Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

Yêu cầu về kỹ thuật mang tính kỹ thuật thuần túy và các yêu cầu khác liên Yêu cầu về kỹ thuật bao gồm các nội dung cơ bản như sau:

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

- Tên chủ đầu tư: Trung tâm Chuyển đổi số - Bộ Dân tộc và Tôn giáo
- Tên nhiệm vụ: Thực hiện "Đề án thuê dịch vụ công nghệ thông tin, đảm bảo an toàn thông tin và kết nối Đề án 06 của Ủy ban Dân tộc năm 2025 theo Quyết định 509/QĐ-UBDT ngày 31/7/2024 của Bộ trưởng, Chủ nhiệm Ủy ban Dân tộc"
- Tên Gói thầu: Gói thầu 1: Thuê dịch vụ công nghệ thông tin, đảm bảo an toàn thông tin và kết nối Đề án 06 của Bộ Dân tộc và Tôn giáo năm 2025.
- Hình thức LCNT: Đấu thầu rộng rãi trong nước qua mạng.
- Phương thức LCNT: Một giai đoạn một túi hồ sơ
- Thời gian tổ chức lựa chọn nhà thầu: 45 ngày
- Thời gian bắt đầu tổ chức LCNT: Quý III, 2025
- Loại hợp đồng: Trọn gói
- Thời gian thực hiện gói thầu: 3 tháng
- Tùy chọn mua thêm: Không áp dụng
- Nguồn vốn: Ngân sách nhà nước
- Địa điểm thực hiện: Trung tâm Chuyển đổi số - Bộ Dân tộc và Tôn giáo, số 349 phố Đội Cấn, phường Ngọc Hà, thành phố Hà Nội.

2. Mục tiêu

- Thuê dịch vụ hạ tầng điện toán đám mây, dịch vụ đảm bảo an toàn thông tin, dịch vụ vận hành hệ thống, dịch vụ kết nối mạng truyền số liệu chuyên dùng, dịch vụ kiểm tra và đánh giá an toàn thông tin để cài đặt, vận hành, giám sát và đáp ứng các yêu cầu đảm bảo an toàn thông tin cấp độ 3.

- Đảm bảo an toàn mạng, đáp ứng các tiêu chuẩn theo hồ sơ cấp độ 3 đối với Hệ thống thông tin giải quyết thủ tục hành chính của BDTTG, đáp ứng công văn số 1552/BTTTT-THH ngày 26/4/2022 của Bộ TTTT về hướng dẫn kỹ thuật triển khai Đề án 06 (phiên bản 1.0); Công văn số 708/BTTTT-CATTT ngày 02/03/2024 của Bộ Thông tin và Truyền thông về việc sửa đổi, thay thế nội dung về an toàn, an ninh mạng tại Công văn số 1552/BTTTT-THH; thông tư 12/2022/TT-BTTTT ngày 12/8/2022 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 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

- Góp phần hoàn thiện tổ chức, triển khai đảm bảo ATTT theo mô hình "4 lớp" theo Chỉ thị số số 09/CT-TTg ngày 23 tháng 02 năm 2024 của Thủ tướng Chính phủ

về việc tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ.

3. Yêu cầu

Việc thuê dịch vụ CNTT sẽ đảm bảo đáp ứng các yêu cầu kỹ thuật để Hệ thống thông tin giải quyết thủ tục hành chính của Bộ Dân tộc và Tôn giáo sớm được vận hành, kết nối với hệ thống Dữ liệu dân cư theo hướng dẫn của văn bản 1552/BTTTT-THH ngày 26/4/2022 của Bộ TTTT về hướng dẫn kỹ thuật triển khai Đề án 06 (phiên bản 1.0); Công văn số 708/BTTTT-CATTT ngày 02/03/2024 của Bộ Thông tin và Truyền thông về việc sửa đổi, thay thế nội dung về an toàn, an ninh mạng tại Công văn số 1552/BTTTT-THH, đồng thời cũng đảm bảo việc vận hành và cung cấp thông tin của Cổng thông tin điện tử của Bộ được vận hành an toàn theo yêu cầu của Thông tư số 22/2023/TT-BTTTT của Bộ Thông tin và Truyền thông Quy định cấu trúc, bố cục, yêu cầu kỹ thuật cho cổng thông tin điện tử và trang thông tin điện tử của cơ quan nhà nước, trong đó Cổng thông tin điện tử phải đáp ứng cấp độ 3.

