tải, kết nối theo mô hình cluster, có tính năng cao cấp vMotion, HA, FaulTolerance,…. cho phép các máy chủ ảo hoạt động không gián đoạn khi có lỗi máy chủ vật lý/node mạng.	Có
8	Hệ thống lưu trữ đảm bảo tính dự phòng cho hệ thống điều khiển tủ đĩa, SAN Swich, card giao tiếp lưu trữ/server	Hệ thống điều khiển tủ đĩa hoạt động ở chế độ cluster 4 node 2 x SAN switch 2 x card HBA/server
9	Hệ thống lưu trữ có công nghệ Storage Virtual Machine cho phép phân tách các phân vùng lưu trữ riêng biệt cho mỗi chủ trì thuê dịch vụ đảm bảo an toàn thông tin cao	Có
10	Hệ thống lưu trữ có khả năng mở rộng dung lượng lên đến hàng PetaByte. Hỗ trợ dữ liệu di chuyển linh hoạt qua lại giữa các nodes lưu trữ không làm gián đoạn truy nhập dữ liệu.	Có
11	Hệ thống lưu trữ tích hợp công nghệ sao lưu dữ liệu (nhân bảo và sao lưu) cho phép sao lưu và phục hồi dữ liệu một cách nhanh chóng từ Disk sang Disk.	Có
12	Dung lượng lưu trữ trên SAN cấp thực theo nhu cầu sử dụng	100%
13	Hệ thống lưu trữ có công nghệ cho phép giám sát và tạo chính sách đặc quyền truy cập, thao tác ở mức file nhằm ngăn chặn việc mã hoá ransomware dữ liệu, đồng thời cho phép người quản trị quản lý các định dạng file (file	Có

STT	Các thông số SLA	Chỉ tiêu
	extension) được phép lưu trữ trên hệ thống. Hệ thống thực hiện chặn file dựa trên chữ ký số mã thuật của file.	
14	Hệ thống lưu trữ có tính năng phân tích cung cấp khả năng hiển thị trên cơ sở hạ tầng của nhà cung cấp dịch vụ. Khắc phục sự cố, giám sát và tối ưu hóa các tài nguyên được sử dụng trong cơ sở hạ tầng điện toán đám mây. Nền tảng phân tích sử dụng công nghệ UEBA (User Entity Behavior Analytics), Machine Learning, AI và Storage Workload Security để : + Thực hiện các hành động tự động như Sao chép Snapshot khi hệ thống bị Ransomware, chặn người dùng khi có hoạt động bất thường + Phân tích hành vi người dùng + Phát hiện thay đổi bất thường trong hoạt động của người dùng. + Phân tích các mẫu hành vi bất thường để xác định loại mối đe dọa, phát hiện ransomware. + Cung cấp thông tin chi tiết về các cuộc tấn công tiềm ẩn.	Có
15	Hệ thống lưu trữ có tính năng bảo vệ chống Ransomware tự động (ARP hoặc tương đương) thực hiện cải thiện khả năng phục hồi mạng bằng cách áp dụng mô hình học máy để phân tích chống phần mềm tống tiền, phát hiện các dạng phần mềm tống tiền liên tục phát triển với độ chính xác 99%. Mô hình học máy của ARP được đào tạo trước trên một tập dữ liệu lớn các tệp trước và sau một cuộc tấn công phần mềm tống tiền mô phỏng. Việc đào tạo tốn nhiều tài nguyên này được thực hiện bên ngoài hệ thống, nhưng việc học từ quá trình đào tạo được sử dụng cho mô hình bên trong hệ thống.	Có
16	Hệ thống lưu trữ có tính năng "ghi một lần, đọc nhiều lần" (Write Once Read Many - WORM) thay thế cho kiểu lưu trữ dữ liệu truyền thống. Tính năng này được sử dụng để lưu trữ dữ liệu WORM chỉ đọc mà không được ghì đè, chỉnh sửa hoặc xoá. Mục tiêu chính của tính năng này là cung cấp chức năng lưu giữ và WORM được thực thi bằng lưu trữ bằng cách sử dụng các giao thức tệp mở như CIFS và NFS (không sử dụng được với FC). Tính năng này có	Có

STT	Các thông số SLA	Chỉ tiêu
	thể được triển khai để bảo vệ dữ liệu trong môi trường quản lý nghiêm ngặt theo cách mà ngay cả quản trị viên lưu trữ cũng được coi là bên không đáng tin cậy.	
17	Hệ thống lưu trữ có tính năng Snapshot bất biến tạo bản sao dữ liệu không thể thay đổi, không thể xóa tại một thời điểm nhất định, được lưu trữ theo nguyên tắc WORM (Write Once, Read Many)	Có
18	Hệ thống lưu trữ có tính năng Multi Admin Verification (MAV) là tính năng quản lý, phê duyệt các lệnh được thực thi trên hệ thống SAN bằng việc các lệnh thực thi đều phải có sự đồng ý của các quản trị viên. Tính năng này nhằm mục đích kiểm soát các hoạt động xoá dữ liệu backup chỉ được thực thi sau khi có sự đồng ý của các quản trị viên. Việc này đảm bảo an toàn đối với trường hợp như quản trị viên có hành vi, ý định phá hoại hoặc quản trị viên thiếu kinh nghiệm gây ra những thay đổi không mong muốn, mất mát dữ liệu.	Có
19	Hệ thống lưu trữ có tính năng xác thực đa yếu tố (MFA) cho phép quản trị viên tăng cường bảo mật bằng cách yêu cầu người dùng cung cấp hai phương thức xác thực để đăng nhập vào quản trị viên	Có
20	Hệ thống lưu trữ có tính năng đồng bộ dữ liệu Async / Sync - cho phép đồng bộ dữ liệu với các hệ thống lưu trữ cùng loại	Có
21	Hệ thống lưu trữ có tính năng mã hóa dữ liệu: Hardware Encryption At Rest, Software Encryption At Rest, Encrypted Data In Flight	Có
22	IOPS (Input Output per second) theo phương pháp đọc/ghi ngẫu nhiên random operation 4K.	IOPS >= 30.000, trong đó IOPS write >= 7.680
23	Throughput (thông lượng ghi, theo phương pháp ghi tuần tự sequence operation)	>= 300MB/s
24	Latency (độ trễ)	<= 5ms

STT	Các thông số SLA	Chỉ tiêu
25	Công nghệ lưu trữ	RAID 1,5,6,10 cam kết hoạt động 99,9%
26	Toàn quyền quản trị hệ thống Private Cloud	Có
27	Cung cấp cổng dịch vụ tự quản lý và vận hành hạ tầng private cloud của mình gồm: tạo/xoá máy chủ ảo (VM); các lớp mạng khác nhau (tổ chức theo mô hình Front End – Back End); điều chỉnh cấu hình và hoạt động VPS trong private cloud như: Khởi động (Power ON), Tạm dừng (Subspend), Ngừng hoạt động (Power OFF), Thiết lập lại trạng thái hoạt động (Reset), Sao chụp ảnh máy chủ (Snapshot), nâng cấp máy chủ (vCPU, RAM, Lưu trữ (GB) không làm gián đoạn hoạt động	Có
28	Cung cấp công cụ để lựa chọn cấp phát các máy chủ ảo (VM) với hệ điều hành Windows, CentOS, Linux…; các ứng dụng: Microsoft SQL, MySQL, Sharepoint…. từ danh sách phần mềm có sẵn hoặc tự tạo trong Private Cloud theo nhu cầu của mình	Có
29	Số lượng domain được host	không giới hạn
30	Cung cấp hệ điều hành có bản quyền cho VM	100%
31	Cổng trong nước	300 Mbps
32	Cổng quốc tế	10 Mbps
33	IP cho máy chủ ảo	01 địa chỉ IP cho 01 máy chủ ảo
34	Lưu lượng thông tin được gởi nhận	Không giới hạn (Unlimited)
35	Support Help Desk / Phone	24x7x365
36	Khởi động Server miễn phí	24x7x365
37	Nhà cung cấp đảm bảo cung cấp hệ thống dịch vụ Private Cloud vận hành tốt, ổn định (hoạt động 99,9%) độ tin cậy cao (không phát sinh lỗi hệ thống), đảm bảo tính mở rộng không giới hạn với các mô hình triển khai hệ thống phần	Có

STT	Các thông số SLA	Chỉ tiêu
	mềm ứng dụng hỗ trợ trên các hệ điều hành theo khuyến cáo của nhà cung cấp: Mô hình máy chủ đơn (non-clustering). Mô hình clustering: Failover/failback clustering (cả hai mô hình active-active clustering và active-standby clustering), network loadbalancing. Mô hình High-Availability (HA): HA, HA-Load balancing. Các mô hình triển khai khác theo Nguyên tắc RAS (Reliability-Availability-Scalability).	

1.4.4. Yêu cầu tiêu chuẩn chung về dịch vụ hệ thống private cloud

Dịch vụ hệ thống Private cloud phải đảm bảo các yếu tố cơ bản sau:

Nhà cung cấp dịch vụ cung cấp hạ tầng kỹ thuật dành riêng theo mô hình private cloud (IaaS) đặt tại TTDL phải đạt cấp độ 3 về an toàn hệ thống thông tin đối với Trung tâm dữ liệu theo tiêu chuẩn quốc gia TCVN 11930:2017 với công nghệ ảo hóa mạnh mẽ, đảm bảo an toàn bảo mật cao. Đảm bảo các yêu cầu tối thiểu sau:

+ On-demand self-service – tự phục vụ nhu cầu: Có khả năng tự quản lý, giám sát dịch vụ đã thuê mà không phụ thuộc vào đơn vị cung cấp cloud.

+ Broad network access – khả năng truy cập mạng diện rộng khắp: các dịch vụ cloud cần được truy cập thông qua các kết nối Metronet, Internet với chính sách truy cập theo yêu cầu.

+ Resource pooling – vùng tài nguyên: các dịch vụ private cloud sử dụng hạ tầng kỹ thuật độc lập, dành riêng, không chia sẻ tài nguyên.

+ Rapid elasticity or expansion – co giãn nhanh chóng: nhà cung cấp dịch vụ cloud phải đảm bảo cung cấp dịch vụ đáp ứng được nhu cầu scale up và down các hệ thống đang vận hành một cách nhanh chóng và đơn giản.

+ Measured service – đo lường dịch vụ: khả năng của dịch vụ cloud được tối ưu cho lưu lượng sử dụng và được báo cáo thường xuyên, tự động.

Nhà cung cấp cung cấp dịch vụ phải hỗ trợ kỹ thuật 24x7x365.

Về quản trị hệ thống: Bên sử dụng dịch vụphải được cung cấp công cụ quản trị và toàn quyền quản trị hệ thống Privite Cloud đối với dịch vụ mình thuê (có quyền chủ động phân chia, cấu hình và quản lý tài nguyên, cài đặt hệ thống phù họp với nhu cầu sử dụng thông qua công cụ quản lý tập trung).

1.4.5. Đường truyền

STT	Các thông số SLA	Chỉ tiêu
1	Độ khả dụng mạng trung bình trên tháng	99,98%
2	Tỉ lệ rớt gói trung bình trên tháng (<)	1%
3	Độ trễ	
-	Trong nước (<)	30ms
-	Quốc tế (<)	350 ms

1.4.6. Yêu cầu giám sát máy chủ

Giám sát tổng thể toàn bộ các máy chủ và hệ thống trong phạm vi dự án.

Dịch vụ giám sát trên 1 máy chủ ảo.

Báo cáo định kỳ hàng tháng, hàng quý, hàng năm về tình hình sử dụng tài nguyên.

Thiết lập cảnh báo thông qua email cho khách hàng về tình trạng tài nguyên Ram, CPU, HDD khi vượt trên 70%.

Cung cấp nhân lực giám sát giao diện web 24/24.

+ Theo dõi trực tiếp trên giao diện Web.

+ Đánh giá dịch vụ bằng việc sử dụng dịch vụ như người dùng: duyệt web, FTP.

Thiết lập và báo cáo giám sát các ứng dụng

+PING (tất cả các server)

+ Giám sát dịch vụ cổng (port) đối với từng ứng dụng cụ thể.

Cung cấp phần mềm giám sát bản quyền chính hãng và được gia hạn hàng năm.

Cập nhật các bản vá lỗi (nếu có trong quá trình vận hành)

Hỗ trợ xử lý sự cố (nếu có) từ chính hãng trong quá trình vận hành

Hỗ trợ kỹ thuật qua điện thoại hoặc hỗ trợ nhanh tại chỗ 24hx7ngày/ tuần

Thời gian đáp ứng (24hx7ngày/ tuần) ≤ 4 giờ

Giám sát hệ thống theo thời gian thực 24hx7ngày/ tuần

Gửi cảnh báo các vi phạm ở mức độ nghiêm trọng qua email

1.4.7. Yêu cầu truy cập kết nối từ xa VPN

Có giải pháp phục vụ truy cập kết nối từ xa VPN đảm bảo bảo vệ tổng thể cho các hệ thống và máy chủ trong phạm vi dự án.

- Hỗ trợ VPN dạng site-to-site hay truy cập xa, đơn giản và quản lý tập trung.
- Hỗ trợ nhiều kết nối truy cập từ xa.

- Liền mạch và tích hợp.
- Bản quyền dịch vụ hỗ trợ từ hãng
- Cập nhật các bản vá lỗi (nếu có trong quá trình vận hành)
- Tất cả các dịch vụ cung cấp đều có sự hỗ trợ xử lý sự cố (nếu có) từ chính hãng trong quá trình vận hành.

1.4.8. Chế độ bảo hành dịch vụ cung cấp

Trong mọi trường hợp nhà cung cấp dịch vụ phải đảm bảo dịch vụ do mình cung cấp hoạt động liên tục 24/7 (trừ trường hợp bất khả kháng do luật quy định). Nếu để xảy ra gián đoạn dịch vụ thì bên thuê dịch vụ sẽ thực hiện giảm trừ chi phí dịch vụ theo thỏa thuận theo hợp đồng.

1.5. Cam kết hỗ trợ dịch vụ an ninh thông tin

1.5.1. Dịch vụ phát hiện và ngăn chặn xâm nhập IPS

1.5.1.1. Phạm vi bảo vệ và cung ứng của hệ thống

Bảo vệ tổng thể toàn bộ các máy chủ và hệ thống trong phạm vi dự án

1.5.1.2. Yêu cầu chất lượng dịch vụ

- Dịch vụ phát hiện và ngăn chặn xâm nhập phải đảm bảo tính HA (High availability): được triển khai trên hệ thống hoạt động dự phòng và chia tải.

- Dịch vụ phát hiện và phòng chống xâm nhập (IPS): thực hiện chức năng giám sát, chống xâm nhập tại cổng kết nối Internet cho toàn mạng.

- Bảo vệ các ứng dụng ảo hóa ở ngay bên trong hạ tầng mạng ảo.

- Có tính năng virtual patching bảo vệ các lỗ hổng bảo mật trong hệ điều hành và các ứng dụng cho tới khi chúng được vá, giúp chống lại các tấn công đã biết hoặc bảo vệ các lỗ hổng bảo mật trong hệ điều hành và các ứng dụng cho tới khi chúng được vá, giúp chống lại các tấn công đã biết hoặc zero-dayero-day.

- Có tính năng Security Filters bảo vệ mạng khỏi các mối đe dọa bằng cách kiểm tra và lọc lưu lượng mạng dựa trên các quy tắc được định nghĩa trước để phát hiện và ngăn chặn các mối đe dọa.

- Có khả năng phát hiện và giám sát nhiều loại ứng dụng từ đó nhanh chóng nhận diện các rủi ro bảo mật

- Có tính năng này cho phép thực hiện cấu hình một số trường hợp ngoại lệ hoặc hạn chế dựa trên bộ chính sách có sẵn

- Có tính năng cho phép cấu hình chính sách để bảo vệ vùng mạng bị tấn công DDoS bằng cơ chế xác định theo số lượng gói tin TCP SYN và thực hiện ngăn chặn truy cập đến vùng mạng cần được bảo vệ DDoS.

- Có tính năng bảo vệ mạng bằng cách sử dụng các bộ lọc dựa trên danh tiếng và vị trí địa lý để phát hiện và ngăn chặn các đối tượng đáng ngờ dựa trên cơ sở dữ liệu danh tiếng, theo quốc gia hay khu vực cụ thể. Các đối tượng này có thể bao gồm địa chỉ IP, tên miền hoặc URL đã được xác định là có nguy cơ về bảo mật.

- Có khả năng khi tích hợp với thiết bị bảo mật khác, các đối tượng đáng ngờ sẽ được chia sẻ và lưu trữ trong cơ sở dữ liệu, từ đó áp dụng các hành động ngăn chặn lên các đối tượng.

Hỗ trợ khả năng vá ảo: để ngăn chặn tấn công vào các lổ hổng bảo mật zero-day như: thiết lập chính sách bảo mật, cập nhập nhận dạng lỗ hổng, cập nhập IOC (Indicator of Compromise) nhân công.

- Sử dụng các mô hình số liệu được phát triển với những kỹ thuật máy học (machine learning) khả năng phát hiện và ngăn chặn hiểm họa theo thời gian thực.

- Theo dõi các hoạt động bất thường đối với hệ thống.

- Xác định ai đang tác động đến hệ thống và cách thức như thế nào, các hoạt động xâm nhập xảy ra tại vị trí nào trong cấu trúc mạng.

- Tương tác với hệ thống firewall để ngăn chặn kip thời các hoạt động thâm nhập hệ thống.

- Kiểm soát các ứng dụng ra/vào hệ thống gateway.

- Kiểm soát và chống các hình thức xâm nhập hệ thống.

- Hệ thống có tính năng dự phòng, đảm bảo tính sẵn sàng.

1.5.1.3. Cam kết từ nhà cung cấp dịch vụ

- Bản quyền dịch vụ hỗ trợ từ hãng
- Cập nhật các bản vá lỗi (nếu có trong quá trình vận hành)
- Hỗ trợ xử lý sự cố (nếu có) từ chính hãng trong quá trình vận hành

1.5.1.4. Khả năng xử lý ứng cứu nhà cung cấp dịch vụ

- Hỗ trợ kỹ thuật qua điện thoại hoặc hỗ trợ nhanh tại chỗ 24hx7ngày/ tuần

- Thời gian đáp ứng (24hx7ngày/ tuần) ≤ 4 giờ

- Giám sát hệ thống theo thời gian thực 24hx7ngày/ tuần

- Gửi cảnh báo các vi phạm ở mức độ nghiêm trọng qua email

1.5.2. Dịch vụ tường lửa đa lớp (Internal Firewall + External Firewall)

1.5.2.1. Phạm vi bảo vệ và cung ứng của dịch vụ

Bảo vệ tổng thể toàn bộ các máy chủ và hệ thống trong phạm vi dự án

1.5.2.2. Yêu cầu chất lượng dịch vụ

- Dịch vụ tường lửa đảm bảo tính HA (High availability): được triển khai trên hệ thống tường lửa hoạt động dự phòng và chia tải.

- Có tính năng triển khai các chính sách kiểm soát truy cập (access control) và NAT (Network Address Translation) trên Security Gateway để đảm bảo không có lưu lượng mạng nào đi qua mà không bị kiểm soát, đồng thời giúp che giấu địa chỉ IP mạng bên trong.

- Có tính năng thiết lập các kênh kết nối mã hóa, an toàn từ những người làm việc bên ngoài mạng, hay các kết nối an toàn tới mạng chi nhánh, đối tác,… đảm bảo tính xác thực, tính riêng tư và tính toàn vẹn dữ liệu.

- Có tính năng: Cho phép người dùng di động và từ xa kết nối dễ dàng và an toàn với các tài nguyên bên trong mạng qua internet. Các kênh truyền được mã hóa theo chuẩn IPsec và SSL/TLS, bảo vệ mạng và máy tính điểm cuối khỏi các mối đe dọa.

- Có tính năng nhận dạng và quản lý người dùng: Cho phép thực thi các chính sách truy cập và kiểm toán dữ liệu dựa trên danh tính: người dùng, nhóm người dùng, máy tính, nhóm máy tính chính xác. Tính năng có thể áp dụng cho cả mạng dựa trên Active Directory và không dựa trên Active Directory cũng như cho nhân viên và người dùng khách.

- Có tính năng nhận thức về nội dung: Cho phép thực thi Chính sách bảo mật dựa trên nội dung của lưu lượng truy cập bằng cách xác định các tệp và nội dung của nó. Tính năng này hạn chế các loại dữ liệu mà người dùng có thể tải lên hoặc tải xuống. Ví dụ: tính năng có thể được sử dụng để xác định tệp nào được tải lên DropBox.

- Có tính năng kiểm soát ứng dụng: Cho phép các nhóm CNTT dễ dàng tạo các chính sách chi tiết, dựa trên người dùng hoặc nhóm, để xác định, chặn hoặc giới hạn việc sử dụng hàng ngàn ứng dụng.

- Có tính năng ngăn chặn xâm nhập: Bảo vệ chủ động chống lại lưu lượng mạng độc hại và không mong muốn, tập trung vào các lỗ hổng ứng dụng và máy chủ, cũng như các cuộc tấn công tự nhiên bằng bộ công cụ khai thác và kẻ tấn công độc hại. Việc thiết lập ngăn chặn dựa trên bộ signatrure được cập nhật liên tục.

- Có tính năng lọc URL: Kiểm soát quyền truy cập vào hàng triệu trang web theo danh mục, người dùng, nhóm và máy để bảo vệ người dùng khỏi các trang độc hại và cho phép sử dụng Internet an toàn. URL Filtering sử dụng công nghệ UserCheck, đưa ra cảnh báo cho người dùng khi có nguy cơ mất dữ liệu hoặc vi phạm bảo mật.

- Có tính năng chống Bot: Phát hiện ra các máy bị nhiễm Bot bằng cách tương quan nhiều phương pháp khác nhau như xác định các địa chỉ C&C, dựa trên mẫu, dựa trên hành vi. Đồng thời vô hiệu hóa mối đe dọa từ Bot và Botnet bằng cách chặn liên lạc C&C trước khi chúng có thể gây thiệt hại và ảnh hưởng đến người dùng, đảm bảo rằng không có thông tin nhạy cảm nào được gửi đi.

- Có tính năng chống vi-rút: Phát hiện tiền lây nhiễm và ngăn chặn phần mềm độc hại tại gateway, thực hiện quét các tệp đến và đi để phát hiện và ngăn chặn trước khi chúng ảnh hưởng tới người dung.

- Có tính năng DNS Security: Phát hiện lưu lượng độc hại và các cuộc tấn công DNS tunneling thông qua ThreatCloud, hệ thống tình báo mối đe dọa toàn cầu. ThreatCloud phân tích các yêu cầu DNS và gửi phán quyết trở lại nhằm loại bỏ hoặc cho phép yêu cầu DNS trong thời gian thực. Điều này ngăn hành vi trộm cắp dữ liệu thông qua DNS tunneling và giao tiếp C2C giữa máy chủ bị nhiễm bên trong và máy chủ bên ngoài.

- Có tính năng Zero-phishing: Ngăn chặn cả các cuộc tấn công lừa đảo đã biết và zero-day, bằng cách phân tích các tính năng khác nhau trên URL trong thời gian thực (bao gồm cả sự tương đồng về thương hiệu, các ký tự không phải ASCII và thời gian đăng ký).

Ngoài ra, nó không chỉ điều tra URL mà còn toàn bộ các thành phần biểu mẫu HTML. Khi người dùng cuối nhấp vào trường nhập liệu, mã JavaScript sẽ quét nội dung trang trong thời gian thực và gửi thông tin đến engine Zero Phishing để phân tích dựa trên AI.

- Có tính năng giả lập mối đe dọa: Cung cấp khả năng chống lại các mối đe dọa không xác định trong các tệp được tải xuống từ Internet hoặc đính kèm với e-mail, bảo vệ mạng chống lại phần mềm độc hại mới, lỗ hổng zero-day và các cuộc tấn công có chủ đích.

- Tính năng trích xuất mối đe dọa: Loại bỏ nội dung có thể khai thác trong tệp để loại bỏ các mối đe dọa tiềm ẩn, đồng thời cấu trúc lại các tệp và cung cấp nội dung đã được khử trùng cho người dùng trong vài giây

- Giao diện giám sát/theo dõi: thời gian thực, báo cáo nhiều định dạng (CSV, PDF, Image), gửi báo cáo/cảnh báo theo nhiều phương thức như email, SNMP.

1.5.2.3. Cam kết từ nhà cung cấp dịch vụ

- Bản quyền dịch vụ hỗ trợ từ hãng.

- Cập nhật các bản vá lỗi (nếu có trong quá trình vận hành).

- Hỗ trợ xử lý sự cố (nếu có) trên Firewall từ chính hãng trong quá trình vận hành.

1.5.2.4. Khả năng xử lý ứng cứu nhà cung cấp dịch vụ

- Hỗ trợ kỹ thuật qua điện thoại hoặc hỗ trợ nhanh tại chỗ 24hx7ngày/ tuần;

- Thời gian đáp ứng (24hx7ngày/ tuần) ≤ 4 giờ;

- Giám sát hệ thống theo thời gian thực 24hx7ngày/ tuần;

- Gửi cảnh báo các vi phạm ở mức độ nghiêm trọng qua email.

1.5.3. Dịch vụ Phát hiện, cảnh báo sớm các vấn đề nguy cơ liên quan đến an toàn thông tin (SIEM)

1.5.3.1. Phạm vi bảo vệ và cung ứng của dịch vụ

Bảo vệ tổng thể toàn bộ các máy chủ và hệ thống trong phạm vi dự án.

1.5.3.2. Yêu cầu chất lượng dịch vụ

- Có khả năng thu thập log trên mọi môi trường: Log Network, Log Server,Môi trường Docker Container, Môi trường ảo hóa hypervisor (VMWare, HyperV..vv), Syslog từ các hệ thống ATTT (firewall, IPS, APT, Endpoint Security, PAM, WAF, DDOS,…vv); lấy trực tiếp hoặc nhận forward từ hệ thống SIEM khác, log từ các hệ thống EDR như Crowstrike, SentinelOne, CarbonBlack, TrendMicro,…

- Có khả năng hợp nhất các bước thu thập, phát hiện, phân tích, phản ứng, ngăn chặn, điều tra truy vết trên một giao diện tập trung duy nhất.

- Có tính năng thu thập và xử lý thông tin: thu thập thông tin từ nhiều nguồn khác nhau (Network traffic, log server, log từ thiết bị mạng, môi trường ảo hóa public/private cloud, container), chuyển đổi dữ liệu thành metadata, kiến trúc hóa lại dưới dạng Interflow, làm sạch, làm giàu dữ liệu bằng Threat Intelligence, geo-location, tương quan dữ liệu…

- Có tính năng phân tích, phát hiện: sử dụng AI, Threat Intelligence, , SANDBOX, UEBA, anti-Phishing, Deception, NTA…

- Có tính năng: Điều tra bằng Threat hunting (manually hoặc tự động), tạo ra các query với nhiều điều kiện lọc khác nhau…

- Cho phép tích hợp với TI hãng thứ 3 qua giao thức STIX/TAXII

- Hỗ trợ tích hợp với các file IOC của khách hàng

  - Các nguồn Open Source.
  - Các nguồn Comecial source.

- Hỗ trợ nhiều loại biểu đồ, hình ảnh đồ họa trực quan.

- Đơn giản hóa quá trình giám sát, phân tích: hỗ trợ tự động xử lý dựa trên nền tảng hợp nhất, giảm số lượng log và cảnh báo, đưa ra hướng dẫn và tham chiếu cho các trường hợp xử lý cụ thể.

- Hỗ trợ các tính năng: Phản ứng, ngăn chặn theo nhiều hình thức khác nhau:

  - Gửi tín hiệu đến tường lửa để ngăn chặn IP.
  - Gửi tín hiệu đến EDR để cô lập host, kill threat.
  - Gửi tín hiệu đến AD để disable user.
  - Gửi tín hiệu đến Email.
  - Gửi tín hiệu đến webhook (hỗ trợ tích hợp với các hệ thống ticket).
  - Gửi tín hiệu qua SSH đến các thiết bị ATTT để phản ứng.

- Hệ thống phải đáp ứng các yêu cầu kỹ thuật cơ bản đối với sản phẩm quản lý và phân tích sự kiện an toàn thông tin theo Quyết định số 1127/QĐ-BTTTT ngày 30/07/2021 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ).

- Hệ thống phải đáp ứng theo yêu cầu kỹ thuật theo Quyết định số 1356/QĐ-BTTTT ngày 07 tháng 7 năm 2022 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ).

1.5.3.3. Cam kết từ nhà cung cấp dịch vụ

- Giám sát ANTT liên tục 24/7 và cảnh báo ngay khi có phát hiện.

- Cam kết hỗ trợ hỗ trợ xử lý sự cố từ các chuyên gia trong và ngoài nước của hãng.

- Cung cấp các cảnh báo trước các hành vi tấn công, hoặc các báo cáo chi tiết truy vết sau tấn công. Cung cáp chi tiết thông tin file lây nhiễm (nếu có) và phân tích chi tiết hành vi, hướng xử lý file mã độc này.

- Đảm bảo lưu trữ log hệ thống đầy đủ (tối thiểu 3 tháng) phòng trường hợp bên sử dụng dịch vụ có yêu cầu cung cấp thông tin log cũ.

- Đảm bảo hệ thống cung cấp đầy đủ các tính năng như mô tả, sự hỗ trợ đầy đủ từ hãng, license vẫn đảm bảo thời gian sử dụng.

- Bản quyền dịch vụ hỗ trợ từ hãng được mua hàng năm

- Hỗ trợ kỹ thuật qua điện thoại hoặc hỗ trợ nhanh tại chỗ 24hx7ngày/ tuần
- Thời gian đáp ứng từ 4h đến 8h
- Cập nhật các bản vá lỗi mới nhất
- Thực hiện các công việc như sau:

STT	Tên công việc	Bộ phận xử lý	Thời gian thực hiện cam kết
1.	Tích hợp dịch vụ vào hệ thống tương ứng đã thuê để bảo vệ.	Quản trị hệ thống	Hành chính.
2.	Cấu hình chính sách policy thích hợp cho từng hệ thống.	Quản trị hệ thống	Hành chính.
3.	Cung cấp danh sách policy đã apply và cam kết thực hiện dịch vụ đúng theo các policy này theo chuẩn SLA cam kết.	Quản trị hệ thống	Hành chính
4.	Giám sát ANTT 24/7 theo chính sách đề ra nhằm đảm bảo thực hiện đủ các policy đã được đồng ý giữa các bên.	Bộ phận NOC.	Thực hiện giám sát 24/7
5.	Cảnh báo thời gian thực khi có vi phạm về policy.	Bộ phận NOC	24/7
6.	Hỗ trợ xử lý, giải quyết dứt điểm sự cố.	Bộ phận NOC.	24/7
7.	Báo cáo sau sự cố, hướng dẫn cách phòng ngừa khắc phục triệt để.	Quản trị hệ thống	Hành chính.
8.	Kiểm tra ANTT trên toàn bộ hệ thống, nhằm đảm bảo sự cố đã giải quyết triệt để, không bị lây nhiễm sang hệ thống khác. Khắc phục, cập nhật lại chính sách policy mới (nếu cần).	Quản trị hệ thống	Hành chính.
9.	Cung cấp các báo cáo định kỳ liên quan của hệ thống.	Quản trị hệ thống	Hành chính.

1.5.3.4. Khả năng xử lý ứng cứu của nhà cung cấp dịch vụ

- Hỗ trợ kỹ thuật qua điện thoại hoặc hỗ trợ nhanh tại chỗ 24hx7ngày/ tuần
- Thời gian đáp ứng (24hx7ngày/ tuần) ≤ 4 giờ
- Giám sát hệ thống theo thời gian thực 24hx7ngày/ tuần
- Gửi cảnh báo các vi phạm ở mức độ nghiêm trọng qua email

1.5.4. Dịch vụ phòng chống phần mềm độc hại trên môi trường mạng (APT)

1.5.4.1. Phạm vi bảo vệ và cung ứng của dịch vụ

Bảo vệ tổng thể toàn bộ các máy chủ và hệ thống trong phạm vi dự án.