I. XÁC ĐỊNH SƠ BỘ CÁC MỤC CHÍNH CẦNTHUÊ; MỤC TIÊU, NỘI DUNG, QUY MÔ, PHẠM VI, ĐỊA ĐIỂM VÀ CƠ QUAN, ĐƠN VỊ SỬ DỤNG CÔNG NGHỆ THÔNG TIN

1. Quy mô thuê dịch vụ

Quy mô thuê dịch vụ CNTT để đảm bảo an toàn thông tin, vận hành và kết nối Hệ thống thông tin giải quyết thủ tục hành chính của BDTTG với Đề án 06 và Cổng thông tin điện tử như sau:

- Dịch vụ hạ tầng điện toán đám mây

STT	Server Role	Số lượng	Cấu hình
1	Máy chủ Web	02	CPU: 16vCore; RAM: 32GB Network: 10Gbps Disk - OS :50GB mountpoint - DATA: 100GB
2	Máy chủ tích hợp (Agent)	01	CPU: 08vCore; RAM: 16GB Network: 10Gbps Disk - Disk1(OS): 50GB - Disk2(DATA): 100GB
3	Máy chủ PostgreSQL	02	CPU: 16vCore; RAM: 32GB Network: 1Gbps Disk - Disk1(OS): 50GB - Disk2(DATA): 100GB
4	Máy chủ FrontEnd	02	CPU: 6vCore; RAM 32GB Network: 1Gpbs Disk: 800GB
5	Máy chủ CSDL	02	CPU: 12vCore; RAM 64GB

STT	Server Role	Số lượng	Cấu hình
			Network: 1Gpbs Disk: 2048GB
6	Máy chủ BackEnd	02	CPU: 4vCore; RAM 16GB Network: 1Gpbs Disk: 900GB
7	Máy chủ Transcode	01	CPU: 6vCore; RAM 16GB Network: 1Gpbs Disk: 500GB
8	Máy chủ image	01	CPU: 6vCore; RAM 18GB Network: 1Gpbs Disk: 2048GB

- Dịch vụ đảm bảo an toàn thông tin:

+ Tường lửa tích hợp IPS (Firewall + IPS)

+ Tường lửa ứng dụng web (WAF)

+ Phòng chống tấn công DDoS (Anti-DDoS)

+ Diệt virus (Anti Virus)

+ Chống thất thoát dữ liệu (DLP)

+ Phát hiện và phản hồi các mối nguy hại (EDR)

+ Sao lưu dự phòng tập trung

+ Giám sát ATTT (SOC)

- Vận hành hệ thống thông tin;

- Đường truyền đến mạng truyền số liệu chuyên dùng.

2. Phạm vi thuê dịch vụ

Dịch vụ CNTT được thuê để đảm bảo an toàn thông tin, vận hành và kết nối Hệ thống thông tin giải quyết thủ tục hành chính của BDTTGvới Đề án 06và Cổng thông tin điện tử của BDTTG.

3. Thời gian thuê dịch vụ

Thời gian thuê dịch vụ: 03 tháng.

4. Địa điểm cung cấp dịch vụ

Địa điểm cung cấp dịch vụ: Số 349 phố Đội Cấn, phường Ngọc Hà, Thành phố Hà Nội.

Đơn vị, cơ quan cho thuê dịch vụ, cung cấp dịch vụ: đơn vị/cơ quan có uy tín trên thị trường CNTT và đảm bảo đủ điều kiện kỹ thuật đáp ứng các quy định về an toàn, an ninh mạng theo Công văn 1552/BTTTT-THH, Công văn 708/BTTTT-CATTT, Thông tư 12/2022-TT-BTTTT, Thông tư 22/2023/TT-BTTTT ngày 31 tháng 12 năm 2023, TCVN 11930:2017.

II. XÁC ĐỊNH SƠ BỘ YÊU CẦU VỀ CHẤT LƯỢNG DỊCH VỤ CNTT; SƠ BỘ VỀ YÊU CẦU KỸ THUẬT, CÔNG NGHỆ ĐỂ ĐÁP ỨNG YÊU CẦU CHẤT

LƯỢNG DỊCH VỤ; YÊU CẦU VỀ KHẢ NĂNG KẾT NỐI, LIÊN THÔNGVỚI ỨNG DỤNG, HỆ THỐNG THÔNG TIN KHÁC; CÁC THÔNG SỐ CỦA HỆ THỐNG MÁY CHỦ, ATTT PHỤC VỤ CHO DVC

1. Phân tích lựa chọn giải pháp kỹ thuật và công nghệ

1.1.Các giải pháp công nghệ hạ tầng máy chủ

Điện toán đám mây (Cloud Computing) hay còn gọi là điện toán máy chủ ảo cung cấp các công nghệ, tài nguyên máy tính liên kết với mạng Internet. Với mô hình điện toán đám mây, người dùng sẽ được tiếp cận các tài nguyên từ công nghệ, năng lực tính toán, lưu trữ cơ sở dữ liệu đến từ những nhà cung cấp dịch vụ đám mây.

Điện toán đám mây mang lại rất nhiều lợi ích giúp cho tổ chức, doanh nghiệp tối ưu lại tài nguyên và nhân lực như:

- Tiết kiệm chi phí: Tổ chức, doanh nghiệp chỉ cần trả tiền cho những dịch vụ mà mình sử dụng mà không cần phải bỏ ra các khoản như phí mua thiết bị lắp đặt hệ thống, phí vận hành và duy trì như các máy chủ vật lý hay VPS.
- Sử dụng linh hoạt và dễ mở rộng cơ sở hạ tầng: Người dùng có thể thay đổi tăng hoặc giảm bớt tài nguyên phù hợp với nhu cầu sử dụng của mình.
- Truy cập và sử dụng ở bất cứ mọi nơi: Người dùng có thể truy cập và sử dụng điện toán đám mây ở bất kỳ nơi nào trên thế giới qua internet.
- Tính sẵn sàng cao: Hệ thống điện toán đám mây luôn có cơ chế dự phòng sau lưu dữ liệu nên người dùng có thể nhanh chóng khôi phục dữ liệu khi gặp sự cố trong quá trình sử dụng.
- Độ bảo mật và an toàn cao: Các nhà cung cấp điện toán đám mây sẽ có những trung tâm dữ liệu lớn, hệ thống bảo mật nhiều tầng nên độ an toàn sẽ tốt hơn nhiều so các doanh nghiệp không chuyên về công nghệ.

1.2.Các giải pháp đảm bảo ATTT

Với hệ thống được triển khai trên môi trường điện toán đám mây sẽ dễ dàng tích hợp thêm các phương án, giải pháp bảo đảm an toàn thông tin và mở rộng theo nhu cầu. Các phương án bảo đảm an toàn thông tin sẽ được cung cấp như một dịch vụ, bao gồm một số dịch vụ sau:

- Dịch vụ Cloud Firewall + IPS
- Dịch vụ bảo mật ứng dụng lớp Web
- Phòng chống tấn công DDoS (Anti-DDoS)
- Dịch vụ chống thất thoát dữ liệu (DLP)
- Phần mềm diệt virus (Anti Virus)
- Dịch vụ sao lưu dự phòng tập trung
- Dịch vụ phát hiện và phản hồi các mối nguy hại cho máy chủ (EDR)
- Dịch vụ giám sát ATTT cho hệ thống
- Dịch vụ vận hành hệ thống thông tin

2. Các tiêu chuẩn, quy chuẩn, hướng dẫn kỹ thuật cần đáp ứng

TCVN 11930:2017: Tiêu chuẩn quốc gia về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ (bắt buộc áp dụng).

III. TCVN ISO/IEC 27001:2019: Tiêu chuẩn quốc gia về Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Các yêu cầu.

TCVN ISO/IEC 27002:2020 về Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành Quản lý an toàn thông tin.

TCVN 9801-2:2015 : Tiêu chuẩn quốc gia về Công nghệ thông tin - Các kỹ thuật an toàn mạng - Phần 2: Hướng dẫn thiết kế và triển khai an toàn mạng (ISO/IEC 27033-2:2012).