1.5.4.2. Yêu cầu về chất lượng dịch vụ

- Hỗ trợ kiểm tra, phân tích các lưu lượng mạng để phát hiện các hành vi đáng ngờ
- Hỗ trợ khả năng phát hiện và kiểm tra các loại mã độc dựa trên các phương thức khác nhau.
- Hỗ trợ phân tích các tập tin đính kèm mã độc, bị nghi là mã độc.
- Hỗ trợ theo dõi tất cả các cổng mang và đa dạng giao thức (tối thiểu 80 giao thức)
- Hỗ trợ khả năng phát hiện toàn bộ các giai đoạn của kiểu tấn công APT, cung cấp khả năng phân tích theo từng giai đoạn từ giai đoạn khai thác hệ thống cho tới giai đoạn lấy cắp thông tin
- Hỗ trợ khả năng hiển thị các trường thông tin chi tiết của các mối nguy được phát hiện như loại mã độc, mức độ nguy hiểm, địa chỉ IP, port, giao thức, Domain, timestamp, nguồn và đích của cuộc tấn công
- Hỗ trợ khác năng phát hiện và phân tích các mối đe dọa thông thường, các mối đe dọa nâng cao trong hệ thống nội bộ của doanh nghiệp
- Hỗ trợ khả năng cập nhật các mối đe dọa mới nhất.
- Hỗ trợ khả năng cập nhật thường xuyên danh sách các URL, C&C Server, các domain, địa chỉ IP… có chứa mã độc.
- Hỗ trợ khả năng phát hiện các kết nối tới các máy chủ điều khiển (C&C Server) đối với các loại mã độc malware, bot, downloader, data stealing, worm, … thông qua tính năng Malware, C&C, Attacker Activity
- Hỗ trợ khả năng ngăn chặn kết nối độc hại.
- Hỗ trợ tính năng XFF (X-Forwarder-For) trong môi trường có sử dụng Proxy (tính năng Proxy Monitoring).
- Hỗ trợ phân tích các hành vi dựa trên thư viện các hành vi có sẵn dựa vào Malicious Behavior Patterns.
- Hỗ trợ khả năng phát hiện các mối nguy tồn tại trong hệ thống như: các kiểu tấn công zero day, exploit code, các lỗ hổng phổ biến.

- Hỗ trợ môi trường ảo như Sandbox được tích hợp sẵn bên trong giải pháp hoặc tích hợp với các môi trường Sandbox trong các sản phẩm khác để phân tích các mã độc.

- Hỗ trợ khả năng phân tích đầy đủ tất cả các kiểu tập tin như: .swf, JAVA, Aplet, jar, .chm, .Ink, .pdf, .rar, .tar, .exe, .7z, .bz2, .zip, Microsoft Office.

- Hỗ trợ phân tích các tập tin có dung lượng lớn hơn 10 MB (tối đa lên đến 15MB).

- Hỗ trợ khả năng trích xuất các file mã độc, các file bắt gói lưu lượng mạng để phân tích điều tra thêm.

- Hỗ trợ khả năng tương quan, xâu chuỗi, kết hợp các hành vi liên quan với nhau thông qua Correlated Logs, Excutive report.

- Hỗ trợ khả năng phân tích các mã độc trên các hệ điều hành phổ biến của thiết bị di động như Android, iOS.

- Hỗ trợ phân tích 2 chiều: inbound&outbound để xác định các payload/ document độc hại.

- Hỗ trợ nền tảng Cloud.

- Hỗ trợ khả năng hiển thị các máy chủ C&C trên khu vực địa lý khác nhau

- Khả năng tùy chỉnh xuất báo cáo đa dạng: giờ, ngày, tuần, tháng, quý, IP, loại tấn công, ...

- Hỗ trợ tùy chỉnh xuất các báo cáo dưới dạng các định dạng: csv, pdf

- Hỗ trợ khả năng tạo các truy vấn về kết quả các mới nguy được phát hiện tình trạng an ninh của các thành phần trong hệ thống, các URL độc hai, … sau đó xuất các báo cáo

- Thông báo ngay khi có phát hiện bất thường: qua email

- Hỗ trợ khả năng tích hợp với SIEM để tối ưu hóa cảnh báo và xây dựng report

- Hỗ trợ khả năng sử dụng các định dạng phổ biến của các loại log như CEF, LEEF

- Khả năng kết hợp với các giải pháp khác để phân tích chiều sâu, hỗ trợ mở rộng quản lý đa điểm thông qua tính năng IOC Information Sharing.

1.5.4.3. Cam kết từ nhà cung cấp dịch vụ

- Cam kết hỗ trợ xử lý sự cố từ các chuyên gia trong và ngoài nước của hãng.

- Giám sát ANTT liên tục 24/7 và cảnh báo ngay khi có phát hiện.

- Cung cấp các cảnh báo trước các hành vi tấn công, hoặc các báo cáo chi tiết truy vết sau tấn công. Cung cáp chi tiết thông tin file lây nhiễm (nếu có) và phân tích chi tiết hành vi, hướng xử lý file mã độc này.

- Đảm bảo lưu trữ log hệ thống đầy đủ (tối thiểu 1 quý) phòng trường hợp bên sử dụng dịch vụ có yêu cầu cung cấp thông tin log cũ.

- Đảm bảo hệ thống cung cấp đầy đủ các tính năng như mô tả, sự hỗ trợ đầy đủ từ hãng, license vẫn đảm bảo thời gian sử dụng.

- Bản quyền dịch vụ hỗ trợ từ hãng được mua hàng năm
- Hỗ trợ kỹ thuật qua điện thoại hoặc hỗ trợ nhanh tại chỗ 24hx7ngày/ tuần
- Thời gian đáp ứng từ 4h đến 8h
- Cập nhật các bản vá lỗi mới nhất
- Thực hiện các công việc như sau:

STT	Tên công việc	Bộ phận xử lý	Thời gian thực hiện cam kết
1.	Tích hợp dịch vụ vào hệ thống tương ứng đã thuê để bảo vệ.	Quản trị hệ thống	Hành chính.
2.	Cấu hình chính sách policy thích hợp cho từng hệ thống.	Quản trị hệ thống	Hành chính.
3.	Cung cấp danh sách policy đã apply và cam kết thực hiện dịch vụ đúng theo các policy này theo chuẩn SLA cam kết.	Quản trị hệ thống	Hành chính
4.	Giám sát ANTT 24/7 theo chính sách đề ra nhằm đảm bảo thực hiện đủ các policy đã được đồng ý giữa các bên.	Bộ phận NOC.	Thực hiện giám sát 24/7
5.	Cảnh báo thời gian thực khi có vi phạm về policy.	Bộ phận NOC	24/7
6.	Hỗ trợ xử lý, giải quyết dứt điểm sự cố.	Bộ phận NOC.	24/7
7.	Báo cáo sau sự cố, hướng dẫn cách phòng ngừa khắc phục triệt để.	Quản trị hệ thống	Hành chính.
8.	Kiểm tra ANTT trên toàn bộ hệ thống, nhằm đảm bảo sự cố đã giải quyết triệt để, không bị lây nhiễm sang hệ thống khác. Khắc phục, cập nhật lại chính sách policy mới (nếu cần).	Quản trị hệ thống	24/7
9.	Cung cấp các báo cáo định kỳ liên quan của hệ thống.	Quản trị hệ thống	Hành chính.

1.5.4.4. Khả năng xử lý ứng cứu của nhà cung cấp dịch vụ

- Hỗ trợ kỹ thuật qua điện thoại hoặc hỗ trợ nhanh tại chỗ 24hx7ngày/ tuần
- Thời gian đáp ứng (24hx7ngày/ tuần) ≤ 4 giờ
- Giám sát hệ thống theo thời gian thực 24hx7ngày/ tuần
- Gửi cảnh báo các vi phạm ở mức độ nghiêm trọng qua email

1.5.5. Dịch vụ phòng chống mã độc trên máy chủ

1.5.5.1. Phạm vi bảo vệ và cung ứng của dịch vụ

Bảo vệ tổng thể toàn bộ các máy chủ trong phạm vi dự án.

1.5.5.2. Yêu cầu về chất lượng dịch vụ

- Có khả năng bảo vệ theo thời gian thực và theo yêu cầu chống lại các mối đe dọa dựa trên tệp (file-based threats), bao gồm malware, virus, trojan và spyware. Để xác định các mối đe dọa, module này sẽ kiểm tra các tệp trên ổ cứng đem so với cơ sở dữ liệu mối đe dọa toàn diện, cũng như kiểm tra các tệp để tìm một số đặc điểm nhất định, chẳng hạn như việc nén và các mã khai thác đã biết.

- Có khả năng sử dụng thông tin IoC về các mẫu malware phổ biến để IR client kiểm tra, đánh giá. Hệ thống IoC được cập nhật thường xuyên: IP blacklist, Url độc hại, C&C server, Virus signatures, MD5 hashes, botnet command.

- Có khả năng sử dụng dữ liệu Threat Intelligent (TI Data) để kiểm tra thông tin về một hành vi, dấu hiệu bất thường để hệ thống đưa ra quyết định tệp tin có bị nhiễm malware không. Dữ liệu Threat Intelligent (TI Data) bao gồm các thông tin như IP blacklist, Url độc hại, C&C server, thuật toán/kỹ thuật mã độc sử dụng (Ví dụ: thuật toán DGA sinh tên miền mã độc tự động), hành vi bất thường (Ví dụ: tiến trình cha chạy dưới quyền người dùng thấp hơn tiến trình con).

- Có khả năng sử dụng thuật toán học máy (Machine Learning) nhằm phát hiện và cảnh báo các sự kiện bất thường trên máy client. Ngoài ra, hệ thống còn có khả năng tự học liên tục từ các dữ liệu bất thường thu thập được từ máy client. So với phương pháp truyền thống chủ yếu sử dụng signature, các rule, hash để phát hiện như hiện nay, thì phương pháp này có khả năng phát hiện, ngăn chặn và loại bỏ mã độc sớm hơn, giảm thiểu tối đa thiệt hại do mã độc gây ra

- -Cung cấp giao diện theo dõi, quản trị cho quản trị viên, trích xuất những thông tin cần thiết. Mỗi quản trị viên tại các đơn vị chỉ theo dõi được hoạt động của các Agent cài trên đơn vị của mình theo phân quyền. Quản trị viên của hệ thống sẽ có quyền xem dữ liệu toàn bộ Agent trong hệ thống và phân quyền cho quản trị viên tại các đơn vị khác.

- Đảm bảo các chức năng:

STT	Nội dung yêu cầu
1	Chức năng tự động cập nhật

	Có chức năng cho phép cập nhật tự động phiên bản mới của các phần mềm phòng, chống mã độc được cài đặt trên các máy trạm (agent)
	Có chức năng cho phép cập nhật tự động dấu hiệu phát hiện mã độc mới trên các agent
2	Chức năng quản trị tập trung
	Hỗ trợ các hệ điều hành Windows Server từ 2019 trở lên, Linux CentOS, Redhat, Ubuntu
	Có khả năng phân quyền cho người quản trị và cán bộ phân tích vận hành bảo mật
3	Chức năng quét virus trực tuyến (Online Scanner)
	Scan các tập tin
	Thống kê các tập tin đã quét
	Thống kê các tập tin mã độc đã phát hiện
	Theo dõi tài nguyên máy chủ đang sử dụng
	Quản lý các key API đã cấp phát
4	Chức năng cho phép chia sẻ thông tin, dữ liệu thống kê tình hình lây nhiễm mã độc với hệ thống kỹ thuật của cơ quan chức năng có thẩm quyền
	Có chức năng kết nối, chia sẻ thông tin từ hệ thống quản lý tập trung với hệ thống kỹ thuật của cơ quan chức năng theo tiêu chuẩn, quy chuẩn quốc gia và yêu cầu kỹ thuật tại Văn bản số 2290/BTTTT-CATTT ngày 17/7/2018.
	Thông tin chia sẻ bao gồm nhưng không giới hạn những thông tin sau:
	Thông tin về cơ quan, tổ chức chia sẻ thông tin tại Phụ lục 2 Văn bản số 2290/BTTTT-CATTT ngày 17/7/2018.
	Thông tin về tình hình lây nhiễm mã độc trên các máy trạm của cơ quan, tổ chức tại Phụ lục 2 Văn bản số 2290/BTTTT-CATTT ngày 17/7/2018
5	Giám sát, dò quét các mối nguy hại phát tán qua email và website độc hại
	Giám sát, dò quét các đối tượng nguy hiểm được phát tán bằng email thông qua giao thức POP3, SMTP.

	Giám sát, dò quét các đối tượng nguy hiểm được phát tán qua các website độc hại, các url độc hại thông qua giao thức HTTP, HTTPS.

Các yêu cầu chi tiết tính năng phần mềm phòng chống mã độc và phần mềm diệt virus như sau:

STT	Yêu cầu kỹ thuật	Yêu cầu kỹ thuật chi tiết
I	**Nhóm chức năng giám sát bất thường**	
1	Thu thập thông tin, giám sát sự kiện ATTT	Thống kê process trên máy tính, phát hiện kịp thời các process bất thường
		Liệt kê những kết nối trong mạng, phát hiện những kết nối bất thường
		Giám sát việc tạo file trên hệ thống
2	Phân tích, cảnh báo	Phát hiện những hành vi bất thường trên máy chủ
		Cho phép tìm kiếm, điều tra log event của toàn bộ các máy chủ
		Phân tích các tiến trình đang chạy từ xa trên máy mục tiêu
		Đưa ra cảnh báo đối với những bất thường trong toàn mạng của tổ chức đến quản trị viên
		Cho phép điều tra phản ứng trên một giao diện duy nhất
3	Ứng phó	Thực hiện remote console từ xa tới máy mục tiêu để điều tra xử lý
		Hỗ trợ cô lập tạm thời các máy phục vụ điều tra.
		Hỗ trợ tạo kịch bản phản ứng và deploy trên diện rộng
II	**Nhóm chức năng diệt virus**	
1	Phát hiện, cách ly, xóa bỏ các loại mã độc như: virus, mã độc mã hóa tống tiền (ransomeware), lừa đảo (phishing), thư rác	
2	Kiểm soát, bảo vệ máy chủ khỏi các phần mềm có nguồn gốc không rõ ràng	

STT	Yêu cầu kỹ thuật	Yêu cầu kỹ thuật chi tiết
3	Bảo vệ chủ động theo thời gian thực (Real-time Protection)	
4	Tự động quét lọc khi phát hiện có thay đổi file, thư mục	
5	Quét virus theo lịch	
III	**Nhóm chức năng thống kê, báo cáo**	
1	Thống kê thông tin về mã độc, tuân thủ chính sách	Thống kê những lỗ hổng nghiêm trọng có thể trở thành mục tiêu tấn công của hacker
		Thống kê các sự kiện bất thường được phát hiện
		Thống kê thông tin về các loại mã độc được phát hiện trong mạng lưới
2	Báo cáo về tình hình mã độc, tuân thủ chính sách trong tổ chức	Báo cáo về số lượng mã độc
		Báo cáo về mức độ tuân thủ chính sách ATTT
IV	**Chức năng cho phép chia sẻ thông tin, dữ liệu thống kê tình hình lây nhiễm mã độc với hệ thống kỹ thuật của cơ quan chức năng có thẩm quyền**	
1	Có chức năng kết nối, chia sẻ thông tin từ hệ thống quản lý tập trung với hệ thống kỹ thuật của cơ quan chức năng theo tiêu chuẩn, quy chuẩn quốc gia và yêu cầu kỹ thuật tại Văn bản số 2290/BTTTT-CATTT ngày 17/7/2018.	
2	Thông tin chia sẻ bao gồm nhưng không giới hạn những thông tin sau:	
3	Thông tin về cơ quan, tổ chức chia sẻ thông tin tại Phụ lục 2 Văn bản số 2290/BTTTT-CATTT ngày 17/7/2018.	

1.5.5.3. Cam kết từ nhà cung cấp dịch vụ

- Bản quyền dịch vụ hỗ trợ từ hãng
- Cập nhật các bản vá lỗi (nếu có trong quá trình vận hành)
- Hỗ trợ xử lý sự cố (nếu có) từ chính hãng trong quá trình vận hành

1.5.5.4. Khả năng xử lý ứng cứu của hệ thống của nhà cung cấp dịch vụ

- Hỗ trợ kỹ thuật qua điện thoại hoặc hỗ trợ nhanh tại chỗ 24hx7ngày/ tuần

- Thời gian đáp ứng (24hx7ngày/ tuần) ≤ 4 giờ
- Giám sát hệ thống theo thời gian thực 24hx7ngày/ tuần
- Gửi cảnh báo các vi phạm ở mức độ nghiêm trọng qua email

1.5.6. Dịch vụ phòng chống tấn công DDoS

1.5.6.1. Phạm vi bảo vệ và cung ứng của dịch vụ

Bảo vệ tổng thể toàn bộ các máy chủ và hệ thống trong phạm vi dự án.

1.5.6.2. Yêu cầu chất lượng dịch vụ

- Giám sát và ngăn chặn các tấn công nhằm chiếm hết tài nguyên của hệ thống. Khi số lượng yêu cầu truy cập quá lớn, máy chủ sẽ quá tải và không còn khả năng xử lý, làm cho hệ thống không thể phục vụ các yêu cầu của người dùng thật.
- Bảo vệ thực hiện giám sát lưu lượng truy cập thông qua các lưu lượng mẫu bao gồm cả header và payload của gói tin. Kiểm tra và phát hiện nhanh chóng, chính xác mọi lưu lượng tấn công DDoS bằng cách kết hợp phân tích dựa trên quy tắc và học máy.
- Thông tin về các tấn công bị phát hiện ở thời gian thực: khi phát hiện tấn công, Traffic Monitoring thể hiện trên giao diện.
- Cập nhật tự động bảo vệ, chủ động chống lại các cuộc tấn công DDoS và các mối đe dọa về an ninh hệ thống.
- Hỗ trợ băng thông dò quét tấn công DdoS năng lực xử lý tối thiểu >= 100Gbps.

1.5.6.3. Cam kết từ nhà cung cấp dịch vụ

- Bản quyền dịch vụ hỗ trợ từ hãng
- Cập nhật các bản vá lỗi (nếu có trong quá trình vận hành)
- Tất cả các dịch vụ cung cấp đều có sự hỗ trợ xử lý sự cố (nếu có) từ chính hãng trong quá trình vận hành

1.5.6.4. Khả năng xử lý ứng cứu của nhà cung cấp dịch vụ

- Hỗ trợ kỹ thuật qua điện thoại hoặc hỗ trợ nhanh tại chỗ 24hx7ngày/ tuần
- Thời gian đáp ứng (24hx7ngày/ tuần) ≤ 4 giờ
- Giám sát hệ thống theo thời gian thực 24hx7ngày/ tuần
- Gửi cảnh báo các vi phạm ở mức độ nghiêm trọng qua email

1.5.7. Dịch vụ tường lửa ứng dụng Web

1.5.7.1. Phạm vi bảo vệ và cung ứng của dịch vụ

Bảo vệ tổng thể toàn bộ các máy chủ và hệ thống trong phạm vi dự án.

1.5.7.2. Yêu cầu chất lượng dịch vụ

Dịch vụ phòng chống các cuộc tấn công ở lớp ứng dụng web cho hệ thống các website sử dụng thiết bị chuyên dụng với các tính năng như sau:

- Hỗ trợ các giao thức ở tầng ứng dụng: HTTP, HTTPS.

- Mã hóa kết nối quản lý của quản trị viên

- Dịch vụ tường lửa ứng dụng web (WAF) có các tính năng bảo vệ như sau:

- Có tính năng kiểm tra giao thức kết nối Web có tuân theo chuẩn RFC không, nhằm phát hiện các bất thường trong địa chỉ URL và các giao thức.

- Có khả năng "Vá ảo" (Virtual Patching) các lỗ hổng ứng dụng web được WAF phát hiện bảo vệ các điểm yếu ngay lập tức trước khi công việc cài đặt, sửa chữa lỗ hổng có thể được thực hiện trên máy chủ ứng dụng Web. Có thể sử dụng kết quả từ các giải pháp quét đánh giá điểm yếu ứng dụng web của các hãng thứ ba như WhiteHat, IBM, Cenzic, NT OBJECTives, Qualys,.. để tạo policy bảo vệ các điểm yếu được phát hiện ra.

- Có tính năng cho phép học và hiểu được cấu trúc và logic hoạt động của ứng dụng, giúp ngăn chặn cả những tấn công chưa biết.

- Có tính năng nhận biết và ngăn chặn dữ liệu nhạy cảm thất thoát qua website.

- Chống các tấn công tinh vi nhằm vào các điểm yếu trên ứng dụng web được nêu trong top 10 OWASP như là SQL injection, Cross-Site Scripting (XSS), cross site request forgery (CSRF), tấn công tràn vùng đệm, DoS... chống lây nhiễm mã độc hại vào website.

- Có tính năng "tự học", phân tích và hiểu rất sâu về kết nối và đặc thù hoạt động của một ứng dụng Web cụ thể. Tường lửa có thể phân tích và hiểu được cấu trúc và cơ cấu hoạt động của website; kiểm tra mọi thành phần của ứng dụng như các tham số URL, cookies, trường nhập liệu, các truy vấn SQL cũng như nhiều yếu tố khác.. Nhờ vậy tường lửa có thể bảo vệ tốt các điểm yếu mà rất riêng và đặc thù với từng ứng dụng Web cụ thể. Khả năng "tự học" cấu trúc, các thành phần và cơ chế hoạt động của ứng dụng, dịch vụ web cũng cho phép tường lửa tự động cập nhật chính sách mỗi khi có thay đổi và không phải can thiệp bằng tay.

- Có tính năng liên hệ/xâu chuỗi nhiều sự kiện để phát hiện tấn công: khả năng này cho phép xử lý các hành vi/vi phạm đáng ngờ bằng việc đánh giá các sự kiện qua khoảng thời gian dài và qua nhiều lớp phát hiện (malicious encoding, HTTP protocol violations, application proile violations, data leak prevention, signatures, Web worms)

- Có tính năng kiểm tra nội dung mã hóa – SSL để phát hiện và ngăn chặn các tấn công

- Có tính năng tự động nhận biết tên của người sử dụng ứng dụng web và các hoạt động; liên kết tất cả các phiên giao dịch với người sử dụng cụ thể. Khi giải pháp được mở rộng để bảo vệ cơ sở dữ liệu, nó có thể theo dõi các truy vấn SQL tương ứng với người dùng và ứng dụng web.

- Hỗ trợ tính năng cho phép chủ động phân tích, tìm kiếm và cung cấp thông tin về các nguồn gốc phát động tấn công từ Internet để ngăn chặn nguy hiểm ngay từ nguồn trước khi các cuộc tấn công có thể xảy ra. Với cách thức này, giải pháp cho phép ngăn chặn những tấn công tự động đồng loạt trên diện rộng một cách hiệu quả.

1.5.7.3. Cam kết từ nhà cung cấp dịch vụ

- Bản quyền dịch vụ hỗ trợ từ hãng
- Cập nhật các bản vá lỗi và nhận dạng tấn công (nếu có trong quá trình vận hành)
- Hỗ trợ xử lý sự cố (nếu có) từ chính hãng trong quá trình vận hành

1.5.7.4. Khả năng xử lý từ nhà cung cấp dịch vụ

- Hỗ trợ kỹ thuật qua điện thoại, email hoặc hỗ trợ nhanh tại chỗ 24hx7ngày/ tuần
- Thời gian đáp ứng ≤ 4h
- Giám sát hệ thống theo thời gian thực 24hx7ngày/ tuần
- Gửi cảnh báo các vi phạm ở mức độ nghiêm trọng qua email.

1.5.8. Dịch vụ cân bằng tải

1.5.8.1. Phạm vi bảo vệ và cung ứng của dịch vụ

Bảo vệ tổng thể toàn bộ các máy chủ và hệ thống trong phạm vi dự án.

1.5.8.2. Yêu cầu chất lượng dich vụ

Dịch vụ cân bằng tải cho hệ thống, sử dụng thiết bị chuyên dụng với các tính năng như sau:

- Có tính năng cân bằng tải ứng dụng đóng vai trò quan trọng cân bằng tải cho một nhóm Server cung cấp cùng một dịch vụ theo chiều Inbound từ Internet và cân băng tải traffic kết nối Internet theo chiều Outbound. Một số tính năng chính như sau:
  - Cân bằng tải thông minh, bao gồm cả Layer 4 và Layer 7 Load Balancing.
  - SSL Offloading và tăng tốc ứng dụng.
  - Tối ưu TCP Client-side.
  - Tối ưu TCP Server-side.
  - IPv6 Gateway.
  - Fast Cache.
  - Nén thông minh.
  - Chia băng thông L7.
  - Giám sát trạng thái ứng dụng.
- Có tính năng cân bằng tải địa lý bằng cách tận dụng Hệ thống tên miền trên toàn thế giới (DNS). Tích hợp với tính năng cân bằng tải ứng dụng để đảm bảo rằng các yêu cầu ứng dụng luôn được chuyển đến tài nguyên thích hợp và có sẵn trong bất kỳ trung tâm dữ liệu nào trên toàn thế giới. GTM cũng cung cấp các dịch vụ DNS thông minh cả bên trong lẫn bên ngoài. Một số tính năng chính như sau:
  - Định tuyến lưu lượng truy cập thông qua vị trí địa lý.
  - Bảo mật phân phối ứng dụng toàn cầu.
  - IP Anycast.
  - DNS Security Extensions (DNSSEC).
  - DNS v6.
  - DNS Caching & Resolving.

+ Phòng thủ các tấn công DNS.
+ Tường lửa DNS.
+ DNS Express cho các phản hồi truy vấn tốc độ cao.

- Có tính năng kiểm tra lưu lượng truy cập lớp 7 được sử dụng để đảm bảo an ninh cho các tài nguyên nằm phía sau nó.Một số tính năng chính như sau:

+ Bảo vệ các tấn công web.
+ Nhận biết ứng dụng L7.
+ Tích hợp tường lửa XML.
+ Bảo vệ và che giấu dữ liệu.
+ Sự tương quan vi phạm và nhóm sự cố.
+ Triển khai in-line.
+ Báo cáo toàn diện.
+ Tích hợp các giải pháp quét lỗ hổng web.
+ Làm xáo trộn dữ liệu quan trọng tránh bị đánh cắp.
+ Chống tấn công DdoS.
+ Nhận diện địa chỉ IP xấu.
+ Logs toàn bộ HTTP request/response.
+ Virtual Patching.
+ Bot Defense: Chủ động bảo vệ các ứng dụng của bạn khỏi các cuộc tấn công tự động bằng bot và các công cụ tấn công khác. Điều này ngăn chặn các cuộc tấn công DoS của lớp 7, tấn công web và tấn công brute-force. Phòng chống bot chủ động giúp xác định và giảm thiểu các cuộc tấn công trước khi chúng gây thiệt hại cho dịch vụ web.
+ Datasafe: bảo vệ khách hàng khỏi phần mềm độc hại và keylogger ăn cắp dữ liệu và thông tin đăng nhập để truy cập trái phép vào tài khoản người dùng trên broswer client.
+ Bảo mật API: Triển khai các công cụ bảo mật các API REST / JSON, XML và GWT.
+ Phân tích hành vi: Phân tích hành vi DoS cung cấp sự bảo vệ tự động chống lại các cuộc tấn công DDoS bằng cách phân tích hành vi lưu lượng sử dụng máy học và phân tích dữ liệu. Bằng cách liên tục theo dõi tình trạng máy chủ và tải bất thường (giảm tốc độ hoạt động hoặc tăng lưu lượng truy cập) có thể được phát hiện chính xác và giảm thiểu khi cần thiết.
+ SDK Mobile: có khả năng cung cấp cho bạn toàn quyền kiểm soát ứng dụng.

1.5.8.3. Cam kết từ nhà cung cấp dịch vụ

- Bản quyền dịch vụ hỗ trợ từ hãng
- Cập nhật các bản vá lỗi (nếu có trong quá trình vận hành)
- Hỗ trợ xử lý sự cố (nếu có) từ chính hãng trong quá trình vận hành

1.5.8.4. Khả năng xử lý ứng cứu của nhà cung cấp dịch vụ

- Hỗ trợ kỹ thuật qua điện thoại hoặc hỗ trợ nhanh tại chỗ 24hx7ngày/ tuần
- Thời gian đáp ứng (24hx7ngày/ tuần) ≤ 4 giờ
- Giám sát hệ thống theo thời gian thực 24hx7ngày/ tuần

- Gửi cảnh báo các vi phạm ở mức độ nghiêm trọng qua email

1.5.9. Dịch vụ phòng chống thất thoát dữ liệu

1.5.9.1. Phạm vi bảo vệ và cung ứng dịch vụ

Bảo vệ tổng thể toàn bộ các máy chủ và hệ thống trong phạm vi dự án

1.5.9.2. Năng lực xử lý và ứng cứu hệ thống

Dịch vụ phòng chống thất thoát dữ liệu xác định và ngăn chặn các hành vi vi phạm, trích xuất hoặc phá hủy dữ liệu nhạy cảm ngoài ý muốn. Các doanh nghiệp, tổ chức sử dụng dịch vụ này để bảo mật và bảo vệ dữ liệu cũng như tuân thủ các yêu cầu pháp lý.

Mô hình triển khai: Client - Server (Máy trạm và các máy chủ được cài agent phòng chống thất thoát dữ liệu, và được kết nối đến máy chủ quản trị tập trung)

Tính năng Gateway Anti – Malware, hỗ trợ HTTPS

- Ngăn chặn phần mềm độc hại xâm nhập vào hệ thống giảm thiểu gánh nặng cho các giải pháp bảo mật trên endpoint. Tối ưu hóa bảo mật trong một giải pháp duy nhất với nhiều công nghệ khác nhau. Kiểm tra sâu nội dung gói tin, quét các file dữ liệu: PDF, word, excel,… tìm phần mềm độc hại ẩn.
- Ngăn chặn việc download mã độc, virus, spyware… các hành vi của botnet cũng như các kết nối C&C callback ra ngoài Internet. Cô lập các Spyware trước khi chúng có thể phát tán hay chiếm quyền hệ thống
- Kiểm soát các kết nối HTTPS thông qua cơ chế giải mã và kiểm tra nội dung gói tin được mã hóa.

Tính năng Web Reputation kết hợp tương quan dữ liệu thời gian thực

- Ngăn chặn các truy cập vào các trang web độc hại. Smart Protection Network sử dụng thông tin từ hàng triệu sensor trên toàn thế giới, xử lý hàng tỷ query hàng ngày. Bên cạnh cơ sở dữ liệu về những website, URL, domain độc hại, Web Reputation cung cấp cơ chế tính điểm đối với từng website, URL cụ thể để đánh giá mức độ an toàn khi người dùng kết nối tới.
- Cơ chế tương quan các sự kiện cho phép chống lại các mối đe dọa mới và hoạt động đáng ngờ trong thời gian thực.
- Xác định, ngăn chặn botnet và các kết nối C&C trong các cuộc tấn công có chủ đích.

Phân loại và lọc nội dung (URL Filtering)

- Sử dụng cơ sở dữ liệu về URL bao gồm các nhóm Website khác nhau giúp chuẩn đoán nội dung và các hoạt động của các website này, phân loại nội dung website được truy cập theo thời gian thực để nhận dạng các trang web không phù hợp hoặc Website độc hại từ đó đưa ra các đề xuất giúp bảo vệ toàn hoạt động của doanh nghiệp.
- Ngăn chặn việc truy cập tới các website giả mạo, tải các phần mềm gián điệp.

Kiểm soát truy cập ứng dụng:

- Liên tục giám sát và báo cáo các ứng dụng trên cloud và các ứng dụng internet khác nhau bao gồm: Office 365, G Suite, Dropbox, ứng dụng instant messaging, peer-to-peer, mạng xã hội, ứng dụng streaming media…

- Quản trị tập trung, xây dựng chính sách chi tiết, linh hoạt để kiểm soát tất cả hoạt động web.
- Thiết lập chính sách bảo mật khác nhau cho từng người dùng, nhóm người dùng hoặc các thành phần web gateway cụ thể.

Predictive Machine Learning:

- Hỗ trợ cơ chế Predictive Machine Learning sử dụng các thuật toán thông minh quét các nội dung của đối tượng, mô phỏng và hiểu hành vi của nó, dự đoán ý định. Predictive Machine Learning giúp lọc dữ liệu không an toàn trước khi gửi đến cloud sandboxing. Nó làm tăng hiệu quả và giảm thiểu thời gian phát hiện, ngăn chặn hiểm họa trong thời gian thực.

Ngăn chặn thất thoát dữ liệu (Cloud DLP):

- Sử dụng các template liên quan tới DLP để bảo vệ dữ liệu quan trọng, ngăn chặn rò rỉ do vô ý hoặc cố ý của con người.

Cung cấp giao diện giám sát, quản lý và báo cáo hợp nhất.

1.5.10. Dịch vụ ký số HSM

Năng lực xử lý và ứng cứu của hệ thống :

Tính năng	Đặc điểm
Lưu trữ khoá/ chứng thư số	Cho phép người dùng lựa chọn lưu trữ khoá/chứng thư số bên ở bên trong thiết bị hoặc bên ngoài hệ thống dưới dạng file mã hoá.
Số lượng partitions/ slots	Không giới hạn số lượng slots/ partitions
Số lượng kết nối tới các server ứngdụng	Không giới hạn số lượng kết nối. Có thể sử dụng HSM cho nhiều server ứng dụng khác nhau.
Tốc độ ký tối thiểu	Đáp ứng tối thiểu tốc độ ký là **16tps** (với độ dài khoá 2048 bit) có khả năng xử lý được đến **57,600** giao dịch trong vòng 01 giờ

1.5.11. Dịch vụ sao lưu và phục hồi dữ liệu

1.5.11.1. Phạm vi bảo vệ và cung ứng của dịch vụ

- Sao lưu toàn bộ máy chủ trong phạm vi dự án
- Theo nhu cầu và tình hình thực tế đề xuất thời gian cam kết sao lưu là 30 ngày.