TCVN 9801-2:2014: Tiêu chuẩn quốc gia về Công nghệ thông tin - Các kỹ thuật an toàn mạng - Phần 3: Các kịch bản kết nối mạng tham chiếu - Nguy cơ, kỹ thuật thiết kế và các vấn đề kiểm soát (ISO/IEC 27033-3:2010).

TCVN 11239:2015: Tiêu chuẩn quốc gia về Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý sự cố an toàn thông tin.

TCVN 27017:2020: Tiêu chuẩn quốc gia về Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành cho biện pháp kiểm soát an toàn thông tin dựa trên ISO/IEC 27002 cho các dịch vụ đám mây.

Văn bản số 761/VPCP-KSTT ngày 29/01/2022 của Văn phòng Chính phủ về việc hướng dẫn kết nối, tích hợp, chia sẻ với CSDLQG về dân cư.

Văn bản số 677/BTTTT-THH ngày 03/3/2022 của Bộ trưởng Bộ Thông tin và Truyền thông về hướng dẫn kết nối và chia sẻ dữ liệu thông qua Nền tảng tích hợp, chia sẻ dữ liệu quốc gia.

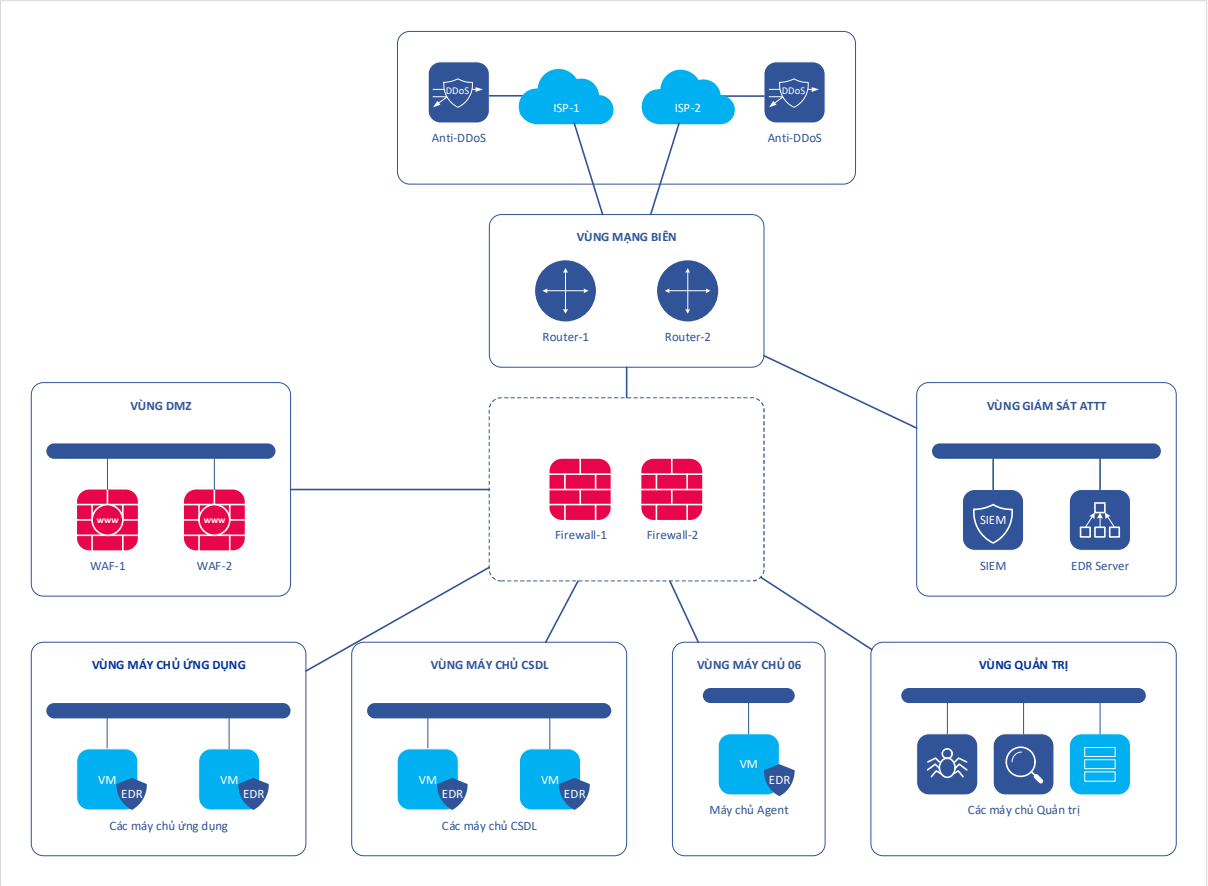
Thông tư 12/2022/TT-BTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Căn cứ theo công văn số 708/BTTTT-CATTT ngày 02/03/2024 của Bộ Thông tin và Truyền thông về việc sửa đổi, thay thế nội dung về an toàn, an ninh mạng tại Công văn số 1552/BTTTT-THH.