1.5.11.2. Yêu cầu chất lượng dịch vụ

- Đảm bảo dữ liệu được sao lưu dự phòng ở 02 vùng lưu trữ khác nhau và ở 02 vị trí khác nhau.
- Cung cấp vùng lưu trữ để chứa các bản sao dữ liệu backup dựa trên giải pháp lưu trữ Cluster với ứng dụng các công nghệ tiên tiến nhất:

+ Tổ chức các nodes lưu trữ dữ liệu theo mô hình cluster dự phòng chia tải.

+ Kiến trúc Unified – hỗ trợ đồng thời SAN (8/16Gbps)

+ Khả năng mở rộng dung lượng lớn (>100TB).

+ Các ổ cứng trên các máy chủ ảo được gửi tới tủ đĩa lưu trữ được bảo vệ theo cấu hình RAID 6 hoặc tương đương với mục tiêu đảm bảo vận hành 24/7/365, không downtime một giây phút nào (Zero-Downtime)

+ Dữ liệu được di chuyển linh hoạt qua lại giữa các nodes lưu trữ. Đáp ứng như cầu nâng cấp mở rộng, bảo trì bảo dưỡng linh hoạt, không làm gián đoạn truy nhập dữ liệu.

ĐẶC ĐIỂM	Disk to disk	Disk to Tape
Sao lưu tự động	Có	Có
Nén dữ liệu	Có	Không
Thời gian restore cam kết (không chậm hơn)	Có. Chi tiết như sau: Restore Full VM: 100GB/ 90 phút Restore dữ liệu chỉ định: 20GB/ 45 phút	Có. Chi tiết như sau: Restore Full VM: 100GB/ 120 phút Restore dữ liệu chỉ định: 20GB/ 60 phút
Hỗ trợ live Support	Có	Có
Mã hóa truyền dữ liệu 256 bit - AES	Có	Có
Số lượng bản lưu và thời gian lưu	07 phiên bản khác nhau và phải khôi phục máy ảo từ bản chụp (snapshot). Thời gian lưu trong 30 ngày theo quy tắc sau: + Trên hệ thống sẽ snapshot các máy ảo theo cơ chế (Full backup kết hợp Incremental), số lượng bản sao lưu dự phòng trên hệ thống là 3 bản full và các bản Incremental.	07 phiên bản khác nhau.
Lịch sao lưu	Hàng ngày (sau 19h:00) toàn bộ VM (OS+ ứng dụng) sẽ được snapshot	Thời điểm sao lưu: Sau 19:00 PM. Dữ liệu từ tủ đĩa thứ cấp (Second Storage) sẽ được chuyển xuống Tape
Hỗ trợ hệ điều hành	- Windows	- Windows

	- Mac OS - Linux - Unix	- Mac OS - Linux - Unix
Hỗ trợ sao lưu đối với Ứng dụng và Cơ sở Dữ liệu (Sao lưu đối với dữ liệu đang được khai thác sử dụng tại thời điểm sao lưu)	Oracle (DB HotBackup & Archive Log) - Microsoft SQL Server - Microsoft Exchange Server - Microsoft SharePoint - Microsoft Active Directory - IBM DB2 - IBM Lotus Notes - Informix - Sybase - Symantec Enterprise Vault.	Oracle (DB HotBackup & Archive Log) - Microsoft SQL Server - Microsoft Exchange Server - Microsoft SharePoint - Microsoft Active Directory - IBM DB2 - IBM Lotus Notes - Informix - Sybase - Symantec Enterprise Vault
Hỗ trợ Ảo hóa	- VMWare - MS Window Virtualization - Citrix	- VMWare - MS Window Virtualization - Citrix

1.5.11.3. Cam kết từ nhà cung cấp dịch vụ

- Bản quyền dịch vụ hỗ trợ từ hãng
- Cập nhật các bản vá lỗi và nhận dạng tấn công (nếu có trong quá trình vận hành)
- Hỗ trợ xử lý sự cố (nếu có) từ chính hãng trong quá trình vận hành

1.5.11.4. Khả năng xử lý từ nhà cung cấp cung cấp dịch vụ

- Hỗ trợ kỹ thuật qua điện thoại hoặc hỗ trợ nhanh tại chỗ 24hx7ngày/ tuần
- Thời gian đáp ứng (24hx7ngày/ tuần) ≤ 4 giờ
- Giám sát hệ thống theo thời gian thực 24hx7ngày/ tuần
- Gửi cảnh báo các vi phạm ở mức độ nghiêm trọng qua email

1.6. Thuê đường truyền kết nối

1.6.1. Yêu cầu về cơ sở hạ tầng phục vụ của nhà cung cấp dịch vụ

- Hạ tầng trục trong nước:
  - Hệ thống mạng trục (Backbone) cáp quang có tốc độ 100 Gbps theo tiêu chuẩn mạng đô thị Metro Ethernet cho phép nhà cung cấp dịch vụ triển khai các ứng dụng trên nền mạng thế hệ mới NGN (Next Generation Network).
  - Topology mạng: Ring và Hub and Spoke

- Hạ tầng mạng trục trong nước có dự phòng

- Các hướng kết nối đi quốc tế
  - Nhà cung cấp dịch vụ có đường mạng trục kết nối quốc tế: được triển khai theo hai hướng cáp trên bộ và cáp quang biển (mỗi tuyến đều có dự phòng)
  - Kết nối qua các hướng có độ ổn định cao và có dự phòng.
  - Peering trực tiếp với các content Provider như Google, Facebook, Yahoo, Microsoft…
- Hạ tầng kết nối
  - Kết nối IX (VNIX-HN, VNIX-HCM)
  - Kết nối Peering (FPT Telecom, VNPT, VIETTEL, VTC…)
  - Kết nối IIG (Google, Yahoo, Microsoft…)
- Năng lực hạ tầng truyền dẫn
  - Hạ tầng truyền dẫn 100% cáp quang có dự phòng.
  - Năng lực hạ tầng truyền dẫn đường mạng trục trong nước: hướng Bắc – Nam phải có dự phòng và đi theo các hướng vật lý khác nhau.
  - Topology mạng: Ring và Hub and Spoke, đảm bảo dự phòng.
- Yêu cầu năng lực kỹ thuật đối với nhà cung cấp dịch vụ:
  - Triển khai được các ứng dụng mạng WAN và Intranet chuyên nghiệp
  - Cung cấp kênh truyền đa dạng về tốc độ truyền dẫn theo yêu cầu sử dụng thực tế: cung cấp tốc độ 1Mbps đến 100Mbps cho các site đầu cuối và điểm chính là 1Gbps hoặc cao hơn.
- Kết nối vật lý
  - Giao tiếp kết nối loại GBIC/SFP tốc độ 1Gbps đến 10Gbps.

1.6.2. Yêu cầu cam kết chất lượng dịch vụ truyền dẫn

- Độ khả dụng mạng (Services Availability -SA) ≥ 99, 9%
- Tỷ lệ gây lỗi (Error Second Ratio -ESR) là tỉ lệ phần trăm của số giây mà lỗi được phát hiện trên tổng số giây đo được với khoảng cách truyền dẫn tiêu chuẩn là 27.500 km. Tỷ lệ gây lỗi (ESR) ≤ 1%.
- Tỷ lệ gây lỗi nghiêm trọng (Severely Error Second Ratio- SESR) ≤0,1%
- Cam kết về chất lượng đường truyền: 100% dữ liệu gửi qua các kết nối Wan bằng cáp quang được đảm bảo thành công, có thể sử dụng toàn bộ băng thông của đường truyền đã thuê, độ trễ thấp khi gửi và nhận thông tin
- Cam kết thời gian khôi phục sự cố: ≤ 2 giờ với lỗi kĩ thuật và ≤ 4 giờ với sự cố đứt cáp quang.
- Tư vấn, bảo trì hệ thống,khắc phục sự cố về đường kết nối trong vòng 30 phút.

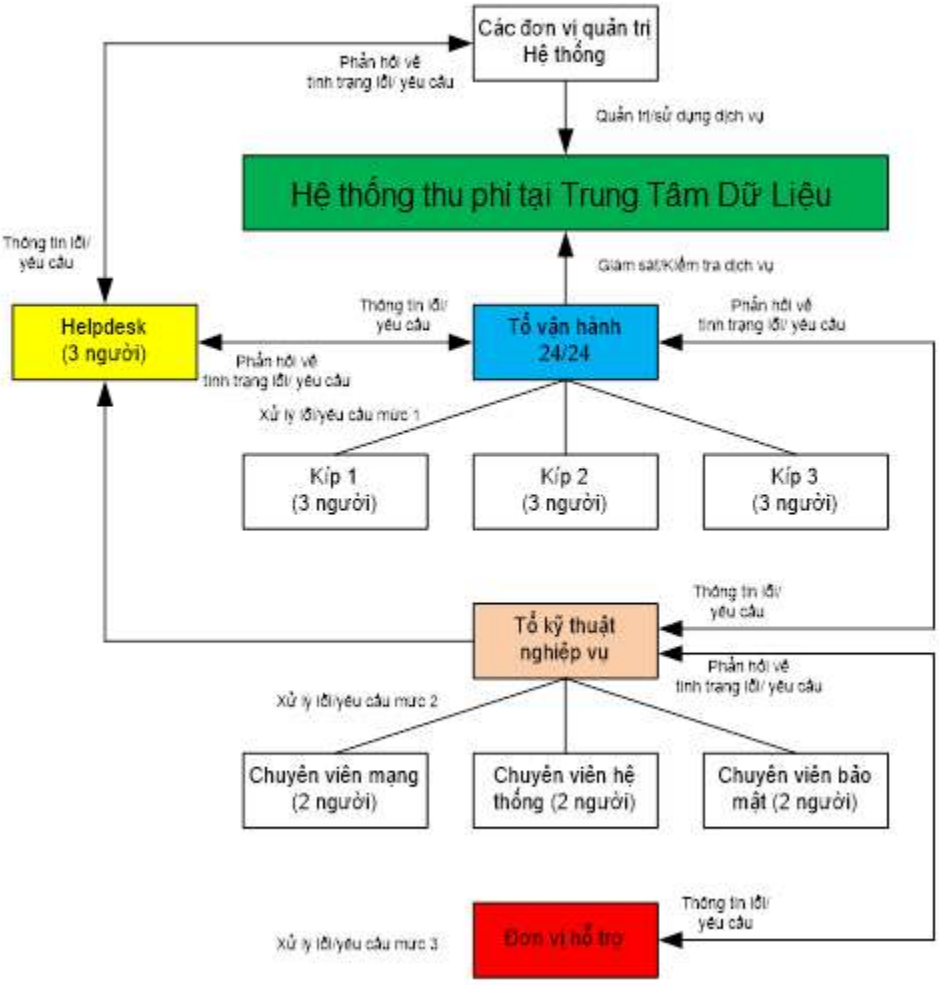
- Hỗ trợ 24h/7 ngày: Khách hàng liên hệ đến số điện thoại của tổng đài chăm sóc khách hàng nhà cung cấp dịch vụ, số điện thoại di động của kĩ thuật viên, số di động của nhân viên trực tiếp làm việc 24/24 khi kí hợp đồng.
- Có quy trình tiếp nhận các yêu cầu và xử lý yêu cầu, xử lý sự cố từ khách hàng sử dụng dịch vụ.

1.7. Phương án, cách thức, điều kiện cung cấp dịch vụ

1.7.1. Quy trình quản trị vận hành và giám sát hệ thống

1.7.1.1. Phạm vi công việc của nhà cung cấp dịch vụ

Sơ đồ và tổ chức nhân sự



Công việc của từng bộ phận

Bộ phận Trực ca của Nhà cung cấp dịch vụ gồm các tổ chức năng như sau:

- **Helpdesk** bố trí 3 người trực Call Center thực hiện công việc:

+ Tiếp nhận thông tin sự cố, yêu cầu từ đơn vị.

+ Chuyển thông tin sự cố, yêu cầu của đơn vị đến Tổ vận hành 24/24 kiểm tra, xử lý.

+ Thu thập thông tin về tình trạng xử lý sự cố.

+ Thông báo/phản hồi với đơn vị về tình trạng xử lý lỗi.

- **Tổ vận hành giám sát 24/24** bố trí 12 người phân làm 4 kíp, các kíp sẽ trực luân phiên theo 3 ca trong ngày. Các công việc thực hiện trong 1 ca trực:

+ Giám sát hệ thống thông qua các công cụ giám sát có bản quyền.

+ Đánh giá dịch vụ bằng việc sử dụng dịch vụ như người dùng: duyệt web, FTP, test gởi nhận email . . .

+ Kiểm tra thông tin lỗi/yêu cầu và đánh giá khả năng khắc phục

+ Xử lý mức 1 thông tin lỗi/yêu cầu

+ Phản hồi tình trạng xử lý thông tin lỗi/yêu cầu mức 1 cho Helpdesk

+ Chuyển thông tin sự cố/ yêu cầu cho Tổ kỹ thuật ngiệp vụ nếu xử lý mức 1 không giải quyết được.

+ Báo cáo tình trạng hoạt động của hệ thống trong ca trực.

- **Tổ kỹ thuật nghiệp vụ** chia làm 3 nhóm thực hiện các công việc:

+ Nhóm chuyên viên mạng:

▪ Kiểm tra, phân tích thông tin lỗi/yêu cầu nhận được từ Tổ vận hành 24/24 và đánh giá khả năng khắc phục

▪ Xử lý mức 2 thông tin lỗi/yêu cầu

▪ Phản hồi tình trạng xử lý thông tin lỗi/yêu cầu mức 2 cho Helpdesk

▪ Chuyển thông tin sự cố/ yêu cầu cho Đơn vị hỗ trợ nếu xử lý mức 2 không giải quyết được.

▪ Báo cáo tình trạng hoạt động của hệ thống mạng định kỳ hằng tuần

+ Nhóm chuyên viên hệ thống

▪ Kiểm tra, phân tích thông tin lỗi/yêu cầu nhận được từ Tổ vận hành 24/24 và đánh giá khả năng khắc phục

▪ Xử lý mức 2 thông tin lỗi/yêu cầu

▪ Phản hồi tình trạng xử lý thông tin lỗi/yêu cầu mức 2 cho Helpdesk

▪ Chuyển thông tin sự cố/ yêu cầu cho Đơn vị hỗ trợ nếu xử lý mức 2 không giải quyết được.

▪ Báo cáo tình trạng hoạt động của hệ thống server định kỳ hằng tuần

+ Nhóm chuyên viên bảo mật

▪ Kiểm tra, phân tích thông tin lỗi/yêu cầu nhận được từ Tổ vận hành 24/24 và đánh giá khả năng khắc phục.

▪ Xử lý mức 2 thông tin lỗi/yêu cầu

- Phản hồi tình trạng xử lý thông tin lỗi/yêu cầu mức 2 cho Helpdesk
- Chuyển thông tin sự cố/ yêu cầu cho Đơn vị hỗ trợ nếu xử lý mức 2 không giải quyết được.
- Báo cáo tình trạng hoạt động của hệ thống bảo mật định kỳ hằng tuần

1.7.1.2. Quy trình xử lý sự cố

Trình tự báo lỗi:

Nhà cung cấp dịch vụ sẽ có một đường dây nóng chuyên dùng cho báo lỗi. Khi có thông tin sự cố hay yêu cầu hỗ trợ, Bộ phận NOC của Nhà cung cấp dịch vụ sẽ tiếp nhận và xử lý trong khoảng thời gian đáp ứng như đã cam kết. Nhà cung cấp dịch vụ đưa ra quá trình ghi nhận cuộc gọi cho phép kiểm soát quá trình xử lý sự cố từ lúc bắt đầu đến lúc kết thúc.

Để tập trung cho công việc, Helpdesk sẽ là bộ phận điều hành trong suốt quá trình. Khi có sự cố liên quan đến hệ thống các đơn vị quản trị sẽ chuyển các yêu cầu cần thiết đến Helpdesk. Chuỗi các hoạt động dịch vụ này được thể hiện theo lược đồ đính kèm. Người trực Helpdesk sẽ nhận cuộc gọi và thi hành các qui trình sau:

Thiết lập cuộc gọi

Việc hỗ trợ sẽ được thực hiện trên đường dây nóng. Người trực Helpdesk sẽ nhận cuộc gọi và ghi nhận vào hệ thống quản lý dịch vụ. Khi đã xác lập cuộc gọi từ Nhà cung cấp dịch vụ xong, thông tin lỗi/yêu cầu sẽ được chuyển tới Tổ vận hành kỹ thuật tiến hành kiểm tra, đánh giá, phân tích và xử lý.

Sử dụng hệ thống quản lý dịch vụ với cơ chế quản lý lỗi theo bậc thang sẽ đảm bảo quá trình bảo trì được thực hiện với chất lượng cao theo các cam kết đã thoả thuận.

Giải quyết yêu cầu

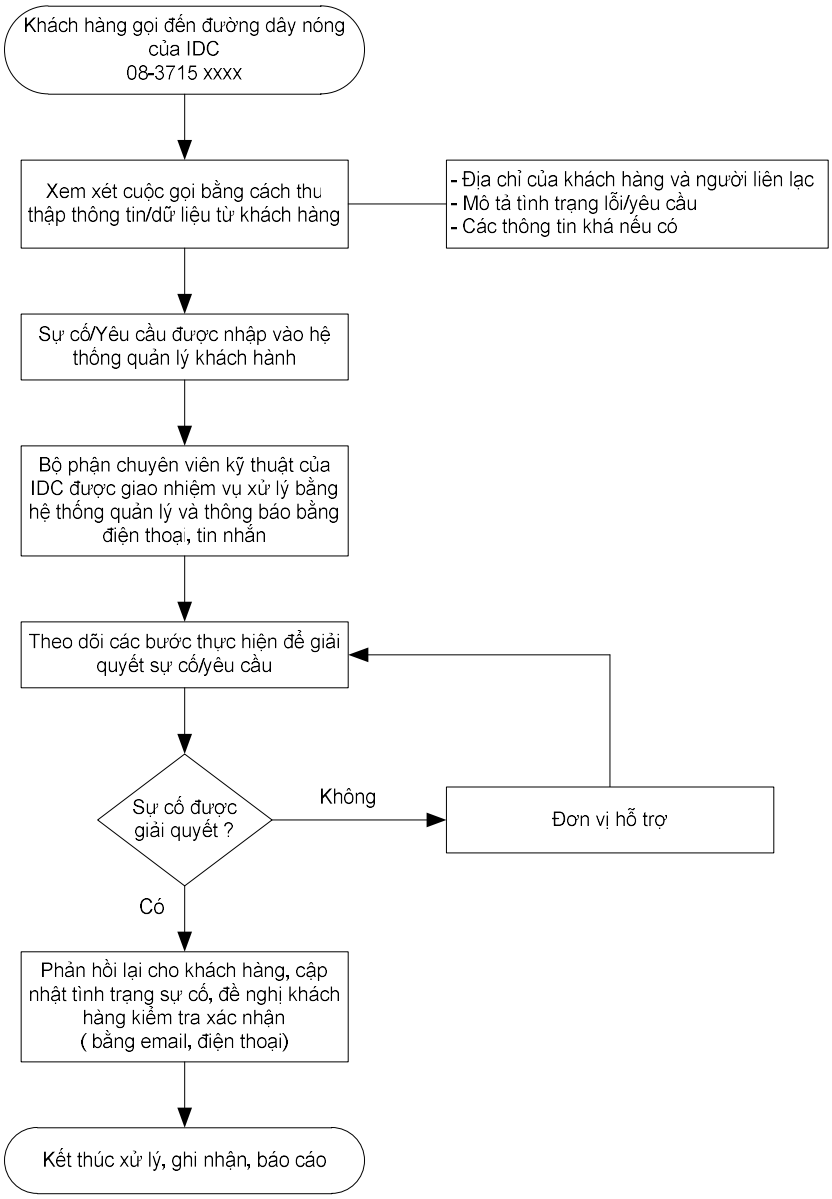
Tổ vận hành kỹ thuật sẽ tiến hành giải quyết yêu cầu theo các qui trình cập nhật đã được lập ra sẵn tại Nhà cung cấp dịch vụ. Các đồ phụ tùng và mức độ liên lạc đến các nhà cung cấp thiết bị có liên quan sẽ được tiến hành nếu thấy cần thiết trong quá trình giải quyết yêu cầu và tất cả sẽ được cập nhật tại Tổ vận hành kỹ thuật.

Trong quá trình xử lý, Tổ vận hành kỹ thuật sẽ cập nhật thường xuyên thông tin tình trạng xử lý lỗi/yêu cầu cho Helpdesk. Sau khi xử lý xong lỗi/yêu cầu Tổ vận hành kỹ thuật sẽ cập nhật quá trình xử lý vào hệ thống quản lý.

Kết thúc hỗ trợ yêu cầu

Khi đã giải quyết xong yêu cầu, Helpdesk sẽ là điểm liên lạc với các đơn vị quản trị để xác nhận và xác nhận kết thúc trường hợp này.

Quy trình xử lý cuộc gọi báo lỗi/yêu cầu chi tiết:



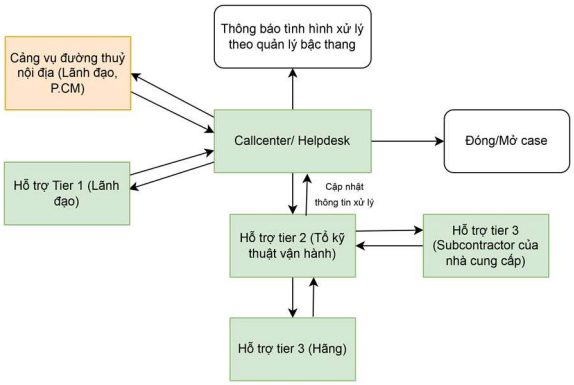
Helpdesk của Nhà cung cấp dịch vụ sẽ tiếp nhận thông tin sự cố thông qua 2 hình thức:

- Công việc giám sát hoạt động của hệ thống 24/24 phát hiện thấy lỗi
- Thông báo qua đường dây nóng, fax, email của các đơn vị quản lý website.
- Khi các đơn vị quản trị liên hệ với Helpdesk của Nhà cung cấp dịch vụ để thông báo sự cố cần cung cấp các thông tin như sau:

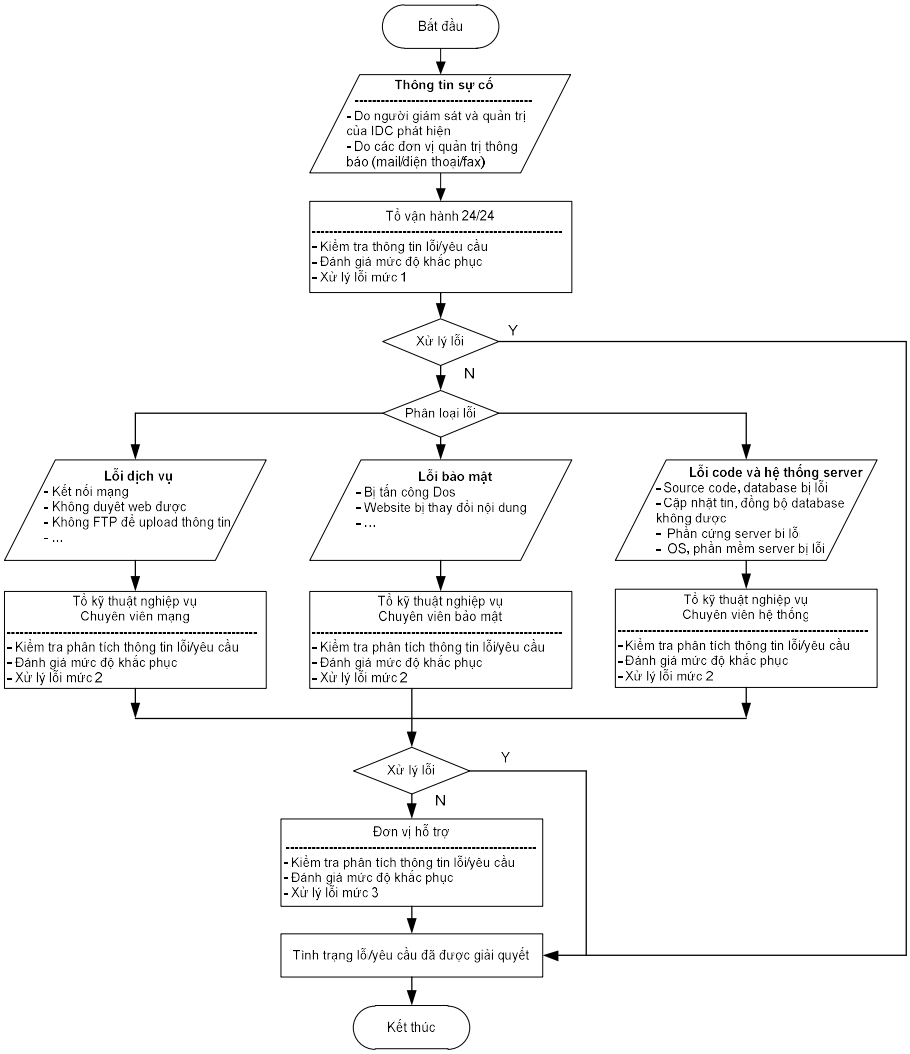
+ Địa chỉ và người liên lạc;
+ Mô tả tình trạng lỗi/yêu cầu;
+ Thời gian xảy ra lỗi;
+ Các thông tin khác nếu có.

Bộ phận Helpdesk sẽ ghi nhận thông tin sự cố/yêu cầu vào mẫu ghi nhận sự cố và nhập nội dung vào trong hệ thống quản lý.

Quá trình tiếp nhận, giải quyết và kết thúc theo mô tả bên trên.



Quy trình xử lý sự cố



Tổ vận hành 24/24 sẽ tiếp nhận thông tin lỗi/yêu cầu từ Helpdesk và tiến hành kiểm tra, đánh giá mức độ, khắc phục và xử lý ở mức 1. Nếu tình trạng lỗi không giải quyết được thì thực hiện phân loại lỗi xãy ra theo nhóm, có 3 nhóm lỗi cơ bản:

- Nhóm 1: Lỗi dịch vụ (kết nối mạng, không duyệt, truy cập web được, không FTP để upload thông tin, …) sẽ được chuyển đến chuyên viên mạng.

- Nhóm 2: Lỗi bảo mật (Bị tấn công bảo mật, website bị thay đổi nội dung, …) sẽ được chuyển đến chuyên viên bảo mật

- Nhóm 3: Lỗi code và hệ thống server (source code, database bị lỗi, cập nhật tin qua trang quản trị và đồng bộ database qua mạng không được, phần cứngserver bị lỗi, OS, phần mềmserver bị lỗi, …) sẽ được chuyển đến chuyên viên hệ thống.

Tổ kỹ thuật nghiệp vụ sẽ tiếp nhận thông tin lỗi/yêu cầu từ Tổ vận hành 24/24 và tiến hành kiểm tra, phân tích, đánh giá mức độ, khắc phục và thực hiện xử lý ở mức 2. Nếu tình trạng lỗi không giải quyết được thì liên hệ với các đơn vị hỗ trợ để tiếp tục xử lý lỗi/yêu cầu ở mức 3 và kết thúc quá trình xử lý.

Thông tin về tình trạng xử lý lỗi sẽ được cập nhật vào hệ thống quản lý và thông báo với Helpdesk.

Quản lý theo bậc thang

Nhà cung cấp dịch vụ có các quy trình theo bậc thang nhằm đảm bảo các sự cố lớn nhanh chóng được cấp báo lần lượt đến các cấp của công ty và Cảng vụ đường thủy nội địa, đảm bảo nhận được sự quan tâm và tài nguyên cần thiết để giải quyết vấn đề nhanh chóng. Nó cũng duy trì liên lạc thường xuyên giữa mọi nhân viên có liên quan trong quy trình.

Thời gian báo cáo trong quy trình theo bậc thang sẽ bắt đầu được tính khi bô phận Helpdesk của Nhà cung cấp dịch vụ nhận được thông báo sự cố. Bộ phận Helpdesk sẽ liên hệ với Tổ vận hành 24/24 của Nhà cung cấp dịch vụ kiểm tra, tìm hiểu và xử lý. Chừng nào trạng thái sự cố còn đó, thì thời gian trong quy trình vẫn tiếp tục tính và sự cố sẽ được báo lên các cấp cao hơn trong công ty. Điều này đảm bảo rằng mỗi sự cố không giải quyết được trong thời gian cụ thể sẽ nhận đuợc sự quan tâm nhiều hơn, và nhiều tài nguyên hơn sẽ được tập trung để giải quyết nó.

- **Phân chia cấp độ ưu tiên:**

- **Ưu tiên cấp 1 (Mức độ khẩn cấp)**

Áp dụng đối với trường hợp hệ thống đang sử dụng hoàn toàn không hoạt động được, hoặc gây ảnh hưởng khẩn cấp/ nguy hiểm tới nội dung thông tin và hoạt động thu phí. Nhà cung cấp dịch vụ và các đơn vị liên quan sẽ sử dụng toàn bộ thời gian để giải quyết sự cố và làm việc 24/24h trong trường hợp này.

- **Ưu tiên cấp 2 (Mức độ quan trọng)**

Áp dụng đối với trường hợp hệ thống bị chập chờn gây ảnh hưởng lớn đến sự hoạt động của hệ thống thu phí. Nhà cung cấp dịch vụ và các đơn vị liên quan sẽ sử dụng toàn bộ thời gian trong giờ hành chính tiêu chuẩn để giải quyết sự cố.

- **Ưu tiên cấp 3 (Mức độ trung bình)**

Áp dụng đối với trường hợp hệ thống thành phố đang sử dụng bị hỏng, hoặc gây ảnh hưởng đến sự hoạt động của hệ thống khác quy định ở ưu tiên cấp 2. Nhà cung cấp

dịch vụ và các đơn vị sẽ giải quyết sự cố trong thời gian hành chính tiêu chuẩn để khôi phục lại hoạt động của hệ thống.

- **Ưu tiên cấp 4 (Mức độ thấp)**

Áp dụng đối với trường hợp các đơn vị yêu cầu cung cấp thông tin hoặc hỗ trợ về lắp đặt, cấu hình hệ thống. Sự cố/vấn đề chỉ ảnh hưởng rất ít hoặc không ảnh hưởng tới hoạt động của hệ thống. Nhà cung cấp dịch vụ và các đơn vị liên quan sẽ làm việc trong giờ hành chính để cung cấp thông tin hoặc các sự hỗ trợ theo yêu cầu.

Phân loại và cấp độ xử lý sự cố

Để quá trình xử lý lỗi/yêu cầu được nhanh chóng, Nhà cung cấp dịch vụ thực hiện phân chia, định nghĩa mức độ, cách xử lý lỗi và bộ phận thực hiện như sau:

Mức độ sự cố	Áp dụng cho trường hợp	Cách xử lý	Mức độ xử lý	Bộ phận thực hiện
Thấp	Lỗi nhẹ là những lỗi không cần phân tích chuyên sâu đến kỹ thuật như: đứt cáp, cổng thiết bị treo/hư, dịch vụ mạng, ứng dụng không hoạt động	- Reset thiết bị mạng, server - Thay thế cáp, thiết bị, server	Mức 1	Tổ vận hành 24/24
Trung bình	Lỗi nặng mà bộ phận xử lý ở mức 1 không giải quyết được. Những lỗi này liên quan đến những vấn đề về kỹ thuật, cấu hình hệ thống, cần người có kinh nghiệm phân tích chuyên sâu.	- Theo tài liệu kỹ thuật vận hành hệ thống. - Theo hướng dẫn của tài liệu kỹ thuật hoặc chuyên gia	Mức 2	Tổ kỹ thuật nghiệp vụ Đơn vị hỗ trợ (SI, Hãng …)
Quan trọng	Lỗi nặng mà bộ phận xử lý ở mức 2 không giải quyết được. Những lỗi này liên quan đến công nghệ, đặc điểm phần mềm và phần cứng của thiết bị.	- Theo cách xử lý của nhà sản xuất. - Thay thế	Mức 3	Tổ kỹ thuật nghiệp vụ Đơn vị hỗ trợ (SI, Hãng …) Lãnh đạo nhà cung cấp dịch vụ
Khẩn cấp	Hệ thống bị tấn công Hệ thống bị hư hỏng, ngưng hoạt động hoàn toàn	Theo kịch bản phòng chống tấn công	Mức 3	Tổ kỹ thuật nghiệp vụ Đơn vị hỗ trợ (SI, Hãng …)

Mức độ sự cố	Áp dụng cho trường hợp	Cách xử lý	Mức độ xử lý	Bộ phận thực hiện
	Hệ thống bị mất nguồn điện	Theo kịch bản đảm bảo kinh doanh liên tục		Lãnh đạo Nhà cung cấp dịch vụ

1.7.1.3. Kế hoạch ứng phó sự cố an toàn thông tin

Việc quản lý sự cố ATTT thực hiện như sau:

a) Phân nhóm sự cố ATTT:

- Sự cố do bị tấn công mạng: tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; tấn công truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; tấn công phá hoại thông tin, dữ liệu, phần mềm; tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu;...

- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

- Sự cố do lỗi của cán bộ quản trị, vận hành hệ thống.

- Sự cố do các thảm họa tự nhiên.

b) Phân loại mức độ nghiêm trọng sự cố

- Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan.

- Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của cơ quan.

- Cao: Sự cố tác động đến khả năng vận hành của HTTT, ảnh hưởng đến dữ liệu, thiết bị, gây ảnh hưởng đến hoạt động chung của cơ quan và hoạt động cung cấp dịch vụ công cho người dân, doanh nghiệp.

- Nghiêm trọng: Sự cố gây gián đoạn hoặc đình trệ hệ thống trong một khoảng thời gian ngắn, ảnh hưởng nghiêm trọng đến dữ liệu, thiết bị của hệ thống, gây thiệt hại nghiêm trọng cho cơ quan, người dân, doanh nghiệp.

- Đặc biệt nghiêm trọng: Sự cố làm tê liệt toàn bộ hoạt động của hệ thống, gây thiệt hại đặc biệt nghiêm trọng cho cơ quan, người dân, doanh nghiệp, đe dọa trật tự an toàn xã hội.

c) Quy trình ứng cứu xử lý sự cố

- Bước 1: Tiếp nhận sự cố

Chủ quản HTTT, đơn vị vận hành tiếp nhận thông tin, cảnh báo về việc mất ATTT của hệ thống từ các đơn vị chuyên trách ATTT, từ người sử dụng hoặc tự rà soát, phát hiện hệ thống có hiện tượng bất thường, có nguy cơ mất ATTT.

- Bước 2: Xác minh và phân loại sơ bộ sự cố

Đơn vị vận hành tiến hành xác minh, phân loại sơ bộ sự cố; đánh giá tình trạng, mức độ, phạm vi và khả năng xử lý của sự cố.

- Bước 3: Báo cáo thông tin sự cố

+ Trường hợp xác định sự cố nằm trong thẩm quyền, khả năng xử lý, đơn vị vận hành báo cáo lãnh đạo cơ quan chủ quản và thực hiện xử lý theo phương án ứng cứu xử lý sự cố nội bộ đã được phê duyệt hoặc theo hướng dẫn của Đơn vị. Khi hoàn thành xử lý, báo cáo kết quả xử lý sự cố (theo Mẫu) về Đơn vị để theo dõi, tổng hợp;

- Trường hợp xác định sự cố có mức độ cao, vượt ngoài thẩm quyền, khả năng xử lý, đơn vị vận hành lập tức báo cáo lãnh đạo cơ quan chủ quản và thông báo (qua điện thoại, email,...) đầu mối tiếp nhận sự cố của Đơn vịđể kịp thời phối hợp với Đội ứng cứu sự cố và các đơn vị chuyên trách ATTT. Ngay trong ngày xảy ra sự cố, đơn vị vận hành thực hiện báo cáo ban đầu sự cố ATTT (theo Mẫu) và gửi về Đơn vị. Đơn vị vận hành có trách nhiệm phối hợp, hỗ trợ Đội ứng cứu sự cố thực hiện các bước ứng cứu xử lý sự cố tiếp theo.

- Bước 4: Cách ly

Đội ứng cứu sự cố cách ly máy chủ, thiết bị, phân vùng bị sự cố ra khỏi môi trường mạng nhằm ngăn chặn khả năng lây lan của sự cố sang những máy chủ, thiết bị, phân vùng khác.

- Bước 5: Thu thập thông tin sự cố

Đội ứng cứu sự cố thu thập thông tin, phục vụ phân tích sự cố, bao gồm: Thông tin về đầu mối liên hệ; thông tin hệ thống; thông tin chức năng của hệ thống; thông tin cấu hình của hệ thống (hệ điều hành, dịch vụ, phiên bản, cấu trúc mạng...); thu thập chứng cứ, thông tin bộ nhớ, trạng thái mạng và các kết nối; tiến trình đang chạy, ổ cứng (trong và ngoại vi); thu thập logfile...

- Bước 6: Phân tích sự cố

Đội ứng cứu sự cố tiến hành phân tích sự cố, bao gồm các thông tin sau: Phân tích dòng thời gian; thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi; thời gian thực hiện các cập nhật lớn đối với hệ thống; thời điểm mà hệ thống sử dụng lần cuối cùng; phân tích dữ liệu; kiểm tra sự thay đổi cấu hình; kiểm tra hệ thống tập tin có bị mã độc; kiểm tra tập tin lịch sử Internet (Internet History) và các tập tin lịch sử khác; kiểm tra Registry và tiến trình; quan sát các tập tin, tiến trình lúc khởi động; phân tích logfile...

- Bước 7: Xử lý sự cố

Đội ứng cứu sự cố xây dựng phương án xử lý sự cố, báo cáo xin ý kiến lãnh đạo Đơn vị, chủ quản HTTT về phương án xử lý sự cố; tiến hành xử lý sự cố, bao gồm các bước: Gỡ bỏ sự cố; xác định và gỡ bỏ các backdoors; phân tích và kiểm tra lỗ hổng sau khi

thực hiện các bản vá lỗi; khôi phục dữ liệu; thu thập các tập tin, hình ảnh, email,... bị xóa, thời gian bị xóa; tìm kiếm và khôi phục các tập tin phù hợp,... để khôi phục HTTT hoạt động bình thường trở lại.

- Bước 8: Tổng hợp, báo cáo

Đội ứng cứu sự cố và đơn vị vận hành hệ thống tiến hành tổng hợp kết quả phân tích và xử lý sự cố, báo cáo với lãnh đạo Đơn vịvà chủ quản HTTT để tổ chức họp phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp phòng ngừa xảy ra sự cố tương tự. Chủ quản HTTT gửi báo cáo hoàn thành xử lý sự cố ATTT (theo Mẫu số 04) về Đơn vị tổng hợp.

- Bước 9: Lưu hồ sơ

Các cơ quan, đơn vị tham gia ứng cứu sự cố lưu toàn bộ các hồ sơ trong quá trình xử lý sự cố để phục vụ các hoạt động quản lý và theo dõi định kỳ. Hồ sơ lưu trữ gồm: Báo cáo ban đầu sự cố; kế hoạch xử lý sự cố, hồ sơ xử lý sự cố, báo cáo phân tích kết quả điều tra xử lý sự cố, báo cáo hoàn thành xử lý sự cố.

d) Kế hoạch ứng cứu sự cố

Đơn vị đã xây dựng các kịch bản ứng cứu, khắc phục các sự cố tấn công mạng phổ biến như sự cố tấn công thay đổi giao diện, sự cố tấn công chiếm quyền máy chủ, sự cố tấn công từ chối dịch vụ,... Đặc biệt tại các thời điểm quan trọng như các ngày lễ, tết, 2/9, 30/4,... có kế hoạch ứng phó sự cố riêng, trong đó thực hiện sao lưu dự phòng đầy đủ các dữ liệu, cấu hình hệ thống để phòng ngừa, khôi phục sau thảm họa.

đ) Diễn tập ứng cứu xử lý sự cố

Đơn vị vận hành hệ thống tổ chức định kỳ các đợt diễn tập ứng cứu sự cố ATTT cho dội ngũ kỹ thuật và cán bộ chuyên trách CNTT của đơn vị; đồng thời tham gia các đợt diễn tập trong nước và quốc tế để nâng cao năng lực.

1.7.1.4. Phối hợp kiểm tra các bản vá lỗi của Hệ điều hành và phần mềm ứng dụng trên máy chủ

- Phối hợp kiểm tra, cập nhật các Patch, fix lỗi, mã nhận dạng virus thường xuyên.

- Kiểm tra, phối hợp cập nhật khi có yêu cầu các thông tin bản vá lỗi mới của các phần mềm ứng dụng và update vào hệ thống. Cụ thể:

+ Đối với hệ thống Web: Kiểm tra, cập nhật các bản update, patch, hotfix của ứng dụng IIS, Tomcat, Apache, …

+ Các ứng dụng cơ sở dữ liệu như: My SQL, MS SQL Server, ….

1.7.1.5. Khắc phục sự cố khi hệ thống phát sinh lỗi, cập nhật tài liệu kỹ thuật, ghi nhận đầy đủ các bước xử lý lỗi

- Phân tích sự cố máy chủ, thiết bị và các ứng dụng nhằm nhận dạng nguyên nhân và xác định các giải pháp khả thi, kiểm tra (test) và thực thi giải pháp xử lý trong thời gian sớm nhất (Theo biên bản báo cáo sự cố đính kèm).

- Hỗ trợ xử lý kỹ thuật, phản hồi thông tin ngay sau khi kiểm tra, xác định lỗi. Đảm bảo giải quyết các yêu cầu của khách hàng về dịch vụ trong thời gian sớm nhất.

- Lập tài liệu các vấn đề, lỗi, sự cố và cách giải quyết để phục vụ cho việc tham khảo trong tương lai.

1.7.1.6. Phạm vi và trách nhiệm

Nhà cung cấp dịch vụ phân chia trách nhiệm các bên tham gia quản trị hệ thống theo mô hình quản lý dịch vụ cloud.

Với yêu cầu dịch vụ, Nhà cung cấp dịch vụ đề xuất chọn mô hình quản lý dịch vụ IaaS (Infrastructure as Service). Nhà cung cấp dịch vụ sẽ chịu trách nhiệm quản lý về hạ tầng: mạng, lưu trữ, server và ảo hoá.

Mô tả một số trách nhiệm khi nhà cung cấp dịch vụ trúng thầu thực hiện:

STT	Yêu cầu phạm vi trách nhiệm
1	Đảm bảo dịch vụ liên tục, ổn định, an toàn đối với dịch vụ cung cấp 24x7x365
2	Đảm bảo tất cả các SLA về dịch vụ cung cấp đã cam kết
3	Giám sát, quản lý và báo cáo các vi phạm SLA, sự cố trên hạ tầng cloud từ mức hệ điều hành máy chủ ảo trở xuống cho khách
4	Chịu trách nhiệm xử lý sự cố dịch vụ liên quan đến tất cả dịch vụ mình cung cấp
5	Đảm bảo cung cấp đủ tài nguyên hệ thống (resource pool) thực theo yêu cầu
6	Thực hiện các yêu cầu khác của bên sử dụng dịch vụ liên quan đến dịch vụ do mình cung cấp
7	Đảm bảo có đội ngũ chuyên gia thực hiện quản trị vận hành, xử lý sự cố các dịch vụ do mình cung cấp

Trong quá trình xử lý các sự cố, nếu sự cố có tính phức tạp khó xử lý và đòi hỏi thời gian gấp thì sự cố sẽ được chuyển lên bộ phận chuyên trách có trình độ chuyên môn cao hơn. Riêng đối với hệ thống tại Nhà cung cấp dịch vụ thì được phân làm 3 mức độ như sau:

Mức độ	Áp dụng cho trường hợp	Cách xử lý	Bộ phận thực hiện
1	Lỗi nhẹ là những lỗi không cần phân tích chuyên sâu đến kỹ thuật như: đứt cáp, cổng thiết bị treo/hư, dịch vụ mạng, ứng dụng không hoạt động	- Reset thiết bị mạng, server - Thay thế cáp, thiết bị, server	Tổ vận hành 24/24.

Mức độ	Áp dụng cho trường hợp	Cách xử lý	Bộ phận thực hiện
2	Lỗi nặng mà bộ phận xử lý ở mức 1 không giải quyết được. Những lỗi này liên quan đến những vấn đề về kỹ thuật, cấu hình hệ thống, cần người có kinh nghiệm phân tích chuyên sâu.	- Theo tài liệu kỹ thuật vận hành hệ thống. - Theo hướng dẫn của tài liệu kỹ thuật hoặc chuyên gia	Tổ kỹ thuật nghiệp vụ. Đơn vị hỗ trợ (SI, Hãng …).
3	Lỗi nặng mà bộ phận xử lý ở mức 2 không giải quyết được. Những lỗi này liên quan đến công nghệ, đặc điểm phần mềm và phần cứng của thiết bị.	- Theo cách xử lý của nhà sản xuất. - Thay thế.	Tổ kỹ thuật nghiệp vụ. Đơn vị hỗ trợ (SI, Hãng …). Lãnh đạo Nhà cung cấp dịch vụ.

Các sự cố sau khi phát hiện và xử lý sẽ được phản hồi và báo cáo Lãnh đạo nhà cung cấp dịch vụ, Cảng vụ đường thủy nội địa và cập nhật hồ sơ tình trạng sự cố theo Biểu đồ quản lý bậc thang.

1.7.2. Các công cụ giám sát và cảnh báo

Nhà cung cấp dịch vụ phải cung cấp cho bên sử dụng dịch vụ giải pháp toàn diện về giám sát dịch vụ và tài nguyên máy chủ ảo trong hệ thống Private Cloud, tuỳ biến quản trị tài nguyên tập trung, hỗ trợ mềm dẻo linh động và nhanh chóng trong việc cấp phát tài nguyên CPU, RAM, LƯU TRỮ cũng như mở rộng tài nguyên trên các máy chủ chạy ứng dụng mà không làm gián đoạn dịch vụ, cụ thể:

Bên sử dụng dịch vụ sẽ quản lý và giám sát các dịch vụ và tài nguyên máy chủ thông qua các portal. Việc giám sát hoạt động của hệ thống máy chủ được thực hiện 24/7/365 bằng các công cụ do nhà cung cấp dịch vụ cung cấp:

- Dashboard giám sát tổng quát tình hình vận hành tại datacenter: network, tổng tài nguyên máy chủ ảo vCPU, RAM, Storage, các dịch vụ vận hành trên máy chủ ảo (up-down),
- Hệ thống cảnh báo tự động qua email, SMS.

1.7.3. Chế độ báo cáo

1.7.3.1. Báo cáo khẩn

- Báo cáo khẩn nhằm thông báo tức thời cho các cấp lãnh đạo của Nhà cung cấp dịch vụ, Cảng vụ đường thủy nội địa thông tin sơ bộ về tình trạng sự cố/ lỗi nghiêm trọng đang xảy ra. Dành cho trường hợp sau:

+ Hệ thống bị mất kết nối không thể khắc phục trong thời gian ngắn.
+ Hệ thống bị lỗi không thể khắc phục trong thời gian ngắn.

+ Hệ thống bị tấn công,

+ Các Server của hệ thống bị lỗi nghiêm trọng.

- Hình thức báo cáo: điện thoại, email đính kèm mẫu báo cáo

- Thời gian báo cáo: **sau 5 phút** khi hệ thống xảy ra sự cố/lỗi nghiêm trọng

- Bộ phận báo cáo: **Tổ vận hành 24/24**

- Nơi nhận báo cáo: Lãnh đạo Nhà cung cấp dịch vụ, Lãnh đạo Cảng vụ đường thủy nội địa.

1.7.3.2. Báo cáo định kỳ

- Báo cáo định kỳ hằng tháng với nội dung tổng hợp ghi nhận lại tình hình hoạt động của hệ thống và đề xuất biện pháp phòng ngừa và cải tiến.

- Hình thức báo cáo: Email đính kèm mẫu báo cáo

- Thời gian báo cáo: Hằng tháng.

- Bộ phận báo cáo: Bộ phận quản trị hệ thống.

- Nơi nhận báo cáo: Lãnh đạo nhà cung cấp dịch vụ, Lãnh đạo Cảng vụ đường thủy nội địa.

1.7.3.3. Các biểu mẫu báo cáo

Chi tiết xem Phụ lục mẫu báo cáo

1.8. Yêu cầu, điều kiện về khả năng kết nối, liên thông với ứng dụng, hệ thống thông tin khác (nếu có)

Hệ thống phải đáp ứng theo yêu cầu tại Thông tư số 13/2017/TT-BTTTT quy định các yêu cầu về kết nối các hệ thống thông tin, cơ sở dữ liệu với cơ sở dữ liệu quốc gia.

Hệ thống thuê tại nhà cung cấp dịch vụ phải đảm bảo khả năng tích hợp, kết nối, thu thập các thông tin, dữ liệu trên hệ thống thông tin ở đơn vị Hải Quan, Ngân hàng.

Đảm bảo thông suốt, chặt chẽ, đồng bộ trên cơ sở kết nối hệ thống thông tin giữa các đơn vị liên quan đến thu nộp phí kết cấu hạ tầng mang lại hiệu quả trong công tác và kiểm soát thu phí cơ sở hạ tầng cảng biển trên địa bàn thành phố Hồ Chí Minh.

Bảo đảm dữ liệu chia sẻ phải có khả năng gửi, nhận, lưu trữ, xử lý được bằng thiết bị số.

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

Các đơn vị sử dụng dịch vụ có quyền sở hữu, tải về phần dữ liệu do chính đơn vị tạo lập trong suốt quá trình sử dụng.

Nhà cung cấp có trách nhiệm bảo mật mọi thông tin về dữ liệu của các đơn vị thuê dịch vụ và không được phép tiết lộ cho bất kỳ bên thứ 3 nào khác ngoại trừ yêu cầu của cơ quan có thẩm quyền của nhà nước.

Các dịch vụ an ninh thông tin phải có khả năng tích hợp tạo thành một hệ thống phòng thủ liên kết chia sẻ thông tin, trao đổi các thông tin phân tích, nhận dạng các mối đe

dọa với nhau, cùng phối hợp tương tác trong thời gian thực, giúp cho việc phát hiện (Detect) nhanh chóng, phản ứng (Respond) kịp thời và bảo vệ ngăn chặn (Protect) các mối đe dọa tấn công vào hệ thống; đồng thời, các sự kiện an toàn thông tin của hệ thống phải được kết nối, chia sẻ về Trung tâm Giám sát an toàn không gian mạng quốc gia theo quy định.

1.10. Yêu cầu về kiểm tra, đánh giá an toàn thông tin

Nhà cung cấp dịch vụ phải có cơ chế đánh giá tổng thể dịch vụ bảo mật an ninh thông tin từ bên thứ ba tối thiểu 1 lần/năm;

Chủ trì thuê dịch vụ có thẩm quyền trực tiếp kiểm tra, đánh giá dịch vụ bảo mật an ninh thông tin được giao nhiệm vụ thuê dịch vụ bằng nguồn lực hiện có hoặc thuê đối tác nhằm đảm bảo độ tin cậy và có chính sách xử lý kịp thời khi có sự cố.

1.11. Yêu cầu khác

1.11.1. Yêu cầu về triển khai, vận hành hệ thống

Yêu cầu về triển khai

Nhà cung cấp dịch vụ phải cung cấp phương án triển khai và thực hiện chuyển đổi dữ liệu cho các máy chủ ảo hoá trong thời gian khởi tạo dịch vụ; phương án trên phải đảm bảo không làm gián đoạn các dịch vụ hoạt động liên tục, an toàn an ninh thông tin và toàn vẹn dữ liệu sau khi chuyển đổi.

Tổ chức triển khai vận hành hệ thống

Đảm bảo triển khai nhanh, hoàn thành đưa vào sử dụng tối đa trong 30 ngày trên hạ tầng sẵn có của nhà cung cấp dịch vụ. Trong đó:

- Thời gian triển khai, chuyển đổi hệ thống và dữ liệu tối đa 25 ngày (kể cả ngày thứ bảy, chủ nhật, nghỉ lễ).

- Thời gian kiểm tra, nghiệm thu, bàn giao dịch vụ công nghệ thông tin để đưa vào sử dụng tối đa 5 ngày (kể cả ngày thứ bảy, chủ nhật, nghỉ lễ).

1.11.2. Yêu cầu về tài liệu

Tài liệu sơ đồ thiết kế hệ thống.

Tài liệu mô tả cấu hình, chính sách được thiết lập trên hệ thống.

Tài liệu mô tả quy trình quản lý vận hành, giám sát, xử lý sự cố.

Tài liệu mô tả báo cáo công tác vận hành định kỳ.

Tài liệu mô tả báo cáo xử lý sự cố.

1.11.3. Yêu cầu về năng lực chuyên môn, kinh nghiệm, điều kiện kỹ thuật của nhà cung cấp dịch vụ

Nhà cung cấp dịch vụ phải đạt cấp độ 3 về an toàn hệ thống thông tin đối với Trung tâm dữ liệu theo tiêu chuẩn quốc gia TCVN 11930:2017;

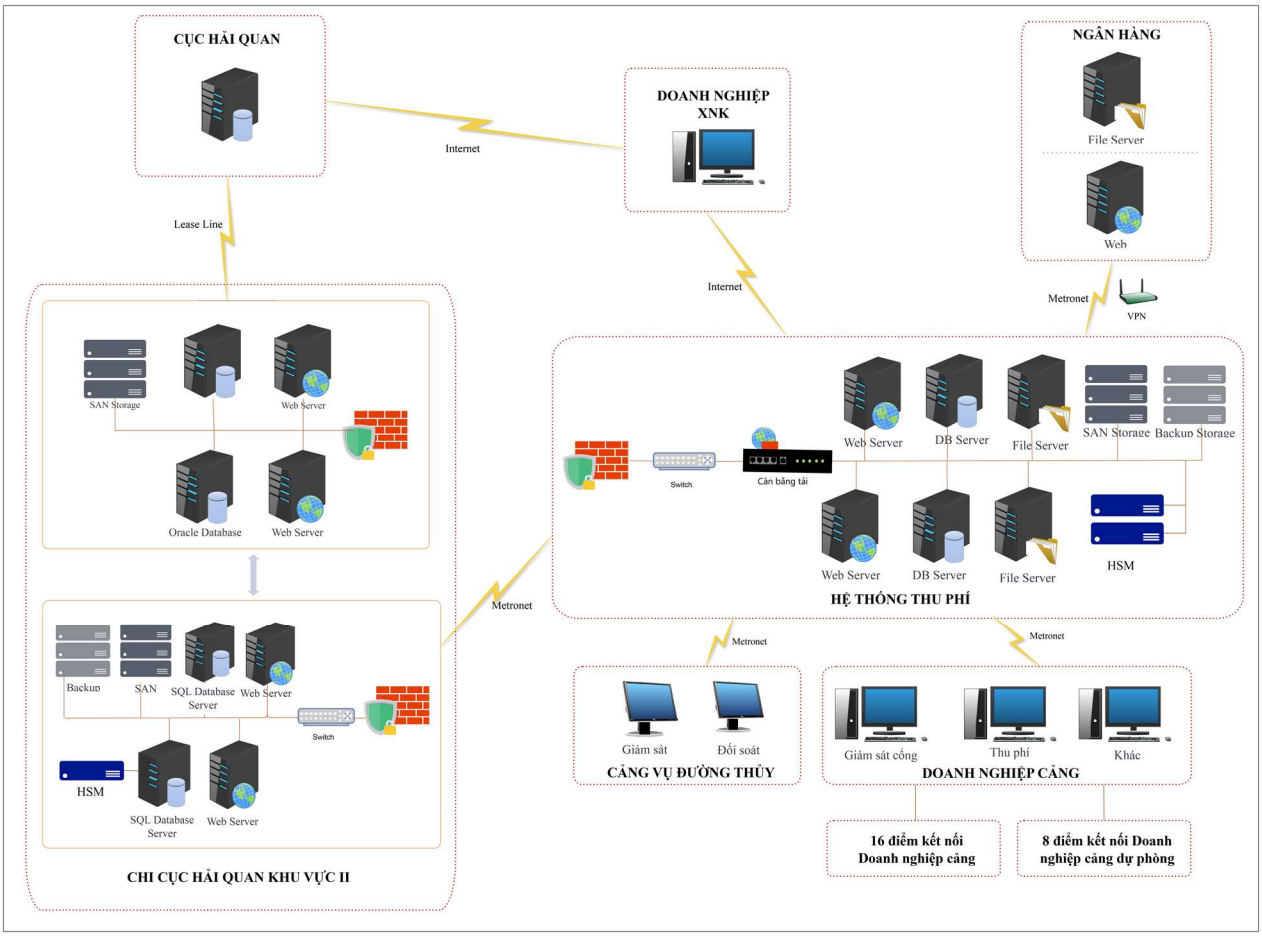
Trung tâm dữ liệu được thiết kế theo tiêu chuẩn đáp ứng mức đảm bảo kỹ thuật: Hạng 3 theo tiêu chuẩn quốc gia TCVN 9250:2021 (hoặc Rate-3 theo tiêu chuẩn ANSI/TIA-942-B:2017), hoặc Tier 3 theo tiêu chuẩn của Uptime Institute.

Nhà cung cấp dịch vụ phải có chứng nhận kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng theo quy định.

Nhà cung cấp dịch vụ có chứng nhận ISO/IEC 27001 về hệ thống quản lý an ninh thông tin.

2. Yêu cầu về giải pháp, kỹ thuật để đáp ứng yêu cầu chất lượng cung cấp dịch vụ

2.1. Mô hình tổng thể



Mô hình thu phí tự động

2.2. Phương án kỹ thuật hạ tầng Công nghệ thông tin, an ninh thông tin phục vụ triển khai hệ thống

Chi tiết tại Phần III: Phương án kỹ thuật hạ tầng Công nghệ thông tin, an ninh thông tin phục vụ triển khai hệ thống

3. Yêu cầu về tuân thủ các yêu cầu về khung kiến trúc

Tuân thủ khung kiến trúc theo Quyết định số 292/QĐ-BKHCN ngày 25/03/2025 của Bộ Thông tin và Truyền thông về ban hành khung kiến trúc chính phủ số việt nam, phiên bản 4.0, hướng tới chính phủ số.

PHẦN 2: XÁC ĐỊNH, LÀM RÕ VIỆC SỞ HỮU CÁC THÔNG TIN, DỮ LIỆU HÌNH THÀNH TRONG QUÁ TRÌNH CUNG CẤP DỊCH VỤ VÀ PHƯƠNG ÁN QUẢN

LÝ, CHUYỂN GIAO CHO BÊN THUÊ

1. Xác định, làm rõ việc sở hữu các thông tin, dữ liệu hình thành trong quá trình cung cấp dịch vụ

- Các đơn vị sử dụng dịch vụ có quyền sở hữu, tải về phần dữ liệu do chính đơn vị tạo lập trong suốt quá trình sử dụng.

- Nhà cung cấp có trách nhiệm bảo mật mọi thông tin về dữ liệu của các đơn vị thuê dịch vụ và không được phép tiết lộ cho bất kỳ bên thứ 3 nào khác ngoại trừ yêu cầu của cơ quan có thẩm quyền của nhà nước.

2. Phân tích quá trình cung cấp dịch vụ và phương án quản lý, chuyển giao cho bên thuê

- Đơn vị thuê dịch vụ có quyền sử dụng dịch vụ đã thuê để phục vụ công việc của đơn vị và có quyền tải về thông tin, dữ liệu do chính đơn vị tạo lập trong thời gian sử dụng dịch vụ.

- Nhà cung cấp dịch vụ có trách nhiệm đảm bảo tính an toàn bảo mật thông tin, dữ liệu do đơn vị thuê dịch vụ tạo lập, đảm bảo hệ thống có thể khôi phục lại dữ liệu khi xảy ra các sự cố ngoại trừ những trường hợp bất khả kháng.

- Nhà cung cấp dịch vụ có trách nhiệm cung cấp công cụ quản lý, giám sát hệ thống dịch vụ cho đơn vị thuê dịch vụ sau khi đã hoàn tất thủ tục cung cấp dịch vụ cho bên thuê.

- Nhà cung cấp dịch vụ có trách nhiệm chuyển giao toàn bộ thông tin, dữ liệu phát sinh cho đơn vị thuê dịch vụ khi hết hạn thuê dịch vụ mà bên thuê không gia hạn sử dụng dịch vụ nữa hoặc khi có yêu cầu bằng văn bản của bên thuê dịch vụ.

PHẦN 3: THỜI GIAN THUÊ VÀ TIẾN ĐỘ, THỜI GIAN XÂY DỰNG, PHÁT TRIỂN, HÌNH THÀNH DỊCH VỤ

1. Thời gian xây dựng, phát triển, hình thành dịch vụ

- Thời gian chuẩn bị cung cấp dịch vụ là 30 ngày (01 tháng).

2. Thời gian thuê

- Thời gian thuê dịch vụ là 60 tháng (Tính từ thời điểm nghiệm thu, bàn giao dịch vụ để đưa vào sử dụng đến khi kết thúc thời gian thuê dịch vụ).

PHẦN II: NỘI DUNG THUÊ DỊCH VỤ CÔNG NGHỆ THÔNG TIN

I NỘI DUNG THUÊ DỊCH VỤ NĂM THỨ 01

1 Thuê hạ tầng công nghệ thông tin trên nền điện toán đám mây phục vụ hệ thống thu phí sử dụng kết cấu hạ tầng, công trình dịch vụ tiện ích công cộng trong khu vực cửa khẩu cảng biển

1.1 Thuê dịch vụ máy chủ ảo trên nền điện toán đám mây dành riêng (private cloud)

STT	Dịch vụ	Đơn vị tính	Khối lượng
1	**Máy chủ Web**	**Máy chủ**	**2**
	Cấu hình: 32 vCore, 128 GB RAM, 1000 GB SSD		
	01 địa chi IP		
	Hệ điều hành Windows phiên bản 2022 trở lên		
	Dịch vụ giám sát máy chủ		
	Kết nối VPN		
2	**Máy chủ Database**	**Máy chủ**	**2**
	Cấu hình: 70 vCore, 512 GB RAM, 10.000 GB SSD		
	01 địa chi IP		
	Hệ điều hành Windows phiên bản 2022 trở lên		
	Bản quyền SQLSvrEntCore 2019 trở lên		
	Dịch vụ giám sát máy chủ		
	Kết nối VPN		
3	**Máy chủ File**	**Máy chủ**	**2**
	Cấu hình: 32vCore, 128 GB RAM, 12.000 GB SSD		
	01 địa chi IP		
	Hệ điều hành Windows phiên bản 2022 trở lên		
	Dịch vụ giám sát máy chủ		
	Kết nối VPN		

1.2 Thuê dịch vụ tăng cường an ninh thông tin

TT	MÔ TẢ DỊCH VỤ	ĐVT	SỐ LƯỢNG
1	Dịch vụ phát hiện và ngăn chặn xâm nhập IPS	máy chủ	6
2	Dịch vụ tường lửa ứng dụng web (WAF)	Dịch vụ	1
3	Dịch vụ cân bằng tải	Dịch vụ	1
4	Dịch vụ tường lửa đa lớp (Internal Firewall + Externam Firewall)	máy chủ	6
5	Dịch vụ phòng chống tấn công Ddos	Dịch vụ	1

6	Dịch vụ dịch vụ Phát hiện, cảnh báo sớm các vấn đề nguy cơ liên quan đến an toàn thông tin	máy chủ	6
7	Dịch vụ phòng chống phần mềm độc hại trên môi trường mạng	máy chủ	6
8	Dịch vụ phòng chống mã độc trên máy chủ	máy chủ	6
9	Dịch vụ phòng chống thất thoát dữ liệu	máy chủ	6
10	Dịch vụ giải pháp ký số HSM	Dịch vụ	2
11	Dịch vụ sao lưu và phục hồi dữ liệu		
	Disk to disk	GB	46.000
	Disk to tape	GB	46.000

1.3 Thuê đường truyền kết nối

STT	Dịch vụ	Đơn vị tính	Khối lượng
1	Chi phí 'Thuê đường truyền kết nối về hệ thống thu phí tốc độ băng thông 200 Mbps a. Chi cục Hải quan khu vực II - Hệ thống thu phí b. Đơn vị thu phí (Cảng vụ đường thủy nội địa - Hệ thống thu phí)	Đường truyền	2
2	Thuê đường truyền kết nối Doanh nghiệp thu phí về hệ thống thu phí, tốc độ băng thông 50Mbps	Đường truyền	16

1.4 Dịch vụ thuê thiết bị tại Chi cục Hải quan khu vực II

STT	Mô tả sản phẩm	Số lượng	ĐVT
1	**Dich vu cho hệ thống may chủ**		
1.1	**Máy chủ web**	**2**	**Bộ**
	Intel Xeon : CPU>= 2.1GHz 20-core	1	
	RAM >= 32GB (1x32GB)	8	
	Ổ cứng >= 480GB SATA 6G Read Intensive SFF	2	
	Card HBA >= 16Gb Dual Port Fibre Channel Host Bus Adapter	1	
	Card mạng >= 10Gb 2-port SFP+ SR Transceiver	1	
	Hot Plug Power Supply Kit	2	
	Win Server Std Core 16 SL	1	
	Microsoft Windows Server 5 Users CAL	1	
	Phần mềm Antivirus	1	
1.2	**Máy chủ DB**	**2**	**Bộ**
	Intel Xeon : CPU>= 2.1GHz 20-core	1	

STT	Mô tả sản phẩm	Số lượng	ĐVT
	RAM >= 32GB (1x32GB)	8	
	Ổ cứng >= 480GB SATA 6G Read Intensive SFF	2	
	Card HBA >= 16Gb Dual Port Fibre Channel Host Bus Adapter	1	
	Card mạng >= 10Gb 2-port SFP+ SR Transceiver	1	
	Hot Plug Power Supply Kit	2	
	Win Server Std Core 16 SL	1	
	Microsoft Windows Server 5 Users CAL	1	
	Phần mềm Antivirus	1	
	SQL Server 2019 Standard Edition	1	
	SQL Server 2019 Standard - 1 User CAL	1	
2	**Hệ thống lưu trữ**	**1**	**Bộ**
	Dual Controller Configure-to-order Base Array	1	
	Storage 2x16Gb Fibre Channel 2-port FIO Adapter Kit	1	
	1,44TB FIO Cache Bundle	2	
	2x16Gb FC 2p Adptr Supp	1	
	1.8m Universal FIO Power Cord	2	
	Storage: 21TB SAS 12G HDD Bundle	1	
3	**Hệ thống kết nối lưu trữ**	**2**	**Bộ**
	Cổng kết nối: >= 16Gb 24/8 8-port Short Wave SFP+ Fibre Channel Switch	1	
	2.4m Jumper (IEC320 C13/C14 M/F CEE 22)	1	
	HPE Premier Flex LC/LC Multi-mode OM4 2 fiber 15m Cable	8	
4	**Thiết bị tường lửa**	**2**	**Bộ**
	- Firewall throughput: 47,000 Mbps		
	- Firewall IMIX: 23,500 Mbps		
	- Firewall Latency (64 byte UDP): 4 µs		
	- IPS throughput: 10,500 Mbps		
	- Threat Protection throughput: 7,400 Mbps		
	- NGFW: 9,000 Mbps		
	- Concurrent connections : 12,260,000		
	- New connections/sec : 186,500		
	- IPsec VPN throughput: 25,000 Mbps		
	- IPsec VPN concurrent tunnels: 6,500		
	- SSL VPN concurrent tunnels: 5,000		
	Xstream SSL/TLS Inspection : 2,470 Mbps		
	- Xstream SSL/TLS Concurrent connections : 55,296		
	- Hard drive for local quarantine and logs:Integrated min. 240 GB SATA-III SSD		

STT	Mô tả sản phẩm	Số lượng	ĐVT
	Physical interfaces		
	- Ethernet interfaces (fixed): 8 x GE copper, 2 x SFP fiber* 2 x SFP+ 10 GbE fiber*		
	- Number of Flexi Port slots : 1		
	EnterpriseGuard Subscription Includes: - Base License: Networking, wireless, Xstream Architecture, unlimited remote access VPN, site-to-site VPN, reporting - Network Protection: Xstream TLS and DPI engine, IPS, ATP, Security Heartbeat, manage SD-RED, reporting - Web Protection: : Xstream TLS and DPI engine, Web Security and Control, Application Control, reporting - Enhanced Support: 24/7 support, feature updates, advanced replacement hardware warranty for term		
5	**Thiết bị mạng**	**2**	**Bộ**
	24G 4SFP+ 1-slot HI Switch	1	
	10G SFP+ to SFP+ 0.65m Direct Attach Copper Cable	1	
	10G SFP+ to SFP+ 3m Direct Attach Copper Cable	3	
	150W 100-240VAC to 12VDC Power Supply	2	
	150W 100-240VAC to 12VDC Power Supply PDU ROW	2	
	Networking Comware Module 4-port 1/10G SFP+	1	
6	**Thiết bị sao lưu dữ liệu**	**1**	**Bộ**
	- 24TB Raw Capacity - Hỗ trợ RAID 6 -10/25Gb 2-port SFP Adapter - Transfer rate>= 14 TB/hour - Bảo hành chính hãng. - Nhà sản xuất có trung tâm bảo hành chính hãng tại ViệtNam	1	
7	**Thiết bị ký số HSM**	**1**	**Bộ**

STT	Mô tả sản phẩm	Số lượng	ĐVT
	Cho phép người dùng lựa chọn lưu trữ khoá/chứng thư số bên ở bên trong thiết bị hoặc bên ngoài hệ thống dưới dạng file mã hoá. Không giới hạn số lượng slots/ partitions Không giới hạn số lượng kết nối. Có thể sử dụng HSM cho nhiều server ứng dụng khác nhau. Đáp ứng tối thiểu tốc độ ký là 16tps (với độ dài khoá 2048 bit) có khả năng xử lý được đến 57,600 giao dịch trong vòng 01 giờ	1	
8	**Dịch vụ giám sát vận hành 24/7 hệ thống máy hải quan**	**1**	**DV**
9	**Dịch vụ triển khai cài đặt và đào tạo**	**1**	**DV**

II NỘI DUNG THUÊ DỊCH VỤ NĂM THỨ 02

1 Thuê hạ tầng công nghệ thông tin trên nền điện toán đám mây phục vụ hệ thống thu phí sử dụng kết cấu hạ tầng, công trình dịch vụ tiện ích công cộng trong khu vực cửa khẩu cảng biển

1.1 Thuê dịch vụ máy chủ ảo trên nền điện toán đám mây dành riêng (private cloud)

1.1.1 Thuê máy chủ ảo phục vụ hệ thống thu phí

Tương tự Khoản 1.1 Mục 1 Phần I: Nội dung thuê dịch vụ năm thứ 01

1.1.2 Thuê tài nguyên tăng trưởng hàng năm

STT	Tên dịch vụ	Đơn vị	Số Lượng
1	Bổ sung năng lực xử lý vCPU	vCPU	16
2	Bổ sung dung lượng RAM	GB	32
3	Bổ sung dung lượng lưu trữ SSD	GB	4.000
	Tổng cộng chưa bao gồm thuế		

1.2 Thuê dịch vụ tăng cường an ninh thông tin

TT	MÔ TẢ DỊCH VỤ	ĐVT	SỐ LƯỢNG
1	Dịch vụ phát hiện và ngăn chặn xâm nhập IPS	máy chủ	6
2	Dịch vụ tường lửa ứng dụng web (WAF)	Dịch vụ	1
3	Dịch vụ cân bằng tải	Dịch vụ	1
4	Dịch vụ tường lửa đa lớp (Internal Firewall + Externam Firewall)	máy chủ	6

5	Dịch vụ phòng chống tấn công Ddos	Dịch vụ	1
6	Dịch vụ dịch vụ Phát hiện, cảnh báo sớm các vấn đề nguy cơ liên quan đến an toàn thông tin	máy chủ	6
7	Dịch vụ phòng chống phần mềm độc hại trên môi trường mạng	máy chủ	6
8	Dịch vụ phòng chống mã độc trên máy chủ	máy chủ	6
9	Dịch vụ phòng chống thất thoát dữ liệu	máy chủ	6
10	Dịch vụ giải pháp ký số HSM	Dịch vụ	2
11	Dịch vụ sao lưu và phục hồi dữ liệu		
	Disk to disk	GB	50.000
	Disk to tape	GB	50.000

1.3 Thuê đường truyền kết nối

Tương tự Khoản 1.3 Mục 1 Phần I: Nội dung thuê dịch vụ năm thứ 01

1.4 Dịch vụ thuê thiết bị tại Chi cục Hải quan khu vực II

STT	Mô tả sản phẩm	Số lượng	ĐVT
1	**Dịch vụ cho hệ thống máy chủ**		
1.1	**Máy chủ web**	**2**	**Bộ**
	Intel Xeon : CPU>= 2.1GHz 20-core	1	
	RAM >= 32GB (1x32GB)	8	
	Ổ cứng >= 480GB SATA 6G Read Intensive SFF	2	
	Card HBA >= 16Gb Dual Port Fibre Channel Host Bus Adapter	1	
	Card mạng >= 10Gb 2-port SFP+ SR Transceiver	1	
	Hot Plug Power Supply Kit	2	
	Win Server Std Core 16 SL	1	
	Microsoft Windows Server 5 Users CAL	1	
	Phần mềm Antivirus	1	
1.2	**Máy chủ DB**	**2**	**Bộ**
	Intel Xeon : CPU>= 2.1GHz 20-core	1	
	RAM >= 32GB (1x32GB)	8	
	Ổ cứng >= 480GB SATA 6G Read Intensive SFF	2	
	Card HBA >= 16Gb Dual Port Fibre Channel Host Bus Adapter	1	
	Card mạng >= 10Gb 2-port SFP+ SR Transceiver	1	
	Hot Plug Power Supply Kit	2	
	Win Server Std Core 16 SL	1	
	Microsoft Windows Server 5 Users CAL	1	
	Phần mềm Antivirus	1	
	SQL Server 2019 Standard Edition	1	
	SQL Server 2019 Standard - 1 User CAL	1	

STT	Mô tả sản phẩm	Số lượng	ĐVT
2	**Hệ thống lưu trữ**	**1**	**Bộ**
	Dual Controller Configure-to-order Base Array	1	
	Storage 2x16Gb Fibre Channel 2-port FIO Adapter Kit	1	
	1,44TB FIO Cache Bundle	2	
	2x16Gb FC 2p Adptr Supp	1	
	1.8m Universal FIO Power Cord	2	
	Storage: 21TB SAS 12G HDD Bundle	1	
3	**Hệ thống kết nối lưu trữ**	**2**	**Bộ**
	Cổng kết nối: >= 16Gb 24/8 8-port Short Wave SFP+ Fibre Channel Switch	1	
	2.4m Jumper (IEC320 C13/C14 M/F CEE 22)	1	
	HPE Premier Flex LC/LC Multi-mode OM4 2 fiber 15m Cable	8	
4	**Thiết bị tường lửa**	**2**	**Bộ**
	- Firewall throughput: 47,000 Mbps		
	- Firewall IMIX: 23,500 Mbps		
	- Firewall Latency (64 byte UDP): 4 µs		
	- IPS throughput: 10,500 Mbps		
	- Threat Protection throughput: 7,400 Mbps		
	- NGFW: 9,000 Mbps		
	- Concurrent connections : 12,260,000		
	- New connections/sec : 186,500		
	- IPsec VPN throughput: 25,000 Mbps		
	- IPsec VPN concurrent tunnels: 6,500		
	- SSL VPN concurrent tunnels: 5,000		
	Xstream SSL/TLS Inspection : 2,470 Mbps		
	- Xstream SSL/TLS Concurrent connections : 55,296		
	- Hard drive for local quarantine and logs:Integrated min. 240 GB SATA-III SSD		
	Physical interfaces		
	- Ethernet interfaces (fixed): 8 x GE copper, 2 x SFP fiber* 2 x SFP+ 10 GbE fiber*		
	- Number of Flexi Port slots : 1		

STT	Mô tả sản phẩm	Số lượng	ĐVT
	EnterpriseGuard Subscription Includes: - Base License: Networking, wireless, Xstream Architecture, unlimited remote access VPN, site-to-site VPN, reporting - Network Protection: Xstream TLS and DPI engine, IPS, ATP, Security Heartbeat, manage SD-RED, reporting - Web Protection: : Xstream TLS and DPI engine, Web Security and Control, Application Control, reporting - Enhanced Support: 24/7 support, feature updates, advanced replacement hardware warranty for term		
5	**Thiết bị mạng**	**2**	**Bộ**
	24G 4SFP+ 1-slot HI Switch	1	
	10G SFP+ to SFP+ 0.65m Direct Attach Copper Cable	1	
	10G SFP+ to SFP+ 3m Direct Attach Copper Cable	3	
	150W 100-240VAC to 12VDC Power Supply	2	
	150W 100-240VAC to 12VDC Power Supply PDU ROW	2	
	Networking Comware Module 4-port 1/10G SFP+	1	
6	**Thiết bị sao lưu dữ liệu**	**1**	**Bộ**
	- 24TB Raw Capacity - Hỗ trợ RAID 6 -10/25Gb 2-port SFP Adapter - Transfer rate>= 14 TB/hour - Bảo hành chính hãng. - Nhà sản xuất có trung tâm bảo hành chính hãng tại ViệtNam	1	
7	**Thiết bị ký số HSM**	**1**	**Bộ**
	Cho phép người dùng lựa chọn lưu trữ khoá/chứng thư số bên ở bên trong thiết bị hoặc bên ngoài hệ thống dưới dạng file mã hoá. Không giới hạn số lượng slots/ partitions Không giới hạn số lượng kết nối. Có thể sử dụng HSM cho nhiều server ứng dụng khác nhau. Đáp ứng tối thiểu tốc độ ký là 16tps (với độ dài khoá 2048 bit) có khả năng xử lý được đến 57,600 giao dịch trong vòng 01 giờ	1	

STT	Mô tả sản phẩm	Số lượng	ĐVT
8	**Dịch vụ giám sát vận hành 24/7 hệ thống máy hải quan**	**1**	**DV**

III NỘI DUNG THUÊ DỊCH VỤ NĂM THỨ 03

1 Thuê hạ tầng công nghệ thông tin trên nền điện toán đám mây phục vụ hệ thống thu phí sử dụng kết cấu hạ tầng, công trình dịch vụ tiện ích công cộng trong khu vực cửa khẩu cảng biển

1.1 Thuê dịch vụ máy chủ ảo trên nền điện toán đám mây dành riêng (private cloud)

1.1.1 Thuê máy chủ ảo phục vụ hệ thống thu phí

Tương tự Khoản 1.1 Mục 1 Phần I: Nội dung thuê dịch vụ năm thứ 01

1.1.2 Thuê tài nguyên tăng trưởng hàng năm

STT	Tên dịch vụ	Đơn vị	Số Lượng
1	Bổ sung năng lực xử lý vCPU	vCPU	32
2	Bổ sung dung lượng RAM	GB	64
3	Bổ sung dung lượng lưu trữ SSD	GB	8.000

1.2 Thuê dịch vụ tăng cường an ninh thông tin

TT	MÔ TẢ DỊCH VỤ	ĐVT	SỐ LƯỢNG
1	Dịch vụ phát hiện và ngăn chặn xâm nhập IPS	máy chủ	6
2	Dịch vụ tường lửa ứng dụng web (WAF)	Dịch vụ	1
3	Dịch vụ cân bằng tải	Dịch vụ	1
4	Dịch vụ tường lửa đa lớp (Internal Firewall + Externam Firewall)	máy chủ	6
5	Dịch vụ phòng chống tấn công Ddos	Dịch vụ	1
6	Dịch vụ dịch vụ Phát hiện, cảnh báo sớm các vấn đề nguy cơ liên quan đến an toàn thông tin	máy chủ	6
7	Dịch vụ phòng chống phần mềm độc hại trên môi trường mạng	máy chủ	6
8	Dịch vụ phòng chống mã độc trên máy chủ	máy chủ	6
9	Dịch vụ phòng chống thất thoát dữ liệu	máy chủ	6
10	Dịch vụ giải pháp ký số HSM	Dịch vụ	2
11	Dịch vụ sao lưu và phục hồi dữ liệu		
	Disk to disk	GB	54.000
	Disk to tape	GB	54.000

1.3 Thuê đường truyền kết nối

IV Tương tự Khoản 1.3 Mục 1 Phần I: Nội dung thuê dịch vụ năm thứ 01

1.1 Dịch vụ thuê thiết bị tại Chi cục Hải quan khu vực II

Tương tự Khoản 1.4 Mục 1 Phần II: Nội dung thuê dịch vụ năm thứ 02

V NỘI DUNG THUÊ DỊCH VỤ NĂM THỨ 04

1 Thuê hạ tầng công nghệ thông tin trên nền điện toán đám mây phục vụ hệ thống thu phí sử dụng kết cấu hạ tầng, công trình dịch vụ tiện ích công cộng trong khu vực cửa khẩu cảng biển

1.1 Thuê dịch vụ máy chủ ảo trên nền điện toán đám mây dành riêng (private cloud)

1.1.1 Thuê máy chủ ảo phục vụ hệ thống thu phí

Tương tự Khoản 1.1 Mục 1 Phần I: Nội dung thuê dịch vụ năm thứ 01

1.1.2 Thuê tài nguyên tăng trưởng hàng năm

STT	Tên dịch vụ	Đơn vị	Số Lượng
1	Bổ sung năng lực xử lý vCPU	vCPU	48
2	Bổ sung dung lượng RAM	GB	96
3	Bổ sung dung lượng lưu trữ SSD	GB	12.000

1.2 Thuê dịch vụ tăng cường an ninh thông tin

TT	MÔ TẢ DỊCH VỤ	ĐVT	SỐ LƯỢNG
1	Dịch vụ phát hiện và ngăn chặn xâm nhập IPS	máy chủ	6
2	Dịch vụ tường lửa ứng dụng web (WAF)	Dịch vụ	1
3	Dịch vụ cân bằng tải	Dịch vụ	1
4	Dịch vụ tường lửa đa lớp (Internal Firewall + Externam Firewall)	máy chủ	6
5	Dịch vụ phòng chống tấn công Ddos	Dịch vụ	1
6	Dịch vụ dịch vụ Phát hiện, cảnh báo sớm các vấn đề nguy cơ liên quan đến an toàn thông tin	máy chủ	6
7	Dịch vụ phòng chống phần mềm độc hại trên môi trường mạng	máy chủ	6
8	Dịch vụ phòng chống mã độc trên máy chủ	máy chủ	6
9	Dịch vụ phòng chống thất thoát dữ liệu	máy chủ	6
10	Dịch vụ giải pháp ký số HSM	Dịch vụ	2
11	Dịch vụ sao lưu và phục hồi dữ liệu		
	Disk to disk	GB	58.000
	Disk to tape	GB	58.000

1.3 Thuê đường truyền kết nối

Tương tự Khoản 1.3 Mục 1 Phần II: Nội dung thuê dịch vụ năm thứ 02

1.4 Dịch vụ thuê thiết bị tại Chi cục Hải quan khu vực II

Tương tự Khoản 1.4 Mục 1 Phần II: Nội dung thuê dịch vụ năm thứ 02

VI NỘI DUNG THUÊ DỊCH VỤ NĂM THỨ 05

1 Thuê hạ tầng công nghệ thông tin trên nền điện toán đám mây phục vụ hệ thống thu phí sử dụng kết cấu hạ tầng, công trình dịch vụ tiện ích công cộng trong khu vực cửa khẩu cảng biển.

1.1 Thuê dịch vụ máy chủ ảo trên nền điện toán đám mây dành riêng (private cloud)

1.1.1 Thuê máy chủ ảo phục vụ hệ thống thu phí

Tương tự Khoản 1.1 Mục 1 Phần I: Nội dung thuê dịch vụ năm thứ 01

1.1.2 Thuê tài nguyên tăng trưởng hàng năm

STT	Tên dịch vụ	Đơn vị	Số Lượng
1	Bổ sung năng lực xử lý vCPU	vCPU	64
2	Bổ sung dung lượng RAM	GB	128
3	Bổ sung dung lượng lưu trữ SSD	GB	16.000

1.2 Thuê dịch vụ tăng cường an ninh thông tin

TT	MÔ TẢ DỊCH VỤ	ĐVT	SỐ LƯỢNG
1	Dịch vụ phát hiện và ngăn chặn xâm nhập IPS	máy chủ	6
2	Dịch vụ tường lửa ứng dụng web (WAF)	Dịch vụ	1
3	Dịch vụ cân bằng tải	Dịch vụ	1
4	Dịch vụ tường lửa đa lớp (Internal Firewall + Externam Firewall)	máy chủ	6
5	Dịch vụ phòng chống tấn công Ddos	Dịch vụ	1
6	Dịch vụ dịch vụ Phát hiện, cảnh báo sớm các vấn đề nguy cơ liên quan đến an toàn thông tin	máy chủ	6
7	Dịch vụ phòng chống phần mềm độc hại trên môi trường mạng	máy chủ	6
8	Dịch vụ phòng chống mã độc trên máy chủ	máy chủ	6
9	Dịch vụ phòng chống thất thoát dữ liệu	máy chủ	6
10	Dịch vụ giải pháp ký số HSM	Dịch vụ	2
11	Dịch vụ sao lưu và phục hồi dữ liệu		
	Disk to disk	GB	62.000
	Disk to tape	GB	62.000

1.3 Thuê đường truyền kết nối

Tương tự Khoản 1.3 Mục 1 Phần II: Nội dung thuê dịch vụ năm thứ 02

1.4 Dịch vụ thuê thiết bị tại Chi cục Hải quan khu vực II

Tương tự Khoản 1.4 Mục 1 Phần II: Nội dung thuê dịch vụ năm thứ 02.

PHẦN III: YÊU CẦU PHƯƠNG ÁN KỸ THUẬT HẠ TẦNG CÔNG NGHỆ THÔNG TIN, AN NINH THÔNG TIN PHỤC VỤ TRIỂN KHAI HỆ THỐNG

1. Giải pháp cung cấp dịch vụ hạ tầng điện toán đám mây dùng riêng (Virtual Private Cloud)

1.1. Hệ thống ảo hóa máy chủ

Hệ thống máy chủ ảo chạy trên nền tảng ảo hóa và điện toán đám mây, các máy chủ ảo được tổ chức theo mô hình Frontend (chứa ứng dụng web) và máy chủ Backend (chứa cơ sở dữ liệu).

Các ổ cứng trên máy chủ nào là các phân vùng lưu trữ nằm trên hệ thống SAN, có độ ổn định và tính sãn sàng cao. Dễ dàng cho việc mở rộng dung lượng, sao lưu, dự phòng dữ liệu.

Hệ thống mạng được cấu hình sẵn, các máy chủ ảo được triển khai ở vùng mạng Frontend hoặc Backend sẽ được gán IP, chính sách bảo mật, định tuyến và chuyển mạch tương ứng.

Các server vật lý cung cấp hạ tầng cloud được cấu hình theo kiểu cluster tạo thành một khối tài nguyên dùng chung đảm bảo ác tính năng sẵn sàng của hệ thống như HA, vMotion, Fault Tolerance.

Hê thống Software Define Network NSX-T cho phép tạo các dịch vụ mạng và bảo mật riêng cho từng ternant, cung cấp khả năng về Self Service về dịch vụ cơ bản hạ tầng Network và Bảo Mật cho Selfporttal.

Hệ thống HA Vcenter gồm được điều khiển giám sát bởt Witness Vcenter đảm bảo độ khả dụng hạ tầng quản trị ảo hóa dự phòng xuyên suốt.

Hê thống Software Define Network NSX.

Việc quản trị tài nguyên tập trung, hỗ trợ mềm dẻo linh động và nhanh chóng trong việc cấp phát tài nguyên CPU, RAM, HDD cũng như mở rộng tài nguyên trên các máy chủ chạy ứng dụng mà không làm gián đoạn dịch vụ. Đáp ứng kịp thời nhu cầu nâng cấp máy chủ khi cần mở rộng máy chủ cho các ứng dụng có lượng truy nhập lớn.

Mỗi VDC sẽ được tổ chức các các máy chủ ứng dụng, các vùng mạng, các lớp thiết bị bảo mật với chính sách ANTT khác nhau với các danh mục dịch vụ (catalog).

Chỉ tiêu kỹ thuật cho cơ sở hạ tầng điện toán đám mây

Theo Công văn 1145/BTTTT-CATTT ngày 03/04/2020, tại Phụ lục 01 hướng dẫn về tiêu chí, chỉ tiêu kỹ thuật tối thiểu cho cơ sở hạ tầng điện toán đám mây, trong đó phần I quy định các tiêu chí về máy ảo phải đáp ứng các tính năng sau đây:

- Tạo máy ảo:

Cho phép tạo máy chủ ảo thông qua giao diện đồ họa (GUI), qua giao diện dòng lệnh (CLI) và giao diện lập trình ứng dụng (API) tích hợp với hệ thống khác.

- Tạo nhiều máy ảo cùng một lúc:

Cho phép người dùng tạo nhiều máy ảo một lúc với số lượng loại hệ điều hành khác nhau.

- Tùy biến máy ảo:

Cho phép người dùng tạo máy ảo từ tệp tin hệ điều hành mà hệ thống hỗ trợ; tùy biến máy ảo muốn tạo và lưu lại máy ảo sau khi tùy biến thành tệp tin hệ điều hành; lưu trữ tệp tin hệ điều hành do người dùng tạo ra trong nhóm tệp tin hệ điều hành tùy biến; sử dụng giao diện cổng thông tin quản trị (web portal) để tạo máy ảo tùy ý.

- Nhập/ xuất máy ảo:

Cho phép người dùng tải lên và tạo máy ảo từ những tệp tin hệ điều hành khác nhau; lưu lại máy ảo đang chạy thành các tệp tin hệ điều hành có định dạng cho phép người dùng tải xuống các tệp tin hệ điều hành.

- Chuyển đổi định dạng tệp tin hệ điều hành:

Yêu cầu này cho phép người dùng chuyển đổi qua lại các định dạng tệp tin hệ điều hành khác nhau cùng một lúc.

- Triển khai máy ảo có cấu hình cao

Hỗ trợ triển khai các máy ảo có số lượng lớn nhân xử lý và có bộ nhớ kích thước lớn mà nặng về bộ nhớ (memory-intensive) hoặc nặng về nhân xử lý (processor-intensive).

- Thay đổi cấu hình phần cứng máy ảo

Cho phép người dùng thay đổi cấu hình phần cứng máy ảo trong khi các máy ảo đang chạy, không yêu cầu đối với trường hợp giảm kích thước ổ cứng.

- Di chuyển máy ảo giữa các máy chủ vật lý

Yêu cầu này cho phép di chuyển dữ liệu của một máy ảo đang chạy từ máy vật lý này sang máy vật lý khác mà không phải tắt hoặc khởi động lại máy ảo.

- Di chuyển dữ liệu máy ảo giữa các bộ lưu trữ khác nhau

Yêu cầu này cho phép di chuyển dữ liệu của một máy ảo đang chạy từ thiết bị lưu trữ này sang thiết bị lưu trữ khác mà không phải tắt hoặc khởi động lại.

- Khôi phục máy ảo sau khi có lỗi xảy ra

Yêu cầu cho phép khôi phục/ khởi động lại tự động máy ảo (khi cơ sở hạ tầng vật lý phát sinh lỗi) phải thỏa mãn 02 điều kiện kèm theo.

- Tính năng phân bổ máy ảo trên các máy vật lý khác nhau (anti-affinity)

Yêu cầu này cho phép người dùng cấu hình các thông số trên máy ảo để xác định vị trí triển khai các máy ảo khác nhau trên các máy vật lý hoặc trung tâm dữ liệu khác nhau (nhằm phòng tránh sự ảnh hưởng của vấn đề nào đó về phần cứng hoặc cơ sở hạ tầng đối với tất cả các máy ảo cùng một lúc).

- Tự động thay đổi cấu hình hệ thống mức cơ bản

Tự động thay đổi theo chiều ngang thông qua 03 cách bao gồm bật/ tắt máy ảo; tạo ra các máy ảo mới dựa theo kế hoạch được lập thủ công trước đó; các tiêu chí sử dụng tài nguyên do người dùng định nghĩa; Cho phép người dùng thiết lập số lượng tối đa máy ảo mới được tạo.

- Tính năng phân bổ máy ảo trên cùng máy vật lý (affinity)

Cho phép người dùng định nghĩa các quy tắc hợp tác trao đổi dữ liệu giữa các máy ảo; Hỗ trợ triển khai các máy ảo thường xuyên trao đổi dữ liệu với nhau trên cùng một máy vật lý.

- Truy cập vào máy ảo thông qua giao diện bảng điều khiển (console)

Cho phép người dùng truy cập vào máy ảo thông qua giao diện bảng điều khiển (console) với các trình duyệt phổ biến.

- Gắn các tệp tin định dạng ISO trên máy ảo

Cho phép gắn các tệp tin định dạng ISO trên máy ảo (các tệp tin định dạng ISO có thể nằm trên một kho dữ liệu riêng của giải pháp).

- Sao lưu/khôi phục máy ảo

Cho phép người dùng sao lưu máy ảo thành các bản chụp (snapshot) theo kế hoạch được lập thủ công hoặc định kỳ trước đó; lưu trữ bản chụp (snapshot) được tạo ra dựa theo thông tin về thời điểm tạo; sao lưu máy ảo thông qua cổng thông tin quản trị hoặc CLI; khôi phục máy ảo từ bản chụp (snapshot).

- Giới hạn IOPS và băng thông ổ đĩa của máy ảo

Cho phép người quản trị và người dùng giới hạn IOPS của máy ảo và giới hạn băng thông ổ đĩa của máy ảo.

- Giới hạn băng thông mạng của máy ảo

Yêu cầu này cho phép người dùng giới hạn băng thông mạng của máy ảo cho cả hai luồng lưu lượng mạng vào/ra.

- Triển khai máy ảo cần sử dụng các công nghệ tăng tốc (accelerator)

Hỗ trợ cấu hình NUMA và Transparent Hugepage, PCI Pass through, SR-IOV, OVS-DPDK, CPU pinning, DPDK và Direct I/O khi triển khai các máy ảo cần sử dụng các công nghệ tăng tốc (accelerator).

- Tự động chọn máy chủ vật lý khi tạo một máy ảo mới

Cho phép tự động chọn máy chủ vật lý để triển khai máy ảo mới tạo nhằm cân bằng tải giữa các máy chủ vật lý.

- Thiết lập hoặc thiết lập lại mật khẩu cho tài khoản quản trị của máy ảo

Cho phép quản trị viên nhập mật khẩu cho tài khoản quản trị của máy ảo.

- Định nghĩa, cấu hình và khởi tạo cụm gồm nhiều máy ảo

Yêu cầu này cho phép người dùng định nghĩa một cluster mới tùy ý. Ví dụ: một cụm máy chủ ảo 3 tầng gồm 06 máy ảo (02 máy chạy ứng dụng ở mạng công cộng, 02 máy chạy các dịch vụ backend ở mạng cục bộ và 02 máy chạy cơ sở dữ liệu ở mạng cục bộ) có thể được tích hợp với tính năng tự động thay đổi cấu hình hệ thống.

1.2. Máy chủ vật lý Host

Theo Công văn 1145/BTTTT-CATTT ngày 03/04/2020, tại Phụ lục 01 hướng dẫn về tiêu chí, chỉ tiêu kỹ thuật tối thiểu cho cơ sở hạ tầng điện toán đám mây, trong đó phần IV quy định các tiêu chí về **Máy vật lý** phải đáp ứng các tính năng sau đây:

- Tự động cài đặt hệ điều hành và phần mềm giám sát máy ảo (hypervisor)

Cho phép tự động cài đặt hệ điều hành và phần mềm giám sát máy ảo sau khi có những thiết bị (ảo hoặc vật lý) mới truy cập mạng. Cho phép người dùng hoặc các thiết bị khác trong mạng có thể sử dụng, giao tiếp với chúng.

- Triển khai nhiều phiên bản hệ điều hành Windows và Linux cho máy chủ vật lý

Cho phép triển khai nhiều phiên bản hệ điều hành Windows và Linux cho máy chủ vật lý bao gồm: Windows 8 và 10, 2012 và 2016, Ubuntu 14.04, 16.04 và 18.04, CentOS 6.x và 7.x, RHEL 6 và 7, Oracle Linux 6 và 7 và các phiên bản hiện hành của các hệ điều hành được liệt kê ở trên.

- Quản trị qua kênh truyền tín hiệu riêng biệt (out-of-band)

Cho phép quản trị qua kênh truyền tín hiệu riêng biệt sử dụng các giao diện quản lý nền tảng như iRMC, iLO, IDRAC, UCS và các giao diện khác tương đương.

- Truy cập vào máy chủ vật lý thông qua giao diện bảng điều khiển

Cho phép người dùng truy cập vào máy chủ vật lý thông qua giao diện bảng điều khiển (console).

- Cấu hình cơ chế dự phòng cho ổ cứng trên máy chủ vật lý

Cho phép người dùng cấu hình RAID trên máy chủ vật lý.

1.3. Lưu trữ dữ liệu

Giải pháp lưu trữ dữ liệu cung cấp phải ứng dụng các công nghệ tiên tiến nhất, cụ thể:

- Cung cấp năng lực bộ nhớ HDD, SSD. Với những nhu cầu cần hiệu năng cao thì người dùng sử dụng SSD, bên cạnh đó đó nếu nhu cầu cần hiệu năng bình thường thì Người dùng có thể dùng HDD.

- Cung cấp không gian lưu trữ dạng Block Storage, Object storage, File Storage

Hệ thống lưu trữ cho phép giám sát và tạo chính sách đặc quyền truy cập, thao tác ở mức file nhằm ngăn chặn việc mã hoá ransomware dữ liệu, đồng thời cho phép người quản trị quản lý các định dạng file (file extension) được phép lưu trữ trên hệ thống. Hệ thống thực hiện chặn file dựa trên chữ ký số mã thuật của file. Điều này tương tự như cách trình quét chống vi-rút phát hiện vi-rút.

Hệ thống lưu trữ sử dụng nền tảng phân tích cung cấp khả năng hiển thị trên cơ sở hạ tầng, on prem và public cloud. Khắc phục sự cố, giám sát và tối ưu hóa các tài nguyên được sử dụng trong cơ sở hạ tầng điện toán đám mây. Nền tảng phân tích sử dụng công nghệ UEBA (User Entity Behavior Analytics), Machine Learning, AI và Storage Workload Security để :

+ Thực hiện các hành động tự động như Sao chép Snapshot khi hệ thống bị Ransomware, chặn người dùng khi có hoạt động bất thường

+ Phân tích hành vi người dùng

+ Phát hiện thay đổi bất thường trong hoạt động của người dùng.

+ Phân tích các mẫu hành vi bất thường để xác định loại mối đe dọa, phát hiện ransomware.

+ Cung cấp thông tin chi tiết về các cuộc tấn công tiềm ẩn.

Hệ thống lưu trữ có tính năng bảo vệ chống Ransomware tự động (Autonomous Ransomware Protection (ARP)) thực hiện cải thiện khả năng phục hồi mạng bằng cách áp dụng mô hình học máy để phân tích chống phần mềm tống tiền, phát hiện các dạng phần mềm tống tiền liên tục phát triển với độ chính xác 99%. Mô hình học máy của ARP được đào tạo trước trên một tập dữ liệu lớn các tệp trước và sau một cuộc tấn công phần mềm tống tiền mô phỏng. Việc đào

tạo tốn nhiều tài nguyên này được thực hiện bên ngoài hệ thống, nhưng việc học từ quá trình đào tạo được sử dụng cho mô hình bên trong hệ thống.

Hệ thống lưu trữ có tính năng "ghi một lần, đọc nhiều lần" (Write Once Read Many - WORM) thay thế cho kiểu lưu trữ dữ liệu truyền thống. Tính năng này được sử dụng để lưu trữ dữ liệu WORM chỉ đọc mà không được ghì đè, chỉnh sửa hoặc xoá. Mục tiêu chính của tính năng này là cung cấp chức năng lưu giữ và WORM được thực thi bằng lưu trữ bằng cách sử dụng các giao thức tệp mở như CIFS và NFS (không sử dụng được với FC). Tính năng này có thể được triển khai để bảo vệ dữ liệu trong môi trường quản lý nghiêm ngặt theo cách mà ngay cả quản trị viên lưu trữ cũng được coi là bên không đáng tin cậy.

Hệ thống lưu trữ có tính năng Multi Admin Verification (MAV) là tính năng quản lý, phê duyệt các lệnh được thực thi trên hệ thống SAN bằng việc các lệnh thực thi đều phải có sự đồng ý của các quản trị viên. Tính năng này nhằm mục đích kiểm soát các hoạt động xoá dữ liệu backup chỉ được thực thi sau khi có sự đồng ý của các quản trị viên. Việc này đảm bảo an toàn đối với trường hợp như quản trị viên có hành vi, ý định phá hoại hoặc quản trị viên thiếu kinh nghiệm gây ra những thay đổi không mong muốn, mất mát dữ liệu.

Hệ thống có tính năng xác thực đa yếu tố (MFA) cho phép quản trị viên tăng cường bảo mật bằng cách yêu cầu người dùng cung cấp hai phương thức xác thực để đăng nhập vào quản trị viên.

Theo Công văn 1145/BTTTT-CATTT năm 2020, tại Phụ lục 01 hướng dẫn về tiêu chí, chỉ tiêu kỹ thuật tối thiểu cho cơ sở hạ tầng điện toán đám mây, trong đó phần II quy định các tiêu chí về **Thiết bị lưu trữ** phải đáp ứng các tính năng sau đây:

- Tích hợp các thiết bị lưu trữ truyền thống và giải pháp lưu trữ bằng phần mềm

Hỗ trợ giải pháp lưu trữ bằng phần mềm (SDS-Software-Defined Storage); tích hợp các thiết bị SAN (Storage Area Network) và NAS (Network-Attached Storage).

- Tích hợp các dịch vụ lưu trữ

Hỗ trợ lưu trữ dạng khối (block storage); lưu trữ dạng đối tượng (object storage) và lưu trữ dạng tệp tin (file storage).

- Áp dụng chính sách đối với các dịch vụ lưu trữ phân tầng

Cho phép người dùng thiết lập chính sách đối với các dịch vụ lưu trữ phân tầng. Ví dụ: một quản trị viên về việc lưu trữ dữ liệu có thể lập kế hoạch lưu những dữ liệu không thường xuyên sử dụng trên thiết bị SATA chậm hơn và ít tốn kém hơn.

- Gắn bộ nhớ trên nhiều máy ảo

Cho phép gắn một ổ cứng ảo (từ SAN hoặc SDS) trên nhiều máy ảo ổ cứng ảo có thể ở chế độ chỉ đọc); gắn một hệ thống tệp tin chia sẻ dùng chung trên nhiều máy ảo một cách linh hoạt và tự động.

- Quản lý, phân bổ các tham số hiệu năng của ổ cứng ảo

Cho phép người dùng chọn một phân lớp hiệu năng cho các ổ cứng ảo. Ví dụ: IOPS hoặc băng thông (đo bằng Mbps).

- Tự động phân bổ dữ liệu trên vùng lưu trữ

Cho phép tự động phân bổ dữ liệu trên vùng lưu trữ để phân tải cho các ổ đĩa.

- Mở rộng vùng lưu trữ

Cho phép người dùng tăng dung lượng của một vùng lưu trữ đã có sẵn.

- Mở rộng các ổ cứng ảo

Cho phép người dùng tăng kích thước của một ổ cứng ảo (ổ cứng ảo của thiết bị SAN hoặc SDS) đã có sẵn mà không phải cấp thêm ổ cứng ảo mới hoặc sao chép dữ liệu sang ổ cứng ảo mới.

- Di dời dữ liệu giữa các vùng lưu trữ khi hệ thống đang vận hành

Cho phép quản trị viên di chuyển dữ liệu giữa các vùng lưu trữ khi hệ thống đang vận hành đảm bảo dữ liệu được sao chép gần như ngay lập tức từ hệ thống lưu trữ nguồn (source) sang hệ thống lưu trữ đích (destination). Khi một thao tác ghi dữ liệu (write operation) diễn ra trên hệ thống lưu trữ nguồn, cùng một thao tác ghi đó sẽ được thực hiện trên hệ thống lưu trữ đích một cách đồng bộ, đảm bảo rằng cả hai hệ thống đều có cùng một bộ dữ liệu tại bất kỳ thời điểm nào.

- Sao lưu ổ cứng ảo

Cho phép người dùng sao lưu ổ cứng ảo tại một thời điểm bất kỳ thành các bản chụp (snapshot) thông qua các cách thức tự thao tác (self-service.); sử dụng các bản chụp (snapshot) thông qua cách thức tự thao tác (self-service) với mục đích để cấp thêm máy ảo mới; sao lưu dữ liệu trên ổ cứng ảo.

- Khả năng cung cấp lưu *trữ dạng đối tượng (Object storage)*

Cho phép lưu trữ và truy xuất dữ liệu thông qua API trên dịch vụ web; hỗ trợ khả năng thay đổi đối với từng đối tượng đơn lẻ và toàn bộ lưu trữ dạng đối tượng (Object storage).

- Mã hóa dữ liệu

Cho phép người dùng mã hóa dữ liệu hoặc cấu trúc dữ liệu.

- Sao lưu đối tượng

Cho phép người dùng sao lưu đối tượng thành nhiều phiên bản tại những thời điểm khác nhau nhằm mục đích phòng ngừa việc mất mát dữ liệu do ghi đè hoặc xóa đối tượng; cấu hình việc sao lưu thông qua CLI, GUI hoặc API đối với từng đối tượng.

1.4. Các phần mềm quản lý

- Phần mềm quản lý cấp phát tài nguyên

Cấp phát dịch vụ điện toán đám mây theo chính sách (policy-enabled) và tự phục vụ (self-service). Hỗ trợ tính năng workflow bắt buộc người dùng yêu cầu tài nguyên cần phải được approved qua người quản trị VDC đó, có khả năng tạo Service –portal, request và approve theo nhiều cấp đồng thời thông báo theo nhiều giao thức (SMS, Email).

Quản lý đầy đủ vòng đời tài nguyên điện toán đám mây mới được cung cấp và đang hiện hữu.

Đảm bảo bảo mật cho gói dịch vụ cho dịch vụ hạ tầng CNTT mới cũng như quản lý tài nguyên điện toán hiện tại từ danh sách các người sử dụng cụ thể đã xác định từ trước.

Quản lý tài nguyên thông minh đảm bảo hiệu suất sử dụng cao thông qua vị trí đặt, biện pháp phòng ngừa và khôi phục kho tài nguyên trên các server ảo và vật lý. Trên giao diện web portal, người dùng có thể chủ động backup, restore, start, stop các máy ảo. Hỗ trợ cập nhật những thay đổi add / update/ remove trên hypervisor.

- Phần mềm quản lý cấp phát tài nguyên máy chủ ảo

Quản lý với cài đặt cầu hình, dung lượng, hiệu suất và sự tuân thủ tự động hóa đem lại tính linh động cho các đám mây đảm bảo mức độ dịch vụ cung cấp, bộ điều chỉnh và sự tuân thủ thực hiện cao nhất và tối đa hóa sử dụng nguồn lực trong môi trường đám mây lai và không đồng nhất, thông qua quản lý cài đặt cấu hình, dung lượng và hiệu suất được tích hợp.

Bảng điều khiển quản lý vận hành và bộ cảnh báo thông minh nhờ cơ chế tự động: mang tới sự toàn diện, có cái nhìn tổng quát về tình trạng và những nguy cơ và hiệu suất của hạ tầng CNTT. Theo dõi, giám sát hiệu suất hệ thống máy ảo, giúp tối ưu hiệu quả sử dụng của hệ thống tài nguyên. Việc theo dõi này giúp user, người quản trị hoàn toàn chủ động trong việc tăng giảm tài nguyên cho mục đích sử dụng của mình cho phù hợp nhất. User có thể theo dõi hiệu suất của máy ảo thông qua 3 thông số CPU, Memory, và Disk.

Tự động phân tích nguyên nhân chính của các vấn đề về hiệu suất: Phân tích hàng triệu số liệu để xác định nguyên nhân và sức ảnh hưởng của các vấn đề về hiệu suất của hạ tầng CNTT. Có công cụ theo dõi, quản lý tài nguyên trên các máy ảo, trên Quota ngay trên Portal. Có thể tạo ra các policy khi tài nguyên đạt đến một ngưỡng nào cho trước và gọi một hành động như gởi email, warning... Có thể tạo ra các policy khi tài nguyên đạt đến một ngưỡng nào cho trước và gọi một hành động như gởi email, warning...

So sánh về hiệu suất và các sự kiện thay đổi: nhanh chóng xác định và khắc phục các vần đề về hiệu suất phát sinh từ sự thay đổi cấu hình.

Lập kế hoạch, báo cáo và tối đa hóa công suất: Xác định các vùng có năng suất còn lãng phí và thiếu hụt để tối đa hóa mật độ máy ảo. Người quản trị có khả năng theo dõi, giám sát real-time theo chart hoặc sơ đồ, xuất report đánh giá toàn bộ tài nguyên hệ thống theo định kỳ trên một giao diện chung.

Tuân thủ liên tục: Phát hiện, khắc phục và tuân thủ theo cấu hình đạt chuẩn để duy trì một hạ tầng CNTT phù hợp.

Phát hiện và hiển thị các ứng dụng và hạ tầng CNTT: Nâng cao khả năng nhận biết mức độ các ứng dụng cung cấp để đảm bảo mức độ dịch vụ cung cấp và bảo vệ khả năng khôi phục thảm họa cho tất cả các ứng dụng của Doanh nghiệp. Có thể giám sát tài nguyên các máy vật lý như: các Blade Chassis, các máy chủ x3650, hệ thống lưu trữ, network

Tích hợp định lượng và báo cáo chi phí: Mang lại tầm nhìn về khả năng sử dụng các nguồn tài nguyên và giá trị tài chính mang lại khi sử dụng nguồn tài nguyên.

Theo Công văn 1145/BTTTT-CATTT ngày 03/04/2020, tại phụ lục 01 hướng dẫn về tiêu chí, chỉ tiêu kỹ thuật tối thiểu cho cơ sở hạ tầng điện toán đám mây, trong đó phần V quy định các tiêu chí về **Quản trị và vận hành** phải đáp ứng các tính năng sau đây:

- Các tính năng quản trị và vận hành:

+ Định nghĩa các hành động sau khi tạo hoặc xóa máy ảo

Cho phép quản trị viên định nghĩa các hành động sau khi tạo hoặc xóa máy ảo.

+ Thực hiện một hành động do người dùng chỉ định sẵn sau khi quá trình khởi động hoàn thành

Cung cấp tính năng thực hiện một hành động do người dùng chỉ định sẵn thông qua cách thức tự hành (self-service) sau khi quá trình khởi động lần đầu hoàn thành đối với máy ảo mới tạo.

+ Hỗ trợ quản trị cấu hình

Hỗ trợ quản trị cấu hình (thông qua Ansible, Puppet, Chef hoặc SaltStack) bao gồm: Hoạt động như một dịch vụ được tích hợp sẵn để cho phép người dùng quản lý, kiểm tra các cấu hình và quy trình triển khai; Tự động hóa toàn bộ quy trình triển khai, nâng cấp, cập nhật và vá lỗi; Tích hợp các thành phần vận hành tự động có khả năng được cấu hình thông qua các ngôn ngữ lập trình (như YAML,…).

+ Quản lý tài nguyên

Cho phép quản trị viên giám sát, đánh giá lịch sử sử dụng tài nguyên của các máy ảo; đưa ra các khuyến nghị về việc cấp thêm tài nguyên khi cần thiết.

+ Quản lý bản vá

Cho phép tự động tạo thống kê, báo cáo về các bản vá đã được cập nhật; tự động áp dụng các bản vá lên nhiều máy chủ một lúc; khôi phục các bản vá đã cập nhật.

+ Tích hợp giao diện cổng thông tin quản trị

Cho phép tích hợp giao diện cổng thông tin quản trị có tính tự hành cho người dùng đầu cuối (để người dùng tự quản lý tài nguyên được cấp) và giao diện cổng thông tin quản trị cho quản trị viên; hỗ trợ giao diện cổng thông tin quản trị.

+ Tùy biến giao diện cổng thông tin quản trị

Cung cấp tính năng cho phép người dùng tùy biến giao diện cổng thông tin quản trị về hiển thị các thông số, tiêu chí như trạng thái, hiệu năng, tính sẵn sàng của tập hợp các máy chủ, dịch vụ.

+ Quản lý, giám sát nền tảng hạ tầng dịch vụ điện toán đám mây

Cho phép hiển thị theo thời gian thực các thông số giám sát về hiệu năng hệ thống; cấu hình tùy theo ý muốn về cảnh báo hoặc báo cáo khi có sự cố xảy ra; cấu hình khoảng thời gian lấy mẫu các thông số giám sát; giám sát được các thành phần của cơ sở hạ tầng vật lý bao gồm bộ chuyển mạch, bộ định tuyến, tủ chứa máy chủ và các thiết bị lưu trữ.

+ Cảnh báo khi có sự kiện/ sự cố về cơ sở hạ tầng xảy ra

Cung cấp tính năng gửi cảnh báo cho người dùng khi có sự kiện / sự cố về cơ sở hạ tầng xảy ra theo giá trị ngưỡng; cho phép người dùng thiết lập các giá trị ngưỡng đối với từng thành phần một; cho phép cảnh báo tới người dùng thông qua email, SMS.

+ Thu thập và lưu trữ log hệ thống

Cung cấp tính năng thu thập, lưu trữ và xoay vòng định kỳ log hệ thống về các tác vụ tạo, đọc, cập nhật, xóa - CRUD (Create, Read, Update, Delete – tạo, đọc, cập nhật, xóa), tài nguyên được sử dụng,…

+ Tích hợp API giám sát dữ liệu

Cung cấp tính năng tích hợp API dành cho giám sát dữ liệu (bao gồm các thông số về trạng thái hoạt động hiện tại và trong quá khứ đối với từng thành phần được giám sát) để cho phép người dùng giám sát, phân tích dữ liệu thông qua các hệ thống giám sát in-house hoặc của bên thứ ba sử dụng API đó.

+ Ghi log về các sự kiện liên quan đến tài khoản

Cung cấp tính năng ghi log về các sự kiện liên quan đến tài khoản như: các thao tác

đăng nhập tài khoản, quản lý tài khoản bao gồm tạo / xoá / lập nhóm / gắn thẻ cho tài khoản người dùng và các thao tác khác; Cho phép người dùng xem các bản ghi log thông qua giao diện có tính tự hành và khả năng xuất các bản ghi log để lưu giữ lâu hơn.

1.5. Tổ chức hệ thống mạng

Theo Công văn 1145/BTTTT-CATTT ngày 03/04/2020, tại Phụ lục 01 hướng dẫn về tiêu chí, chỉ tiêu kỹ thuật tối thiểu cho cơ sở hạ tầng điện toán đám mây, trong đó phần III quy định các tiêu chí về Mạng và mạng định nghĩa bằng phần mềm (Software-Defined Networking - SDN) phải đáp ứng các tính năng sau đây:

- Quản lý hiệu năng mạng

Yêu cầu này cho phép người dùng quản lý hiệu năng đối với từng mạng mà máy ảo kết nối đến bao gồm việc giới hạn băng thông, độ trễ, quản lý chất lượng dịch vụ (QoS).

- Tích hợp nhiều cổng giao tiếp mạng ảo trên vNIC một máy ảo

Cho phép nhiều địa chỉ IP khác nhau được gán cho một máy ảo thông qua tích hợp nhiều cổng giao tiếp mạng ảo; định nghĩa nhiều phân đoạn mạng ảo, nhiều mạng con cho mỗi mạng ảo.

- Hỗ trợ khả năng dự phòng từ mức vật lý cho các mạng mà máy ảo kết nối đến

Hỗ trợ khả năng dự phòng từ mức vật lý (ít nhất ở mức cổng vật lý – NIC) cho các mạng mà máy ảo kết nối đến; hoạt động ở mức active-active hoặc active-standby để cải thiện băng thông và bảo đảm tính sẵn sàng.

- Cấp phát địa chỉ IP

Cho phép một máy ảo được gán địa chỉ IP động và địa chỉ IP này phải luôn không đổi giá trị trong suốt quá trình hoạt động của máy ảo.

- Liên kết với bộ chuyển mạch và bộ định tuyến thông thường

Cung cấp tính năng SDN hoặc liên kết với các bộ chuyển mạch và bộ định tuyến thông thường của nhiều hãng khác nhau.

- Phòng chống tấn công giả mạo địa chỉ IP và giả mạo gói tin ARP

Cung cấp tính năng phòng chống tấn công giả mạo địa chỉ IP và giả mạo gói tin ARP đối với mạng nội bộ của máy ảo hoặc các mạng mà máy ảo và máy vật lý kết nối đến.

- Hỗ trợ VLAN và VXLAN

Cung cấp tính năng cho phép người dùng định nghĩa các mạng ảo bao gồm cả VLAN và VXLAN.

- Hỗ trợ bộ định tuyến ảo

Cho phép người dùng sử dụng các chức năng của bộ định tuyến (NAT, định tuyến giữa các VLAN,…) để quản lý kết nối giữa các mạng.

- Tích hợp dịch vụ cân bằng tải

Yêu cầu này cho phép người dùng sử dụng dịch vụ cân bằng tải đã được tích hợp sẵn (dịch vụ bao gồm các chức năng cấu hình giám sát, cấu hình cho thiết bị đầu cuối và tương thích với nhiều máy ảo đang kết nối với nhiều mạng ảo khác nhau).

- Cấu hình chính sách truy cập cho từng cổng trên máy ảo

Yêu cầu này cho phép người dùng cấu hình chính sách truy cập cho từng cổng (thuộc cổng giao tiếp mạng ảo trên vNIC) trên những máy ảo đang chạy.

- Tích hợp dịch vụ tường lửa

Cho phép người dùng sử dụng dịch vụ tường lửa đã được tích hợp sẵn (dịch vụ phải hoạt động bình thường trên tầng IP và Domain).

- Hỗ trợ IPv6 cho cả mạng vật lý và mạng ảo

Cung cấp tính năng hỗ trợ máy ảo hoặc cổng kết nối (ví dụ: bộ cân bằng tải) sử dụng IPv6 trên cả mạng vật lý và mạng ảo.

- Tách biệt các mạng ảo với nhau

Cung cấp tính năng tách biệt hoàn toàn các mạng ảo khác nhau.

- Đảm bảo sự hao phí băng thông đường truyền kết nối giữa các mạng không vượt quá 10%

Cung cấp tính năng đảm bảo sự hao phí băng thông đường truyền kết nối giữa máy ảo với máy ảo và máy ảo với thành phần bên ngoài. Ví dụ: nếu thiết lập 02 mạng VXLAN cho 02 máy ảo khác nhau trong mạng vật lý có băng thông là 10 Gbps thì băng thông thực tế của đường truyền kết nối giữa các máy ảo này phải > 9 Gbps.

- Đảm bảo hạ tầng kỹ thuật cho máy chủ vật lý và máy ảo có tính sẵn sàng cao

Cung cấp tính năng đảm bảo máy chủ vật lý và máy ảo chạy trên hạ tầng kỹ thuật có tính sẵn sàng cao, đảm bảo tính nguyên vẹn và tính bí mật của dữ liệu.

- Hỗ trợ cấu trúc liên kết mạng có tính phân cấp do người dùng định nghĩa

Cho phép người dùng tự thiết kế các thành phần và sơ đồ mạng bao gồm tường lửa ảo, VLAN / VXLAN / GRE, mạng con, NAT, r bộ cân bằng tải ảo.

- Hỗ trợ SDN

Cung cấp tính năng tạo bộ chuyển mạch ảo và bộ định tuyến ảo.

- Tách biệt các mặt phẳng SDN với nhau

Cung cấp tính năng tách biệt các mặt phẳng điều khiển, mặt phẳng chuyển tiếp và mặt phẳng quản trị với nhau.

- Hỗ trợ Open Flow hoặc tương đương

Cung cấp tính năng hỗ trợ OpenFlow cho SDN hoặc tương đương.

- Hỗ trợ tích hợp nền tảng điện toán đám mây

Cung cấp tính năng hỗ trợ API sử dụng nền tảng điện toán đám mây để tạo bộ chuyển mạch ảo và bộ định tuyến ảo.

- Quản trị và điều khiển bộ chuyển mạch ảo và bộ định tuyến ảo

Cung cấp tính năng quản trị và điều khiển bộ chuyển mạch ảo và bộ định tuyến ảo.

- Tự động tạo và quản trị bộ chuyển mạch ảo và bộ định tuyến ảo

Cung cấp tính năng tự động tạo và quản trị bộ chuyển mạch ảo và bộ định tuyến ảo.

- Hỗ trợ AAA

Cung cấp tính năng tích hợp các thành phần để xác thực, phân quyền, ghi log hoạt động (authenticate, authorize, account – AAA) người dùng.

- Quản trị các thành phần trong mạng

Cho phép người dùng sử dụng SNMP, Netconf hoặc tương đương có chức năng quản trị các thành phần khác trong mạng.

- Đảm bảo bộ điều khiển có tính sẵn sàng cao

Cung cấp tính năng đảm bảo bộ điều khiển cho SDN có tính sẵn sàng cao.

- Hỗ trợ Jumbo Frame

Cung cấp tính năng sử dụng Jumbo Frame (các khung có kích thước gói tin lớn nhất – MTU – có thể lên đến 9000 byte) trong việc truyền tải gói tin.

- Tích hợp CLI và GUI

Cho phép người dùng cấu hình, quản lý các thành phần trong mạng, bộ điều khiển cho SDN thông qua CLI và GUI.

- Hỗ trợ các chức năng của bộ chuyển mạch ảo và bộ định tuyến ảo

Hỗ trợ SPAN, RSPAN hoặc tương đương; LACP (mode 1, 2, 3, 4) từ máy ảo, máy vật lý, 802.1Q VLAN with trunking, multicast snooping, LLDP, STP, RSTP, quản lý chất lượng dịch vụ (QoS), VXLAN.

1.6. Tích hợp hệ thống

Theo Công văn 1145/BTTTT-CATTT ngày 03/04/2020, tại Phụ lục 01 hướng dẫn về tiêu chí, chỉ tiêu kỹ thuật tối thiểu cho cơ sở hạ tầng điện toán đám mây, trong đó phần VI quy định các tiêu chí về Tích hợp phải đáp ứng các tính năng sau đây:

- Tích hợp giao diện tương tác với thành phần quản lý chức năng mạng ảo (Virtual Network Function – VNF)

Cung cấp tính năng tích hợp giao diện tương tác với thành phần VNF từ nhiều hãng (như Nokia, Ericsson, Huawei, ZTE,…) mà tuân theo kiến trúc ETSI MANO để hỗ trợ quản lý vòng đời VNF cũng như khả năng mở rộng.

- Tích hợp CLI và API tương tác với hệ thống

Cung cấp tính năng tích hợp CLI và API cho phép quản trị viên thực hiện các thao tác trên hệ thống.

- Hỗ trợ thư viện phục vụ cho lập trình, phát triển phần mềm tương tác với hệ thống

Cung cấp tính năng hỗ trợ các thư viện (mã nguồn mở hoặc tự cloud provider tạo) phục vụ cho lập trình, phát triển phần mềm tương tác với hệ thống như tương thích với các ngôn ngữ lập trình phổ biến Java, .NET, Perl, Node.js, PHP, Python, Ruby và PowerShell.

1.7. Các tính năng khác

1.7.1. Yêu cầu tính năng khác

Theo Công văn 1145/BTTTT-CATTT năm 2020, tại Phụ lục 01 hướng dẫn về tiêu chí, chỉ tiêu kỹ thuật tối thiểu cho cơ sở hạ tầng điện toán đám mây, trong đó phần VII quy định các tiêu chí về Các yêu cầu khác phải đáp ứng các tính năng sau đây:

- Đảm bảo khả năng mở rộng

Cung cấp tính năng thay đổi hệ thống bao gồm cấp thêm máy chủ, thiết bị lưu trữ, các thiết bị mạng mà không thay đổi kiến trúc.

- Đảm bảo tính sẵn sàng cao của các thành phần dịch vụ

Cung cấp tính năng đảm bảo tính năng sẵn sàng cao của các thành phần như giao diện quản lý của quản trị viên, API, các thành phần điều khiển tập trung.

- Đảm bảo tính sẵn sàng cao của hệ thống

Cung cấp tính năng đảm bảo hệ thống có tính sẵn sàng cao theo tỷ lệ thời gian đáp ứng.

1.7.2. Kết nối từ xa (VPN)

Cung cấp kết nối mạng an toàn cho người dùng từ xa và thiết bị di động thông qua kiểm soát truy cập, xác thực và mã hóa. Hỗ trợ IPsec VPN và SSL VPN (giải pháp an toàn và dễ dàng kết nối các ứng dụng trong công ty qua mạng internet thông qua thiết bị di động, máy tính cá nhân..):

- Hỗ trợ VPN dạng site-to-site hay truy cập xa, đơn giản và quản lý tập trung.

- Nâng cao tính bảo mật của IPSec VPN.

- Hỗ trợ nhiều kết nối truy cập từ xa.

- Đảm bảo tính liền mạch và tích hợp tính năng dự phòng.

1.7.3. Giám sát máy chủ

Dịch vụ giám sát máy chủ là một hệ thống giám sát mạng, dùng để giám sát và quản lý hiệu suất của các thành phần mạng và hệ thống. Các tính năng của dịch vụ giám sát máy chủ:

- Giám Sát Đa Nền Tảng: Hỗ trợ giám sát đa nền tảng, bao gồm Linux, Windows, Unix, và nhiều nền tảng khác.

- Kiểm Soát Hiệu Suất Hệ Thống theo ngưỡng: Theo dõi hiệu suất của CPU, bộ nhớ, ổ đĩa và các thành phần hệ thống khác.

- Giám Sát Mạng: Theo dõi băng thông mạng, sự truy cập từ xa, lưu lượng mạng và các thông số khác liên quan đến mạng.

- Phân Tích Log và Sự Kiện: Tích hợp với các log và sự kiện hệ thống để phân tích thông tin chi tiết về sự kiện xảy ra.

- Báo Cáo và Thống Kê: Cung cấp báo cáo và thống kê về hiệu suất và sự kiện mạng qua thời gian.

- Giám Sát Ứng Dụng và Dịch Vụ: Theo dõi hiệu suất của ứng dụng và dịch vụ chạy trên hệ thống, giúp xác định vấn đề nhanh chóng.

2. Phương án triển khai các dịch vụ an ninh thông tin

2.1. Giải pháp tổng thể

2.1.1. Mô hình tổng thể

Để đảm bảo an ninh thông tin, hệ thống an ninh thông tin được triển khai bảo vệ đa lớp và phòng thủ theo chiều sâu, chi tiết như sau:

Dịch vụ chống tấn công DDoS.

Mã hóa đường truyền VPN (IPSec, SSL), xác thực người dùng.

Dịch vụ cân bằng tải.

Dịch vụ tường lửa hoạt động ở chế độ HA bảo vệ máy chủ ứng dụng/cơ sở dữ liệu ở vùng Backend.

Dịch vụ tường lửa ứng dụng web (Web Application Firewall) kiểm soát và bảo vệ chuyên sâu các ứng dụng trên web.

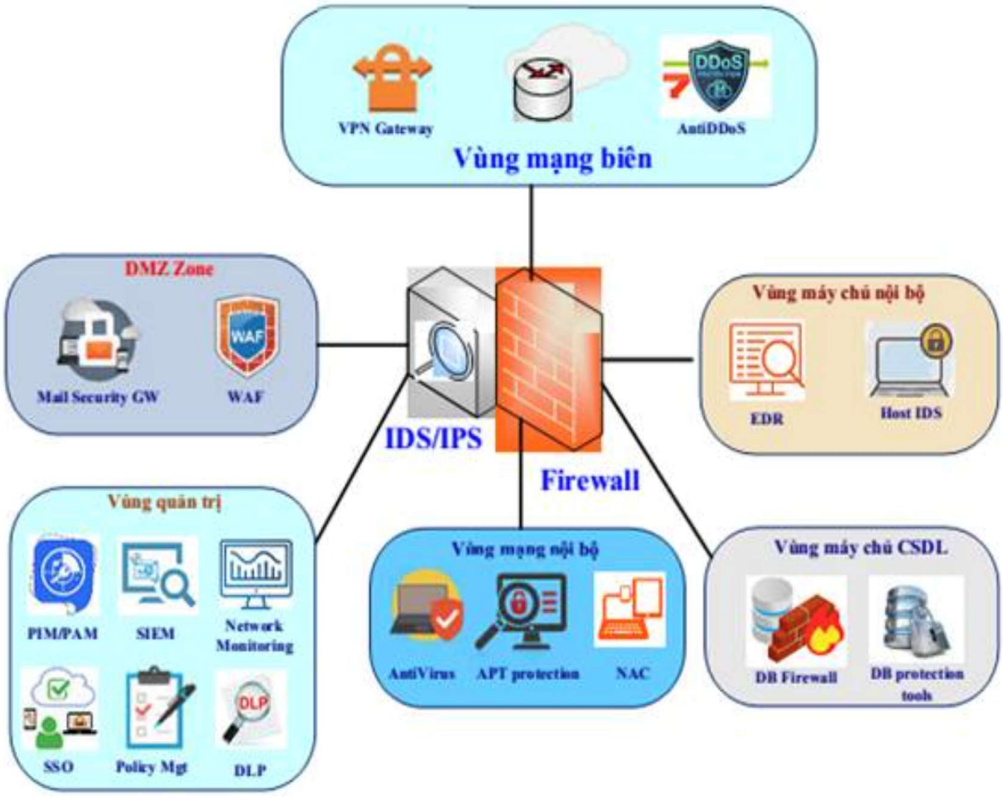
Dịch vụ phát hiện xâm nhập IPS bảo vệ các thành phần mạng lõi.

Dịch vụ phòng chống xâm nhập IPS vòng ngoài tại cổng Internet.

Dịch vụ giám sát và cảnh báo sớm (SIEM).

Dịch vụ phòng chống phần mềm độc hại trên môi trường mạng

Chương trình chống mã độc cài đặt trên các máy chủ, được cập nhật mã nhận dạng virus mới liên tục và quét virus tự động và định kỳ.



2.1.2. Các tiêu chí, chỉ tiêu kỹ thuật an toàn thông tin cho hạ tầng điện toán đám mây

Theo Công văn số 783/TTH-HTDLS ngày 16 tháng 6 năm 2020 của Cục Tin học hóa về tài liệu hướng dẫn ứng dụng dịch vụ điện toán đám mây và thuê dịch vụ điện toán đám mây trong cơ quan nhà nước.

Theo Công văn số 2612/BTTTT-CATTT ngày 17/7/2021 của Bộ Thông tin và Truyền thông về việc bổ sung bộ tiêu chí, chỉ tiêu để đánh giá và lựa chọn giải pháp nền tảng điện toán đám mây phục vụ Chính phủ điện tử/Chính quyền điện tử.

Theo Công văn 1145/BTTTT-CATTT ngày 03/04/2020, tại Phụ lục 02 hướng dẫn về

tiêu chí, chỉ tiêu kỹ thuật an toàn thông tin cho hạ tầng điện toán đám mây, trong đó quy định các tiêu chí cơ bản về tính năng an toàn thông tin đáp ứng các yêu cầu sau đây:

STT	Tên tính năng	Tiêu chí, chỉ tiêu kỹ thuật	Dẫn chứng giải pháp đáp ứng tiêu chí
1	Bảo vệ thông tin cá nhân của người dùng	Giải pháp cung cấp tính năng phòng chống việc mất mát, rò rỉ, giả mạo, thay đổi, lợi dụng thông tin cá nhân của người dùng trong cả quá trình truyền tin và lưu trữ.	Đáp ứng tại giải pháp về mã hóa dữ liệu, giám sát truy cập và an ninh thông tin điểm đầu cuối: Dịch vụ Tường lửa Dịch vụ dò quét mã độc Dịch vụ Dò quét phát hiện và ngăn chặn xâm nhập IPS Dịch vụ phòng chống phần mềm độc hại trên môi trường mạng Dịch vụ Chứng thực số SSL
2	Tích hợp dịch vụ xác thực người dùng	Giải pháp cung cấp tính năng xác thực người dùng thông qua các dịch vụ bên thứ ba có thể được tích hợp vào (dựa trên, LDAP hoặc OpenID / SAM) trước khi người dùng truy cập vào các giao diện gồm cổng thông tin quản trị, danh mục dịch vụ và quản trị.	Đáp ứng tiêu chí tại giải pháp về hệ thống mật khẩu đặc quyền. Dịch vụ VPN
3	Tích hợp điều khiển truy cập dựa trên vai trò - RBAC (Role-Based Access Control)	Giải pháp cung cấp 03 tính năng sau: 1. Tích hợp sẵn các quyền truy cập đã được định nghĩa trước bao gồm ít nhất 02 quyền mức quản trị dành cho nhà cung cấp dịch vụ điện toán đám mây (bên cung cấp) và người sử dụng sử dụng dịch vụ điện toán đám mây (bên sử dụng). 2. Cho phép nhà cung cấp dịch vụ điện toán đám mây định nghĩa	Đáp ứng tiêu chí tại giải pháp về phần mềm quản lý cấp phát tài nguyên

STT	Tên tính năng	Tiêu chí, chỉ tiêu kỹ thuật	Dẫn chứng giải pháp đáp ứng tiêu chí
		các quyền truy cập đối với các thao tác mà nhà cung cấp thực hiện trên tất cả các thành phần của nền tảng nhằm phục vụ mục đích quản trị. 3. Cho phép nhà cung cấp dịch vụ điện toán đám mây định nghĩa các quyền truy cập đối với các thao tác mà người sử dụng sử dụng dịch vụ điện toán đám mây thực hiện trên những thành phần của nền tảng mà người sử dụng muốn sử dụng và tuân theo thỏa thuận giữa hai bên.	
4	Giao tiếp giữa các thành phần qua kênh TLS	Giải pháp cung cấp tính năng cho phép các thành phần giao tiếp qua kênh TLS.	Có
5	Hỗ trợ TLS tự kí (Self-signed TLS)	Giải pháp cung cấp 02 tính năng sau: 1. Cho phép quản trị viên tạo các chứng thư điện tử tự kí (Self-signed) TLS để đẩy nhanh quá trình triển khai. 2. Cho phép các chứng thư điện tử được tạo bởi một đơn vị cấp chứng thư (CA) tin cậy (trusted certificate authority).	Đáp ứng tiêu chí tại Giải pháp ký số HSM
6	Tích hợp giao diện	Giải pháp cung cấp tính năng tích hợp giao	Có

STT	Tên tính năng	Tiêu chí, chỉ tiêu kỹ thuật	Dẫn chứng giải pháp đáp ứng tiêu chí
	cổng thông tin quản trị hỗ trợ sử dụng kênh TLS	diện cổng thông tin quản trị hỗ trợ sử dụng kênh TLS dành cho người dùng đầu cuối và quản trị viên khi muốn kết nối qua kênh TLS.	
7	Chuyển hướng kết nối qua sử dụng TLS	Giải pháp cung cấp tính năng cho phép quản trị viên cấu hình để áp dụng chính sách phải sử dụng kênh TLS đối với mọi kết nối truy cập vào giao diện cổng thông tin trên và dùng các phiên HTTP không mã hóa giống như là một lựa chọn dự phòng	Có
8	Ghi log hoạt động của các hành động	Giải pháp cung cấp 03 tính năng sau: 1. Ghi log hoạt động của các hành động thực hiện trên tất cả các thành phần. 2. Cho phép quản trị viên xem xét, kiểm tra log thu được thông qua thành phần báo cáo. 3. Chuyển log thu thập được cho bên thứ ba cung cấp giải pháp bảo mật để xem xét, kiểm tra kỹ hơn.	Đáp ứng tiêu chí tại Dịch vụ phát hiện, cảnh báo sớm các vấn đề về an ninh thông tin (SIEM)
9	Tách biệt máy ảo với phần mềm giám sát máy ảo	Giải pháp cung cấp tính năng đảm bảo máy ảo được giám sát bởi một phần mềm giám sát máy ảo không gây ảnh hưởng đến phần mềm giám sát đó.	Đáp ứng tiêu chí tại giải pháp về phần mềm quản lý cấp phát tài nguyên

STT	Tên tính năng	Tiêu chí, chỉ tiêu kỹ thuật	Dẫn chứng giải pháp đáp ứng tiêu chí
10	Phân quyền cho máy ảo truy cập đến tài nguyên	Giải pháp cung cấp tính năng đảm bảo phần mềm giám sát máy ảo phân quyền cho máy ảo mà nó giám sát truy cập đến tài nguyên đúng theo chính sách quản trị nền tảng.	Đáp ứng tiêu chí tại giải pháp về phần mềm quản lý cấp phát tài nguyên
11	Cấu hình cho phần mềm giám sát máy ảo	Giải pháp cung cấp tính năng cho phép quản trị viên cấu hình cho phần mềm giám sát máy ảo và kiểm tra được tính hợp lệ của cấu hình phần mềm giám sát máy ảo.	Đáp ứng tiêu chí tại giải pháp về phần mềm quản lý cấp phát tài nguyên
12	Bảo vệ dữ liệu	Giải pháp cung cấp tính năng phòng chống việc mất mát, rò rỉ, thay đổi dữ liệu trong cả quá trình lưu trữ trên các bộ nhớ dùng chung và truyền tin qua các mạng chia sẻ.	Đáp ứng tiêu chí tại mô hình giải pháp tổng thể về các dịch vụ an ninh thông tin.
13	Tách biệt các máy ảo với nhau	Giải pháp cung cấp tính năng tách biệt hoàn toàn các máy ảo với nhau về logic.	Đáp ứng tiêu chí giải pháp ảo hóa máy chủ
14	Đảm bảo các API của hệ thống có ít nhất 02 mức quyền truy cập đã định nghĩa sẵn cho các API của client	Giải pháp cung cấp 02 tính năng sau: 1. Đảm bảo các chức năng quản trị và vận hành của hệ thống định nghĩa sẵn ít nhất 02 mức quyền truy cập cho các API của client (ví dụ: quyền root và quyền user, trong đó	Đáp ứng tiêu chí giải pháp ảo hóa máy chủ

STT	Tên tính năng	Tiêu chí, chỉ tiêu kỹ thuật	Dẫn chứng giải pháp đáp ứng tiêu chí
		quyền root cao hơn quyền user). 2. Đảm bảo các chức năng quản trị và vận hành của hệ thống xác thực được client dựa trên các tiêu chí được định nghĩa trước bởi quản trị viên.	

2.2. Dịch vụ phát hiện và ngăn chặn xâm nhập IPS

Intrusion prevention system (IPS) là một hệ thống giám sát mạng để phát hiện và ngăn chặn các hoạt động xâm nhập độc hại như các mối đe dọa bảo mật hay vi phạm chính sách. Chức năng chính của IPS là xác định các hoạt động nguy hại, lưu giữ các thông tin về chúng, cố gắng chặn lại các hoạt động đó và báo cáo cho quản trị .

Một số tính năng chính

- Phát hiện và phòng chống xâm nhập (IPS) lớp ngoài: thực hiện chức năng giám sát, chống xâm nhập tại cổng kết nối Internet, Metronet cho toàn mạng.

- Bảo vệ các ứng dụng ảo hóa ở ngay bên trong hạ tầng mạng ảo.

- Sử dụng virtual patching bảo vệ các lỗ hổng bảo mật trong hệ điều hành và các ứng dụng cho tới khi chúng được vá, giúp chống lại các tấn công đã biết hoặc bảo vệ các lỗ hổng bảo mật trong hệ điều hành và các ứng dụng cho tới khi chúng được vá, giúp chống lại các tấn công đã biết hoặc zero-day.

- Bảo vệ các lỗ hổng bảo mật trong hệ điều hành và các ứng dụng cho tới khi chúng được vá, giúp chống lại các tấn công đã biết hoặc zero-day.

- Sử dụng các mô hình số liệu được phát triển với những kỹ thuật máy học (machine learning) khả năng phát hiện và ngăn chặn hiểm họa theo thời gian thực.

- Theo dõi các hoạt động bất thường đối với hệ thống.

- Xác định ai đang tác động đến hệ thống và cách thức như thế nào, các hoạt động xâm nhập xảy ra tại vị trí nào trong cấu trúc mạng.

- Tương tác với hệ thống firewall để ngăn chặn kịp thời các hoạt động thâm nhập hệ thống.

- Kiểm soát các ứng dụng ra/vào hệ thống gateway;

- Kiểm soát và chống các hình thức xâm nhập hệ thống.

- Hệ thống phải có tính năng dự phòng đảm bảo tính sẵn sàng của dịch vụ.

2.3. Dịch vụ tường lửa đa lớp

Cung cấp tính năng phòng ngừa mối đe dọa được tích hợp đầy đủ, toàn diện để chống lại những mối đe dọa mới đồng thời giảm bớt sự phức tạp và tăng hiệu quả hoạt động. Giải pháp bao gồm các tính năng bảo mật mạnh mẽ như tường lửa, IPS, Anti-Bot, Antivirus,

Application Control và URL Filtering để chống lại các cuộc tấn công mạng và các mối đe dọa đã biết, bây giờ đã được cải tiến bổ sung với tính năng Threat Emulation và Threat Extraction để bảo vệ hoàn toàn khỏi các mối đe dọa tinh vi nhất và lỗ hổng zero-day.

2.4. Dịch vụ Phát hiện, cảnh báo sớm các vấn đề nguy cơ liên quan đến an toàn thông tin

Giải pháp cung cấp đầy đủ thành phần, chức năng của Trung tâm Điều hành An ninh mạng – SOC bao gồm: Con người, Quy trình và Công nghệ.

- Hỗ trợ thu thập, giám sát và phân tích dữ liệu từ nhiều môi trường và nền tảng khác nhau: Application, Endpoint, Network, MultiCloud.
- Hỗ trợ mô hình multi-site, cho phép triển khai với các khách hàng có nhiều văn phòng, chi nhánh tại nhiều địa điểm địa lý khác nhau.
- Cung cấp đầy đủ, đa dạng các công cụ phân tích an ninh bảo mật trên một nền tảng duy nhất: NG SIEM, NDR, MLIDS, APT SANDBOX, NTA, UEBA, SOAR, SIEM, CASE MANAGEMENT, MULTI TENANCY, THREAT INTELLIGENCE.
- Hợp nhất các bước thu thập, phát hiện, phân tích, phản ứng, ngăn chặn, điều tra truy vết trên một giao diện tập trung duy nhất.
- Thu thập và xử lý thông tin: thu thập thông tin từ nhiều nguồn khác nhau (Network traffic, log server, log từ thiết bị mạng, môi trường ảo hóa public/private cloud, container), chuyển đổi dữ liệu thành metadata, kiến trúc hóa lại dưới dạng Interflow, làm sạch, làm giàu dữ liệu bằng Threat Intelligence, geo-location, tương quan dữ liệu…
- Phân tích, phát hiện: sử dụng AI, Threat Intelligence, IDS, SANDBOX, UEBA, anti-Phishing, Deception, NTA…
- Điều tra: Bằng Threat hunting (manually hoặc tự động), tạo ra các query với nhiều điều kiện lọc khác nhau…
- Phản ứng, ngăn chặn: Dùng module SOAR để phản ứng lại mối đe dọa một cách tự động (gửi thông tin đến firewall, Endpoint để block cuộc tấn công, gửi email, tạo ticket…).

Nâng cao khả năng bảo mật của hệ thống:

- Cung cấp, bổ xung đầy đủ các công cụ bảo mật mà một hệ thống bảo mật mạng cần có.
- Giảm thời gian phát hiện trung bình và thời gian phản ứng trung bình đối với các mối đe dọa.
- Có khả năng phát hiện và phản ứng với các cuộc tấn công có chủ đích APT.
- Thu thập, tích hợp dữ liệu liên quan để nhanh hơn phân tích sự cố chính xác hơn.
- Áp dụng Big Data và Machine Learning phát hiện các nguy cơ phức tạp từ sớm và nâng cao khả năng hệ thống theo thời gian.

Đơn giản hóa thao tác vận hành và khai thác hệ thống:

- Giải pháp cung cấp giao diện web thân thiện, dễ sử dụng, có khả năng tùy chỉnh bằng Tiếng Việt.

- Cung cấp khả năng tự động hóa cho các tác vụ lặp đi lặp lại, tự động cảnh báo, tự động báo cáo.
- Hỗ trợ nhiều loại biểu đồ, hình ảnh đồ họa trực quan.
- Đơn giản hóa quá trình giám sát, phân tích: hỗ trợ tự động xử lý dựa trên nền tảng hợp nhất, giảm số lượng log và cảnh báo, đưa ra hướng dẫn và tham chiếu cho các trường hợp xử lý cụ thể.

Dễ dàng triển khai và tích hợp

- Hỗ trợ, tương thích nhiều mô hình triển khai khác nhau: OnPremise, Cloud, Hybrid.
- Dễ dàng tích hợp với hạ tầng hiện tại của khách hàng.
- Hỗ trợ tích hợp giải pháp của các hãng thứ 3 thông qua API mở.
- Tích hợp 2 chiều với các hãng firewall, gửi phản ứng tự động xuống firewall để ngay lập tức ngăn chặn.
- Linh hoạt trong việc điều chỉnh, mở rộng quy mô sử dụng.

Các thành phần chính.

- Thu thập dữ liệu (collect).
- Phát hiện (Detect).
- Điều tra truy vết (Investigate).
- Phản ứng (Respond).

2.5. Dịch vụ phòng chống phần mềm độc hại trên môi trường mạng (Phòng chống phát hiện tấn công có chủ đích APT)

Hệ thống phòng chống phát hiện tấn công có chủ đích APT (Advanced Persistent Threat) là một hệ thống bảo mật được thiết kế để phát hiện, ngăn chặn và phản ứng lại các cuộc tấn công của những kẻ tấn công có chủ đích, tiên tiến và kiên nhẫn (APT). Các cuộc tấn công APT thường được thực hiện bằng cách sử dụng các kỹ thuật tấn công cao cấp như phishing, spear-phishing, malware, trojan, rootkit, backdoor, và exploitation để xâm nhập vào hệ thống mục tiêu và lấy được dữ liệu quan trọng. Để phát hiện và ngăn chặn các cuộc tấn công APT, các hệ thống phòng chống phải có khả năng theo dõi và phân tích các hoạt động mạng, tìm kiếm các dấu hiệu của các mối đe dọa tiềm năng và đưa ra cảnh báo kịp thời. Giải pháp phải được thiết kế để phát hiện và ngăn chặn các cuộc tấn công có chủ đích APT. Sử dụng các kỹ thuật phân tích nâng cao để phát hiện các mối đe dọa mạng tiềm năng và giải mã các tấn công trước khi chúng có thể gây hại cho hệ thống.

Các thành phần của giải pháp cung cấp dịch vụ:

Network Content Inspection: Giám sát và phân tích lưu lượng mạng để phát hiện các mối đe dọa tiềm ẩn.

Advanced Threat Detection: Sử dụng các kỹ thuật phát hiện tiên tiến để nhận diện các cuộc tấn công phức tạp và các mối đe dọa bền bỉ (APT).

Sandbox Analysis: Môi trường phân tích cách ly để kiểm tra các tệp tin và URL đáng ngờ mà không ảnh hưởng đến hệ thống thực.

Centralized Management: Giao diện quản lý tập trung giúp dễ dàng theo dõi và điều hành các hoạt động bảo mật.

Integration with Other Security Solutions: Tích hợp với các giải pháp bảo mật khác của Trend Micro để cung cấp một hệ thống bảo vệ toàn diện.

2.6. Dịch vụ phòng chống mã độc trên máy chủ

Dịch vụ dò quét mã độc giúp kiểm soát an ninh đầu cuối, cung cấp nền tảng bảo mật toàn diện cho máy chủ, giúp đơn giản hóa hoạt động bảo mật. Các mô đun dịch vụ được tích hợp chặt chẽ giúp bảo mật dữ liệu, ứng dụng và server trên các máy chủ vật lý, ảo và đám mây. Do vậy có thể tùy chỉnh mức độ bảo mật của mình bằng cách kết hợp phương án bảo vệ không sử dụng agent (Agent-less) hoặc sử dụng agent (Agent-based). Kết quả là tạo ra một nền tảng bảo mật hiệu quả, tương thích và toàn diện để bảo vệ dữ liệu và các ứng dụng.

Các thành phần của giải pháp:

- Security Agent: Là một phần mềm cài đặt dưới máy người dùng có nhiệm vụ phát hiện xử lý những malware, thu thập thông tin từ máy tính người dùng bao gồm: Event log, Process log, Connection Log gửi về DB server để phân tích, giám sát và cung cấp dữ liệu cho hệ thống học máy. Agent hoạt động ở dạng ẩn (nền tảng - background) hoàn toàn trong suốt với người sử dụng. Đồng thời Agent tiêu tốn rất ít tài nguyên của máy client (20 MB bộ nhớ RAM, rất ít CPU).

- IR Server (Incident Response Server): Cụm máy chủ có các chức năng:

+ Nhận, thu thập log.

+ Sử dụng thông tin IoC về các mẫu malware phổ biến để IR client kiểm tra, đánh giá. Hệ thống IoC được cập nhật thường xuyên: IP blacklist, Url độc hại, C&C server, Virus signatures, MD5 hashes, botnet command.

+ Sử dụng dữ liệu Threat Intelligent (TI Data) để kiểm tra thông tin về một hành vi, dấu hiệu bất thường để hệ thống đưa ra quyết định tệp tin có bị nhiễm malware không. Dữ liệu Threat Intelligent (TI Data) bao gồm các thông tin như IP blacklist, Url độc hại, C&C server, thuật toán/kỹ thuật mã độc sử dụng (Ví dụ: thuật toán DGA sinh tên miền mã độc tự động), hành vi bất thường (Ví dụ: tiến trình cha chạy dưới quyền người dùng thấp hơn tiến trình con).

+ Sử dụng thuật toán học máy (Machine Learning) nhằm phát hiện và cảnh báo các sự kiện bất thường trên máy client. Ngoài ra, hệ thống còn có khả năng tự học liên tục từ các dữ liệu bất thường thu thập được từ máy client. So với phương pháp truyền thống chủ yếu sử dụng signature, các rule, hash để phát hiện như hiện nay, thì phương pháp này có khả năng phát hiện, ngăn chặn và loại bỏ mã độc sớm hơn, giảm thiểu tối đa thiệt hại do mã độc gây ra

Cung cấp giao diện theo dõi, quản trị cho quản trị viên, trích xuất những thông tin cần thiết. Mỗi quản trị viên tại các đơn vị chỉ theo dõi được hoạt động của các Agent cài trên đơn vị của mình theo phân quyền. Quản trị viên của hệ thống sẽ có quyền xem dữ liệu toàn bộ Agent trong hệ thống và phân quyền cho quản trị viên tại các đơn vị khác.

2.7. Dịch vụ tường lửa ứng dụng Web

Dịch vụ Web Application Firewall (WAF) được triển khai bảo vệ tăng cường cho các website để phòng chống các cuộc tấn công ở lớp ứng dụng web. WAF được triển khai theo Bridge inline, cho phép bypass luồng dữ liệu khi hệ thống WAF bị sự cố, nhằm đảm bảo khả

năng hoạt động liên tục cho hệ thống.

Dịch vụ tường lửa ứng dụng web (WAF) có các tính năng bảo vệ như sau:

- Cung cấp công nghệ Dynamic Profiling:

+ Cung cấp khả năng tự học ứng dụng và hành vi người dùng, tự động cập nhật các thay đổi hợp lệ của ứng dụng.

+ Hỗ trợ cho các thành phần Web profile: URLs List, URL Patterns, Cookies List, Learned Hosts, Web application user tracking

- Hỗ trợ các phương pháp bảo vệ cookie: cookie injection, cookie tampering, cookie signing, cookie encryption.

- Hỗ trợ chỉnh sửa nội dung: thay đổi nội dung URL, mã hóa và xác nhận cookie.

- Có khả năng "Vá ảo" (Virtual Patching) các lỗ hổng ứng dụng web được WAF phát hiện; có khả năng tích hợp với các hệ thống quét điểm yếu của hãng thứ 3 bao gồm WhiteHat, IBM, Cenzic, NT OBJECTives, Qualys.

- Có khả năng chống lại các tấn công dịch vụ Web, tấn công nhằm vào các ứng dụng XML, SOAP và WSDL.

- Có khả năng kiểm tra sâu các loại kết nối HTTP, HTTPS/SSL. Có khả năng kiểm tra tuân thủ giao thức HTTP để đảm bảo rằng các truy cập Web tuân theo tiêu chuẩn RFC nhằm phát hiện ra các bất thường trong địa chỉ URL và các giao thức.

- Có khả năng chống lại 10 tấn công hàng đầu (Top 10) được liệt kê bởi tổ chức OWASP. Đảm bảo chống lại được toàn bộ các loại tấn công sau:

Anonymous Proxy Vulnerabilities	Illegal Encoding
Brute Force Login	Known Worms
Buffer Overflow	Malicious Encoding
Cookie Injection	Malicious Robots
Cookie Poisoning	OS Command Injection
Corporate Espionage	Parameter Tampering
Credit Card Exposure	Patient Data Disclosure
Cross Site Request Forgery (CSRF)	Phishing Attacks
Cross Site Scripting (XSS)	Remote File Inclusion Attacks
Data Destruction	Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI)
Directory Traversal	Session Hijacking
Drive-by-Downloads	Site Reconnaissance

Forceful Browsing	SQL Injection
Form Field Tampering	Web Scraping
Google Hacking	Web server software and operating system attacks
HTTP Denial of Service	Web Services (XML) attacks
HTTP Response Splitting	Zero Day Web Worms
HTTP Verb Tampering	

- WAF có chức năng tường lửa mức mạng (Stateful Network Firewall).

- Cho phép triển khai theo các mô hình:

+ Inline/Transparent Layer 2 Bridge,

+ Layer 3 Router,

+ Reverse Proxy and Transparent Proxy,

+ Non-inline /sniffer Monitor.

- Cung cấp các cấu hình sẵn sàng cao:

+ Active/Passive, Active/Active

+ Fail open interfaces: cho phép cung cấp dịch vụ không bị gián đoạn khi thiết bị WAF gặp sự cố.

+ Non-inline deployment.

- Cho phép tùy chọn bổ sung dịch vụ "ngăn chặn từ xa":

+ Cho phép giảm nhẹ tấn công tự động trên diện rộng bằng việc sử dụng thông tin về nguồn tấn công đã biết. Cho phép ngăn chặn nhanh chóng và chính xác từ nguồn độc hại trước khi tấn công được thực hiện.

- Giao diện quản lý: Có khả năng quản lý thông qua giao diện Web hoặc dòng lệnh (SSH/console).

- Theo dõi/giám sát: hỗ trợ SNMP, Syslog, gởi email cảnh báo, báo cáo có đồ họa, bảng điều khiển thời gian thực.

- Quản lý log:

+ Có khả năng lưu trữ các loại log sự kiện và tất cả các log giao dịch đi qua WAF.

+ Có khả năng tích hợp với hệ thống SIEM của hãng thứ ba bao gồm ArcSight, RSA enVision, BMC Remedy Service Desk, IBM Qradar.

- Quản lý cấu hình:

+ Có khả năng phân quyền cho nhóm/user với các mức quản trị khác nhau như: quyền quản trị đầy đủ, quyền cấu hình chính sách, quyền chỉ xem…

+ Có khả năng tự động cập nhật các Signature và cài đặt.

(*) Danh sách các tấn công WAF phòng chống được:

STT	WAF
1.	Anonymous Proxy Vulnerabilities
2.	Brute Force Login
3.	Buffer Overflow
4.	Cookie Injection
5.	Cookie Poisoning
6.	Corporate Espionage
7.	Credit Card Exposure
8.	Cross Site Request Forgery (CSRF)
9.	Cross Site Scripting (XSS)
10.	Data Destruction
11.	Directory Traversal
12.	Drive-by-Downloads
13.	Forceful Browsing
14.	Form Field Tampering
15.	Google Hacking
16.	HTTP Denial of Service
17.	HTTP Response Splitting
18.	HTTP Verb Tampering
19.	Illegal Encoding
20.	Known Worms
21.	Malicious Encoding
22.	Malicious Robots
23.	OS Command Injection
24.	Parameter Tampering
25.	Patient Data Disclosure
26.	Phishing Attacks
27.	Remote File Inclusion Attacks
28.	Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI)
29.	Session Hijacking
30.	Site Reconnaissance
31.	SQL Injection
32.	Web Scraping
33.	Web server software and operating system attacks
34.	Web Services (XML) attacks
35.	Zero Day Web Worms

2.8. Dịch vụ cân bằng tải

Dịch vụ cân bằng tải phải sử dụng dòng thiết bị chuyên dụng điều khiển ứng dụng cung cấp giải pháp giúp các ứng dụng được bảo mật hơn, nhanh hơn và luôn luôn sẵn sàng, giúp giảm thiểu chi phí đầu tư và tiết kiệm nhiều chi phí liên quan đến việc ngưng trệ việc cung cấp dịch vụ qua các ứng dụng. Khả năng mở rộng phải linh hoạt và thông minh dựa trên việc tích hợp tối ưu hóa ứng dụng, bảo vệ ứng dụng, hệ thống mạng, và phân phối ứng dụng an toàn, tất cả chỉ trên một nền tảng chung.

Giải pháp thiết kế cung cấp dịch vụ trên nhằm cung cấp khả năng sẵn sàng cao, xuyên

suốt giữa các lớp cho hệ thống Trung tâm dữ liệu: Web Tier, Application Tier, Database tier và sẵn sàng đáp ứng cho khả năng phát triển trong tương lai gần, dễ dàng mở rộng hơn theo nhu cầu.

Một số tính năng dịch vụ

a. Tính sẵn sàng

Để đảm bảo cho tính sẵn sàng cao, hệ thống cân bằng tải phải hỗ trợ cơ chế fail-over và thực hiện việc nhân bản toàn bộ tình trạng các kết nối giữa hai thiết bị cân bằng tải không quan tâm đến việc hệ thống, máy chủ hoặc ứng dụng bị lỗi hoặc chết.

Việc quản trị và cấu hình dựa trên giao diện GUI dễ dàng và logic giúp giảm chi phí quản lý, cấu hình và duy trì thiết bị hoạt động.

Ngoài ra, hệ thống cân bằng tải phải đảm bảo việc tích hợp và tính tương thích cao với các ứng dụng, như Apache, BEA Weblogic, Checkpoint, Citrix, HP, IBM WebSphere, Oracle, Microsoft (Exchange, SQL, Outlook Web Access, SharePoint Portal, SharePoint 2007, 2010, IIS, ISA, etc), Siebel, SAP, PeopleSoft, Mercury Business Availabe Center, Tivoli, RSA SecureID, Sun iPlanet Servers, …

b. Tính năng Advanced Health Checking và cân bằng tải thông minh:

Dịch vụ cân bằng tải giúp chịu tải và phân tải các loại dịch vụ khác nhau cho máy chủ web, nhờ đó giúp cải thiện tốc độ truy cập của người dùng và giúp giảm tải cho máy chủ web, giúp máy chủ web chỉ cần tập trung vào vai trò chính là cung cấp nội dung phục vụ người truy cập. Với khả năng nén, phân tải HTTP thông minh và đưa ra các chính sách khác nhau, Hệ thống cân bằng tải có thể chọn lựa nén và phân tải các loại dữ liệu dựa trên yêu cầu cũng như mức độ cần thiết của người quản trị hệ thống. Tính năng này giúp hệ thống đạt được hiệu suất phục vụ cao hơn trong khi sử dụng ít băng thông hơn cho vấn đề web.

Cùng với tính năng kiểm tra tình trạng sức khỏe (health checking) các hệ thống máy chủ tới mức ứng dụng, như Extended Content Verification (ECV) và Extended Application Verification (EAV) có thể giả lập một gói tin yêu cầu thực tế của người dùng và giám sát tình trạng sẵn sàng của nội dung/ứng dụng cần theo dõi, hệ thống cân bằng tải luôn đảm bảo chuyển các kết nối tới các ứng dụng cũng như dịch vụ của máy chủ nào đang trong tình trạng hoạt động tốt nhất để phục vụ.

c. Cung cấp tính năng Local Traffic Manager (LTM)

Local Traffic Manager (LTM) phân phối dữ liệu các ứng dụng một cách thông minh và hiệu quả cho việc đảm bảo tính an toàn, tối ưu và tin cậy đối với dữ liệu các ứng dụng. Với việc kết hợp việc quản lí các dữ liệu ứng dụng thông minh, cân bằng tải, và các tính năng tối ưu, hệ thống cân bằng tải giúp gia tăng và cải thiện tốc độ xử lí dữ liệu từ lớp 4 tới lớp 7, quản trị dễ dàng, và giúp quản lí các kết nối ở mức ứng dụng.

Triển khai tính năng LTM trong hệ thống mạng cho phép các kết nối có thể được phân tải đều trên nhiều máy chủ, với mỗi kết nối được gửi tới máy chủ dựa trên máy chủ nào đang chịu tải ít nhất. Việc này sẽ giúp các kết nối yêu cầu được xử lí nhanh hơn và giúp cho người dùng cuối sử dụng dịch vụ tốt hơn.

Tính năng LTM phải hỗ trợ nhiều ứng dụng và chịu tải cao: với cấu trúc thiết kế có thể chịu tải nặng cho tất cả các dữ liệu từ lớp 4 tới lớp 7 (theo mô hình OSI), đảm bảo hiệu suất xử lí ở lớp 4, lớp 7, các kết nối SSL và nén HTTP (HTTP Compression), tất cả đều chạy đồng thời. Các kiến trúc này cung cấp tính khả mở rất cao trong việc đưa ra các quyết định

nhờ vào việc hiểu sâu dữ liệu ở lớp 7, giúp cho các ứng dụng được tăng tốc và xử lí nhanh hơn và thống nhất duy nhất trong một thiết bị.

Tính năng LTM làm nhiệm vụ cân bằng tải cho các ứng dụng của nhiều Server như: FTP, HTTP, SharePoint, Oracle Form, ... Tính năng này làm tăng khả năng sẵn sàng cao cho các ứng dụng chạy trên mạng, và nếu như các Server được cân bằng tải đứng phía sau nó có sự cố thì có thể dễ dàng thay thế và nâng cấp. Với khả năng giám sát tới trạng thái và số lượng truy cập của từng ứng dụng. Tính năng LTM cân bằng tải sẽ hiệu quả hơn rất nhiều so với công nghệ clustering thông thường trên máy chủ. Công nghệ clustering chỉ kiểm tra được độ sẵn sàng ở lớp mạng/IP, do đó ứng dụng trên máy chủ có thể đang bị down nhưng request từ người dùng vẫn được forward tới máy chủ này với LTM vấn đề đó đã được giải quyết.

Ngoài tính năng cân bằng tài, LTM còn hỗ trợ tính năng tăng tốc truy cập tới ứng dụng giảm tải load tới máy chủ tăng performance của máy chủ, ngoài ra LTM còn bảo mật cho ứng dụng bằng cách kiểm soát đến từng bite/byte trước khi gửi yêu cầu của người dùng tới ứng dụng.

d. Tính năng Tăng tốc ứng dụng - Application Acceleration Manager (AAM)

AAM đã vượt lên các vấn đề về mạng, giao thức, và các vấn đề ứng dụng để giúp hệ thống đáp ứng hiệu suất ứng dụng, các yêu cầu về sao chép dữ liệu, về khôi phục thảm họa từ điện toán đám mây, ứng dụng di động, và phân phối video. Bằng cách giảm tải mạng và máy chủ. AAM giảm nhu cầu bổ sung băng thông và phần cứng, người dùng có thể truy cập nhanh các ứng dụng, và giải phóng các nguồn lực IT cho các dự án chiến lược khác.

AAM tích hợp các công nghệ tối ưu hóa hiệu suất web và kết nối WAN trong việc phân phối ứng dụng. Điều này cho phép các công nghệ tăng tốc truyền thống như giảm tải SSL, nén, bộ nhớ đệm, và ưu tiên lưu lượng mạng để kết hợp với các công nghệ như tối ưu hóa hình ảnh, tối ưu hóa phân phối video, và chống trùng lắp dữ liệu cấp byte, do đó làm giảm sự phức tạp trong trung tâm dữ liệu.

AAM giúp tối ưu một Website trước khi đáp trả tới các user, nó có khả năng nén và tăng tốc. Trang Web sẽ được nén dưới dạng cấu trúc từ điển HTTP trước khi đến máy của người sử dụng và trình duyệt của máy Client này sẽ tự động giải nén theo cấu trúc dòng lệnh HTTP. Một số file dữ liệu trên trang WEB dạng text: .PPT, .Doc; .xls; .pdf; hoặc dạng ảnh như .jpg .png .gif được nén về định dạng tối ưu. Và tính năng tăng tốc cho WEB sẽ tối ưu các mã lệnh Web dạng ajax, java, php, html, css, java script.

AAM giúp giảm tải ứng dụng từ máy chủ bằng cách giảm tải nhiệm vụ chuyên sâu của CPU (như mã hóa, caching, và nén) và nó có thể làm giảm băng thông bằng cách gửi dữ liệu ít hơn trên mạng. Kết quả cuối cùng là một cơ sở hạ tầng hiệu quả hơn. AAM có thể cải thiện hiệu suất của lưu lượng ứng dụng qua kết nối WAN bằng cách tối ưu hóa các giao thức ứng dụng, ưu tiên traffic, tối ưu hóa TCP từ client đến máy chủ, và làm giảm số lượng dữ liệu được gửi qua mạng WAN, giúp tránh việc nâng cấp băng thông gây tốn kém. Các công nghệ QoS đảm bảo rằng các ứng dụng quan trọng hoặc yêu cầu đáp ứng thời gian được ưu tiên hơn những ứng dụng khác để tối đa hóa hiệu suất qua mạng WAN. Chúng cung cấp điều khiển traffic dựa trên những nhu cầu, cho phép hệ thống quản lý và ưu tiên băng thông cho mỗi ứng dụng và cải thiện QoS cho các ứng dụng quan trọng.

- Tính năng DNS giúp định tuyến dựa trên vị trí địa lý, cung cấp cân bằng tải toàn cầu và chuyển hướng dự phòng.

- Tính năng SSL Orchestrator Tối ưu hóa việc mã hóa và giải mã SSL/TLS, cải thiện hiệu suất và bảo mật của các ứng dụng

- Tính năng Access Policy Manager (APM) giúp quản lý truy cập và danh tính, cung cấp Single Sign-On (SSO), xác thực đa yếu tố và kiểm soát truy cập chi tiết, tích hợp với các dịch vụ xác thực và danh tính bên thứ ba như Active Directory, LDAP, và các dịch vụ đám mây.

2.9. Dịch vụ phòng chống tấn công DDoS

Các tính năng của dịch vụ chống tấn công DDoS:

- Ngăn chặn tấn công, bảo vệ hạ tầng Application khỏi nguy cơ tê liệt hệ thống, khai thác lỗ hổng Application, phân tán Malware, trộm cắp thông tin và các hình thức tấn công khác:

+ Bảo vệ toàn diện khỏi các tấn công khai thác lỗ hổng truyền thống: Worm, Trojan, Bot, SSL-based attack, và VoIP attack …

+ Phát hiện và ngăn chặn các tấn công khai thác lỗ hổng chưa được công bố (zero-day, zero-minute attack) và các tấn công không dựa trên khai thác lỗ hổng (flood, phát tán malware, brute-force…) dựa trên phân tích hành vi.

- Tấn công và hạ tầng Mạng: Tấn công Network Flood

- Tấn công hạ tầng Máy Chủ và Ứng Dụng:

+ Tấn công xâm nhập khai thác lỗ hổng (Intrusion)

+ Tấn công dò tìm mật khẩu (Brute Force)

+ Tấn công HTTP Denial of Service

+ Tấn công HTTP Flood…

- Báo cáo realtime: khi phát hiện tấn công, Traffic Monitoring thể hiện trên giao diện.

- Thông tin về các tấn công bị phát hiện ở thời gian thực.

- Phát hiện và ngăn chặn tấn công DDoS chính xác với thuật toán thông minh giúp đưa ra quyết định chính xác hệ thống có đang bị tấn công, loại bỏ trường hợp nhầm lẫn (như người dùng truy cập thật sự tăng đột biến).

- Quy trình phát hiện và ngăn chặn tấn công khép kín có phản hồi giúp nhanh chóng cô lập thông tin, xác định chính xác các tham số của cuộc tấn công để tạo Realtime Signature cho module ngăn chặn.

Cập nhật tự động bảo vệ, chủ động chống lại các cuộc tấn công DDoS và các mối đe dọa về an ninh hệ thống. Dịch vụ này cung cấp gói cập nhật thường xuyên nhằm nâng cao và duy trì an ninh hệ thống. Cung cấp báo cáo thường xuyên, giúp cho việc tổng hợp, phân tích và đánh giá an ninh và an toàn hệ thống tốt hơn.

- Khả năng bảo vệ mạnh mẽ do có thể nhận dạng được các cuộc tấn công ở lớp 3 (lớp mạng), lớp 4 (lớp vận chuyển) và cả lớp 7 (lớp ứng dụng).

2.10. Dịch vụ phòng chống thất thoát dữ liệu

Dịch vụ phòng chống thất thoát dữ liệu xác định và ngăn chặn các hành vi vi phạm, trích xuất hoặc phá hủy dữ liệu nhạy cảm ngoài ý muốn. Các doanh nghiệp, tổ chức sử dụng dịch vụ này để bảo mật và bảo vệ dữ liệu cũng như tuân thủ các yêu cầu pháp lý.

Mô hình triển khai: Client - Server (Máy trạm và các máy chủ được cài agent phòng chống thất thoát dữ liệu, và được kết nối đến máy chủ quản trị tập trung)

Tính năng Gateway Anti – Malware, hỗ trợ HTTPS

- Ngăn chặn phần mềm độc hại xâm nhập vào hệ thống giảm thiểu gánh nặng cho các giải pháp bảo mật trên endpoint. Tối ưu hóa bảo mật trong một giải pháp duy nhất với nhiều công nghệ khác nhau. Kiểm tra sâu nội dung gói tin, quét các file dữ liệu: PDF, word, excel,… tìm phần mềm độc hại ẩn.
- Ngăn chặn việc download mã độc, virus, spyware… các hành vi của botnet cũng như các kết nối C&C callback ra ngoài Internet. Cô lập các Spyware trước khi chúng có thể phát tán hay chiếm quyền hệ thống
- Kiểm soát các kết nối HTTPS thông qua cơ chế giải mã và kiểm tra nội dung gói tin được mã hóa.

Tính năng Web Reputation kết hợp tương quan dữ liệu thời gian thực

- Ngăn chặn các truy cập vào các trang web độc hại. Smart Protection Network sử dụng thông tin từ 250 triệu sensor trên toàn thế giới, xử lý 16 tỷ query hàng ngày. Bên cạnh cơ sở dữ liệu về những website, URL, domain độc hại, Web Reputation cung cấp cơ chế tính điểm đối với từng website, URL cụ thể để đánh giá mức độ an toàn khi người dùng kết nối tới.
- Cơ chế tương quan các sự kiện cho phép chống lại các mối đe dọa mới và hoạt động đáng ngờ trong thời gian thực.
- Xác định, ngăn chặn botnet và các kết nối C&C trong các cuộc tấn công có chủ đích.

Phân loại và lọc nội dung (URL Filtering)

- Sử dụng cơ sở dữ liệu về URL bao gồm 87 nhóm Website khác nhau giúp chuẩn đoán nội dung và các hoạt động của các website này, phân loại nội dung website được truy cập theo thời gian thực để nhận dạng các trang web không phù hợp hoặc Website độc hại từ đó đưa ra các đề xuất giúp bảo vệ toàn hoạt động của doanh nghiệp.
- Ngăn chặn việc truy cập tới các website giả mạo, tải các phần mềm gián điệp.

Kiểm soát truy cập ứng dụng:

- Liên tục giám sát và báo cáo về hơn 30.000 ứng dụng trên cloud và 1.000 ứng dụng internet khác nhau bao gồm: Office 365, G Suite, Dropbox, ứng dụng instant messaging, peer-to-peer, mạng xã hội, ứng dụng streaming media…
- Quản trị tập trung, xây dựng chính sách chi tiết, linh hoạt để kiểm soát tất cả hoạt động web.
- Thiết lập chính sách bảo mật khác nhau cho từng người dùng, nhóm người dùng hoặc các thành phần web gateway cụ thể.

Cloud Sandboxing và Predictive Machine Learning:

- Cloud sandboxing cung cấp khả năng mô phỏng và phân tích chuyên sâu một cách tự động đối với các tệp đính kèm có khả năng gây hại, bao gồm các file thực thi, file tài liệu… dữ liệu được phân tích trong môi trường sandboxing an toàn trên cloud của Trend Micro. Phương thức này giúp phát hiện chính xác những rủi ro về mã độc liên quan tới các cuộc tấn công có chủ đích.
- Cơ chế Predictive Machine Learning sử dụng các thuật toán thông minh quét các nội dung của đối tượng, mô phỏng và hiểu hành vi của nó, dự đoán ý định. Predictive Machine Learning giúp lọc dữ liệu không an toàn trước khi gửi đến cloud sandboxing. Nó

làm tăng hiệu quả và giảm thiểu thời gian phát hiện, ngăn chặn hiểm họa trong thời gian thực.

Ngăn chặn thất thoát dữ liệu (Cloud DLP):

- Sử dụng trên 240 template liên quan tới DLP để bảo vệ dữ liệu quan trọng, ngăn chặn rò rỉ do vô ý hoặc cố ý của con người.
- Cung cấp giao diện giám sát, quản lý và báo cáo hợp nhất.

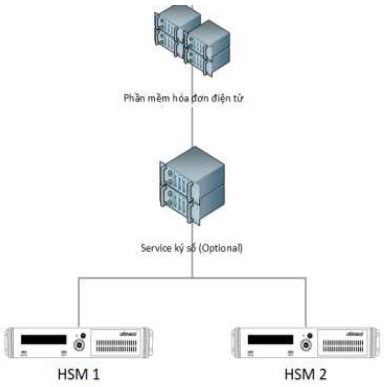
2.11. Dịch vụ giải pháp ký số HSM

2.11.1. Mô hình dịch vụ ký số điện tử

Hệ thống hoá đơn điện tử sẽ gồm 4 thành phần chính:

- Phần mềm hoá đơn điện tử;
- Chứng thư số mua từ các nhà Public CA;
- Thiết bị ký số HSM (Hardware Security Module);
- Web services hỗ trợ kết nối giữa phần mềm/ứng dụng và thiết bị ký số (tuỳ chọn – có thể có hoặc có thể không).

Mô hình triển khai của hệ thống hoá đơn điện tử như sau:



Các thông điệp dữ liệu trao đổi, xử lý giữa hệ thống thu phí hạ tầng cảng biển của UBND TP.HCM và hệ thống khai báo Hải quan được ký chữ ký số và mã hóa theo quy định của pháp luật hiện hành. Thiết bị ký số HSM đặt tại Chi cục Hải quan khu vực II nhằm mục đích ký số trên các giao dịch đối soát dữ liệu tờ khai giữa hệ thống thu phí đặt tại Chi cục Hải quan khu vực II và Cảng vụ.

Mô hình triển khai ký số giao dịch điện tử tại Hải Quan như sau:

2.11.2. Vai trò của thiết bị ký số HSM (Hardware Security Module):

Để đăng ký được chứng thư số mang tính pháp lý của tổ chức/doanh nghiệp, thì cần có một hoặc nhiều khóa bí mật đại diện cho tổ chức/ doanh nghiệp. Sau khi được cấp chứng thư số, thì khoá bí mật này cùng với chứng thư số sẽ được dùng để ký hoá đơn/văn bản/giấy tờ….

Vì vậy, việc lưu trữ và bảo vệ khoá bí mật cùng chứng thư số là yếu tố vô cùng quan trọng đối với tổ chức/doanh nghiệp. Trong trường hợp bị tiết lộ ra bên ngoài, thì có thể gây ảnh hưởng về mặt pháp lý đến tổ chức/doanh nghiệp đó.

Các rủi ro và hạn chế khi lưu trữ và xử lý khóa bí mật trên máy chủ/pc:

- Tiết lộ khóa bí mật do lưu trữ trên đĩa cứng: khóa bí mật sẽ được tạo ra và lưu trữ trên đĩa cứng trong dạng đọc được sẽ dễ dàng bị copy bởi bất kỳ ai từ người dung, người quản trị hệ thống, các phần mềm, mã độc,…
- Tiết lộ khóa bí mật do xử lý trên bộ nhớ RAM: khóa bí mật được tải vào trong RAM để xử lý các thao tác ký sẽ dễ dàng bị đánh cắp bởi các phần mềm, mã độc
- Hiệu năng thấp: máy chủ, pc không được thiết kế để xử lý các thao tác mật mã nên hiệu năng xử lý thấp và ảnh hưởng đến việc xử lý các ứng dụng.
- Khóa bí mật là thành phần chủ chốt để tạo chữ ký số. Do đó nếu nó bị tiết lộ thì chữkýsố sẽ dễ dàng bị giả mạo.

Các lợi ích khi sử dụng thiết bị HSM cho việc ký số:

- Bảo mật tuyệt đối: thiết bị HSM được thiết kế hoàn toàn bảo mật, chống các xâm nhập về phần cứng và phần mềm nên bảo vệ tuyệt đối được khóa bí mật. Tất cả việc lưu trữ và xử lý được thực hiện bên trong thiết bị HSM.
- Hiệu năng cao: được thiết kế chuyên biệt để xử lý các thao tác mật mã nên năng lực xử lý rất cao.
- Tuân thủ các tiêu chuẩn: thiết bị đáp ứng các tiêu chuẩn bảo mật như FIPS 140-2 Level 3, PCI DSS compliance…

2.11.3. Các tính năng của dịch vụ chữ ký số HSM

Cung cấp các tính năng sau đây:

Tính năng	Đặc điểm

Lưu trữ khoá/ chứng thư số	Cho phép người dùng lựa chọn lưu trữ khoá/chứng thư số bên ở bên trong thiết bị hoặc bên ngoài hệ thống dưới dạng file mã hoá.
Số lượng partitions/ slots	Không giới hạn số lượng slots/ partitions
Số lượng kếtnối tới cácserver ứngdụng	Không giới hạn số lượng kết nối. Có thể sử dụng HSM cho nhiều server ứng dụng khác nhau.
Tốc độ ký tối thiểu	Đáp ứng tối thiểu tốc độ ký là **16tps** (với độ dài khoá 2048 bit) có khả năng xử lý được đến **57,600** giao dịch trong vòng 01 giờ

2.12. Dịch vụ sao lưu và phục hồi dữ liệu

- Triển khai theo Công văn 1145/BTTTT-CATTT ngày 03/04/2020 về việc hướng dẫn bộ tiêu chí, chỉ tiêu kỹ thuật để đánh giá và lựa chọn giải pháp nền tảng điện toán đám mây phục vụ Chính phủ điện tử/Chính quyền điện tử) trong đó ở tiêu chí 16.

- Sao lưu/khôi phục máy ảo yêu cầu máy ảo sao lưu ít nhất 07 phiên bản khác nhau và phải khôi phục máy ảo từ bản chụp (snapshot).

- Giải pháp trên đảm bảo tính hiệu quả và để đáp ứng yêu cầu về an toàn dữ liệu, thời gian phục hồi dữ liệu nhanh chóng sau khi có sự cố. Do đó, đề xuất dung lượng lưu trữ dữ liệu backup như sau:

+ Với dịch vụ disk to disk: tính 100% dung lượng của máy chủ.

+ Với dịch vụ disk to tape: tính 100% dung lượng của máy chủ.

2.12.1. Quy trình sao lưu và phục hồi dữ liệu

Trên hệ thống tủ đĩa chính (Primary Storage): Hàng ngày, toàn bộ VM (OS+ ứng dụng) sẽ được snapshot (Full backup) sau 19h:00

Trên hệ thống tủ đĩa phụ (Secondary Storage): Hàng ngày, hệ thống phần mềm sao lưu và phục hồi dữ liệu sẽ sao chép toàn bộ dữ liệu sao chép toàn bộ vùng dữ liệu từ tủ đĩa chín sang tủ đĩa phụ.

Sau đó, hệ thống phần mềm sao lưu và phục hồi dữ liệu thực hiện chuyển dữ liệu tuần tự từ tủ đĩa phụ (Secondary Storage) ra hệ thống tủ đĩa Tape. Mỗi tape LTO8 khoảng 30TB/tape, khi ghi full dữ liệu nhà cung cấp dịch vụ sẽ thay thế tape mới vào và di chuyển các tape đã được sao lưu sang 1 tủ chuyên lưu trữ tape khác (Được tuần hoàn sử dụng lại) và được đặt tại 1 vị trí khác nhằm đảm bảo an toàn dữ liệu.

Vị trí cho tủ đặt Tape phải đảm bảo các yếu tố sau:

Mô tả	
UPS	Có
Máy phát điện	Có
Điều hòa nhiệt độ	Có
Hỗ trợ kỹ thuật	24 x 7 x 365
Hệ thống cảnh báo khói sớm	Có
Hệ thống cảnh báo chống cháy	Có
An ninh (bảo vệ, camera)	Có

2.12.2. Chi tiết quá trình sao lưu được diễn ra như sau:

- Thống nhất danh mục máy chủ và dữ liệu sao lưu (theo hợp đồng)

- Thực hiện sao lưu danh mục máy chủ và dữ liệu theo quy trình backup

- Sau khi sao lưu thành công trên hệ thống thì người quản trị sẽ thực hiện kiểm tra thông tin dữ liệu sao lưu (Nếu một trong hai bước kiểm tra không có trên hệ thống sẽ thực hiện sao lưu lại).

Bươc1: Kiểm tra thông tin bản Primary Snap (ảnh của toàn bộ máy chủ chứa trên vùng lưu trữ đã sao lưu) trên máy chủ quản lý sao lưu.

Bước 2: Kiểm tra thông tin bản Primary Snap hệ thống lưu trữ.

2.12.3. Chi tiết quá trình phục hồi được diễn ra như sau:

- Lệnh phục hồi được chạy trên máy chủ quản lý sao lưu.

- Hệ thống lưu trữ sẽ sử dụng bản Primary Snap đã sao lưu ra một vùng lưu trữ khác.

- Ảnh máy chủ cần phục hồi sẽ được copy và chuyển vào vùng lưu trữ tại máy chủ định sẵn.

- Toàn bộ quá trình thực hiện sẽ thực hiện trên hệ thống lưu trữ.

2.12.4. Mô tả luồng sao lưu dữ liệu:

Bước 1: Sao lưu tại hệ thống primary Storage

Bước 2: Xác định dữ liệu cần backup qua tủ đĩa thứ cấp

Bước 3: Hệ thống chỉ lệnh cho tủ đĩa thứ cấp tạo vùng dữ liệu tương đương hệ thống lưu trữ chính trên vùng lưu trữ thứ cấp

Bước 4: Hệ thống ra chỉ lệnh backup dữ liệu từ tủ đĩa chính sang tủ đĩa thứ cấp.

Bước 5: Hệ thống thực hiện copy dữ liệu đã được lưu trữ trên tủ đĩa thứ cấp ra tape

2.12.5. Tính năng hệ thống

Việc cung cấp vùng lưu trữ để chứa các bản sao dữ liệu backup dựa trên giải pháp lưu trữ 4 Node Cluster với ứng dụng các công nghệ tiên tiến nhất:

- Tổ chức các nodes lưu trữ dữ liệu theo mô hình cluster 6 nodes (có thể mở rộng lên đến 8 nodes trong môi trường SAN) dự phòng chia tải.

- Khả năng mở rộng dung lượng lên đến hàng PB.

- Vận hành 24/7/365.

- Dữ liệu được di chuyển linh hoạt qua lại giữa các nodes lưu trữ. Đáp ứng như cầu nâng cấp mở rộng, bảo trì bảo dưỡng linh hoạt, không làm gián đoạn truy nhập dữ liệu.

- Có sự hỗ trợ xử lý sự cố (nếu có) từ chính hãng trong quá trình vận hành cung cấp dịch vụ.

Giải pháp sao lưu dự phòng từ đĩa sang đĩa sang tape (disk-to-disk-to-tape) được tích hợp trên các tủ đĩa lưu trữ kết hợp với tủ băng từ truyền thống, với khả năng làm đơn giản hóa hoạt động sao lưu dữ liệu dành cho các văn phòng tại chỗ, văn phòng ở xa và bộ phận nội bộ (back office) cũng như có thể hạ thấp yêu cầu về môi trường lưu trữ thứ cấp tới 90% hoặc cao hơn, cung cấp tính năng sao lưu và khôi phục dữ liệu trên đĩa cứng tốc độ cao, được tập trung hóa và có hiệu quả về chi phí.

Môi trường Bảo vệ dữ liệu tích hợp Disk-to-Disk-Tape cung cấp khả năng lựa chọn các giải pháp quản lý sao lưu và khôi phục dữ liệu để đơn giản hóa các quy trình bảo vệ dữ liệu cho một ứng dụng hoặc trên toàn bộ môi trường lưu trữ và môi trường ảo hóa.

Môi trường Bảo vệ dữ liệu tích hợp Disk-to-Disk-Tape giúp đơn giản hóa hoạt động bảo vệ dữ liệu bằng cách tự động hóa các quy trình để cung cấp năng lực quản lý dữ liệu trực quan, ổn định, cho phép lập lịch và tự động hóa hoạt động sao lưu cơ sở dữ liệu, quản lý duy trì bản sao dữ liệu dựa trên chính sách và đơn giản hóa hoạt động chuyển đổi các cơ sở dữ liệu hiện tại sang các hệ thống lưu trữ của . Ngoài ra, hệ thống còn có thể có được các tính năng đảm bảo độ sẵn sàng cao tích hợp, cho phép bạn mở rộng các cơ sở dữ liệu của mình trong môi trường trực tuyến, có thể thực hiện các hoạt động sao lưu dữ liệu ứng dụng đầy đủ, nhất quán của các cơ sở dữ liệu của bạn trong đó chỉ đòi hỏi không gian lưu trữ đủ để lưu trữ phần thay đổi.

Chương trình Agent (client) đọc dữ liệu cần lưu trữ từ các đĩa cứng được gắn trên các web/DB server và gởi chúng trên mạng LAN đến server (server hay còn gọi là Backup server), server ghi/đọc những dữ liệu này và tiếp tục ghi chúng xuống bộ lưu trữ theo đúng các chính sách (policy) đã được định sẵn. Ngoài ra, dữ liệu dùng để quản lý các thông tin về dữ liệu được lưu trữ (metadata) cũng được truyền qua mạng LAN từ các web/DB server đến server và được lưu trữ tại đây.

Quá trình khôi phục lại dữ liệu cũng diễn ra trên cùng đường đi như trên nhưng theo hướng ngược lại: dữ liệu được server đọc lên từ thiết bị lưu trữ nếu dữ liệu đã cũ hoặc đọc dữ liệu trên ổ cứng do quản lý và được truyền đến các web/DB server thông qua mạng LAN, sau đó được ghi lại vào đĩa cứng gắn trên các web/DB server này. Lúc này dữ liệu sẵn sàng để phục vụ cho các ứng dụng.

3. Phương án quy chế đảm bảo an toàn, an ninh thông tin

Ma trận trách nhiệm các bên tham gia vận hành hệ thống:

STT	Nội dung công việc các bên tham gia	Đơn vị sử dụng	Đơn vị cung cấp dịch vụ hạ tầng	Đơn vị cung cấp phần mềm ứng dụng
I	Dịch vụ quản lý về hạ tầng: mạng, lưu trữ, server và ảo hoá.		X	
1	Đảm bảo dịch vụ liên tục, ổn định, an toàn đối với dịch vụ cung cấp 24x7x365		X	
2	Đảm bảo tất cả các SLA về dịch vụ cung cấp đã cam kết với khách hàng		X	
3	Giám sát, quản lý và báo cáo các vi phạm SLA, sự cố trên hạ tầng cloud từ mức hệ điều hành máy chủ ảo trở xuống cho khách		X	
4	Chịu trách nhiệm xử lý sự cố dịch vụ liên quan đến dịch vụ hạ tầng: mạng, lưu trữ, server và ảo hoá		X	

STT	Nội dung công việc các bên tham gia	Đơn vị sử dụng	Đơn vị cung cấp dịch vụ hạ tầng	Đơn vị cung cấp phần mềm ứng dụng
5	Đảm bảo cung cấp đủ tài nguyên hệ thống (resource pool) thực theo yêu cầu của khách hàng		X	
6	Thực hiện các yêu cầu khác của bên sử dụng dịch vụ liên quan đến dịch vụ hạ tầng: mạng, lưu trữ, server và ảo hoá		X	
7	Đảm bảo có đội ngũ chuyên gia thực hiện quản trị vận hành, xử lý sự cố các dịch vụ hạ tầng: mạng, lưu trữ, server và ảo hoá		X	
II	Dịch vụ ATTT			
1	Đảm bảo bản quyền dịch vụ được mua từ hãng hàng năm.		X	
2	Đảm bảo hạ tầng hệ thống cung cấp dịch vụ hoạt động ổn định liên tục.		X	
3	Thiết lập các chính sách bảo mật kiểm soát và ngăn chặn các truy nhập trái phép và tấn công đảm bảo an ninh thông tin cho hệ thống của bên thuê dịch vụ		X	
4	Giám sát, kiểm tra và phân tích log hệ thống các cảnh báo vi phạm chính sách ANTT liên quan đến hệ thống.		X	
5	Cập nhật bản vá, nâng cấp phiên bản mới cho các hệ thống tường lửa theo khuyến cáo của hãng		X	
6	Giám sát tài nguyên, năng lực và tình trạng hoạt động của hệ thống tường lửa và thực hiện nâng cấp hệ thống khi tài nguyên và năng lực xử lý vượt hơn 70%		X	
7	Phối hợp với Bên Thuê dịch vụ, các đơn vị hỗ trợ xử lý khắc phục các lỗi về ANTT, ngăn chặn việc khai thác điểm yếu, lỗ hổng về ANTT đối với hệ thống của Bên Thuê dịch vụ	X	X	
8	Phối hợp với Bên Thuê dịch vụ, các đơn vị hỗ trợ dịch vụ, đơn vị ứng cứu của nhà cung cấp dịch vụ xử lý sự cố khi hệ thống bị tấn công, bị hư hỏng phần cứng.	X	X	X
9	Cung cấp log hệ thống cho Bên Thuê dịch vụ khi có yêu cầu		X	

STT	Nội dung công việc các bên tham gia	Đơn vị sử dụng	Đơn vị cung cấp dịch vụ hạ tầng	Đơn vị cung cấp phần mềm ứng dụng
10	Báo cáo ANTT định kỳ (tuần, tháng, quý, năm)		X	
11	Back up cấu hình của hệ thống khi có thay đổi và định kỳ		X	
12	Thông báo bảo trì và bão dưỡng hệ thống		X	X
13	Phối hợp với các đơn vị liên quan trong quá trình thực hiện bảo trì bảo dưỡng và nâng cấp hạ tầng, hệ thống ứng dụng	X	X	X
14	Yêu cầu và chịu trách nhiệm đối với chính sách tăng cường an ninh cho hệ thống của mình đề nghị nhà cung cấp thực hiện	X		
15	Giám sát và kiểm tra việc thực hiện chính sách, cấu hình của nhà cung cấp dịch vụ đảm bảo an ninh thông tin cho hệ thống của mình	X		
16	Gửi yêu cầu cung cấp log liên quan đến hệ thống của mình. Nếu cung cấp log cho đơn vị thứ 3 thì Bên Thuê dịch vụ phải có văn bản yêu cầu để đảm bảo tính bí mật thông tin mà nhà cung cấp dịch đã cam kết.	X		
17	Chịu trách nhiệm đối với tài khoản quản trị hệ thống mà Bên B cung cấp cho Bên A đảm bảo hệ thống ứng dụng của mình an toàn	X		
II	Dịch vụ quản lý hệ thống thông tin.			
1	Chịu trách nhiệm xử lý sự cố dịch vụ liên quan đến dịch vụ ứng dụng			X
2	Thực hiện các yêu cầu khác của bên sử dụng dịch vụ liên quan đến dịch vụ ứng dụng			X
3	Đảm bảo có đội ngũ chuyên gia thực hiện quản trị vận hành, xử lý sự cố các dịch vụ ứng dụng			X

STT	Nội dung công việc các bên tham gia	Đơn vị sử dụng	Đơn vị cung cấp dịch vụ hạ tầng	Đơn vị cung cấp phần mềm ứng dụng
4	Phối hợp với đơn vị cung cấp dịch vụ hạ tầng thực hiện bảo trì và nâng cấp hệ thống ứng dụng		X	X

Phụ lục:

BIỂU MẪU BÁO CÁO

MẪU 1: MẪU BIÊN BẢN GHI NHẬN VÀ XỬ LÝ SỰ CỐ

…….. CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

…… Độc Lập – Tự Do – Hạnh Phúc

……

Số: …./……..

BIÊN BẢN GHI NHẬN VÀ XỬ LÝ SỰ CỐ

1. Người thông báo sự cố: .....
   - Đại diện công ty: .....
   - Địa chỉ: .....
   - Tel/ Fax: .....
   - Chức vụ: .....
2. Thông báo sự cố lúc: … giờ … phút, ngày … tháng … năm ….
3. Nội dung thông báo sự cố:

   .....

   .....

   .....

4. Người tiếp nhận:.....
5. Tiến hành các bước kiểm tra:

   .....

   .....

   .....

6. Nguyên nhân:

   .....

   .....

   .....

7. Cách khắc phục:

   .....

   .....

   .....

8. Kết quả: Hệ thống hoạt động tốt lúc … giờ … phút, ngày … tháng … năm ….

Biên bản được thành lập 02 bản có giá trị như nhau, mỗi bên giữ 01 bản.

Đại diện kỹ thuật hai Bên cùng xác nhận.

Đại diện Đại diện CĐT

MẪU 2: MẪU BÁO CÁO SỰ CỐ ĐỘT XUẤT

…….. CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

…… Độc Lập – Tự Do – Hạnh Phúc

…….. ……o0o……

BÁO CÁO SỰ CỐ ĐỘT XUẤT

Số: ……

Họ và tên người báo cáo: Đơn vị: Điện thoại: Fax: Thời điểm báo cáo: (hh:mm-dd/mm/yyyy)	Nơi nhận: - Fax: - Fax: - Fax:
Nội dung	
Tên sự cố:	
Thời điểm xuất hiện sự cố (hh:mm-dd/mm/yyyy):	
Thiết bị bị sự cố và sự ảnh hưởng đến hoạt động mạng lưới:	
Mô tả chi tiết sự cố:	
Nguyên nhân sự cố (nếu phát hiện được):	

Các biện pháp khắc phục: Tình trạng hiện tại:
Thời điểm kết thúc sự cố (hh:mm-dd/mm/yyyy) (nếu xử lý xong):
Kiến nghị và đề xuất:

Ý kiến của Lãnh đạo
(Ký và ghi rõ họ tên)

Người báo cáo
(Ký và ghi rõ họ tên)

MẪU 3: MẪU BÁO CÁO HOẠT ĐỘNG HỆ THỐNG

……. CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

…….. Độc Lập – Tự Do – Hạnh Phúc

……. ……o0o……

BÁO CÁO HOẠT ĐỘNG HỆ THỐNG ỨNG DỤNG

Nơi nhận báo cáo:	
Hệ thống	
Người báo cáo	
Ngày báo cáo	...../...../.....
Thời gian	Từ .../... /..... đến ..../...../.....

I. Tình trạng hoạt động

1. Tình trạng hoạt động của hệ thống server:
   Ổn định: Không ổn định:
2. Tình trạng hoạt động của các websites:
   Ổn định: Không ổn định:

II. Những lỗi đã xảy ra – cách khắc phục

1. Hiện tượng lỗi xãy ra: ……
   Cách khắc phục lỗi: ……
   Thời gian xảy ra lỗi: ……. Thời gian kết thúc lỗi: …….
2. Hiện tượng lỗi xãy ra: ……
   Cách khắc phục lỗi: ……
   Thời gian xảy ra lỗi: ……. Thời gian kết thúc lỗi: …….

III. Biện pháp phòng ngừa

1. ……
2. ……

IV. Kiến nghị

1. ……..
2. ……..