Thông tư số 22/2023/TT-BTTT ngày 31/12/2023 của Bộ Thông tin và Truyền thông về việc Quy định cấu trúc, bố cục, yêu cầu kỹ thuật cho Cổng thông tin điện tử và trang tin điện tử của cơ quan nhà nước.

3. Yêu cầu về mô hình triển khai hệ thống

Theo yêu cầu về việc triển khai, kết nối hệ thống hệ thống sẽ được triển khai như sau:



Ở mức tổng quan, kiến trúc hệ thống được chia thành các phân vùng. Mỗi phân vùng/lớp bao gồm nhiều khối với các chức năng nhiệm vụ khác nhau:

Vùng mạng biên (Internet/WAN): Kết nối Internet cung cấp các dịch vụ của dịch vụ công và một cửa điện tử.

Vùng DMZ: Vùng mạng này bao gồm cặp tường lửa ứng dụng web (WAF) để kiểm soát truy cập từ ngoài Internet vào hệ thống bên trong. Mọi luồng dữ liệu đi qua tường lửa được kiểm soát theo chính sách bảo mật định sẵn.

Vùng máy chủ ứng dụng: Bao gồm các máy chủ cài đặt ứng dụng xử lý dữ liệu đầu vào từ lớp web

Vùng máy chủ CSDL: Bao gồm các máy chủ cài đặt và sao lưu phần mềm cơ sở dữ liệu.

Vùng máy chủ 06: máy chủ agent phục vụ kết nối liên thông quốc gia

Vùng mạng quản trị: Chứa các thành phần dùng để quản trị hệ thống. Vùng mạng này bao gồm các máy chủ cài đặt một tập hợp các công cụ quản trị và giám sát toàn bộ các thiết bị mạng, bảo mật, máy chủ trong hệ thống. Các công cụ bao gồm:

- Giải pháp Network Monitoring: Là giải pháp monitor được thiết kế để monitor máy chủ và thiết bị mạng trong hệ thống.

- Giải pháp Anti Virus: là giải pháp phòng chống mã độc tập trung.

- Máy chủ Backup: backup cơ sở dữ liệu từ máy chủ CSDL

Vùng giám sát ATTT

- Giải pháp SIEM: Là giải pháp phần mềm giám sát an ninh mạng dựa trên sức mạnh của việc phân tích Log. Giải pháp thực hiện các công việc tìm kiếm, giám sát và

phân tích dữ liệu logs lớn được sinh ra từ các ứng dụng, các hệ thống và các thiết bị hạ tầng mạng.

- Giải pháp EDR: là giải pháp giám sát, theo dõi và phản ứng lại các nguy cơ gây mất an toàn cho Endpoint.

Danh mục thiết bị cho hệ thống:

STT	Tên thiết bị/ chủng loại	Vị trí triển khai	Mục đích sử dụng
I	**Thiết bị bảo mật**		
1	Firewall-1	Vùng DMZ	Thiết bị tường lửa được thiết lập để quản lý, kiểm soát truy cập vào/ra giữa hệ thống với mạng Internet, mạng WAN
2	Firewall-2	Vùng DMZ	Thiết bị tường lửa được thiết lập để quản lý, kiểm soát truy cập vào/ra giữa hệ thống với mạng Internet, mạng WAN. Dự phòng 1-1 cho Firewall 1
3	WAF-01/ WAF	Vùng DMZ	Thiết bị tường lửa ứng dụng để kiểm soát các kết nối từ ngoài Internet vào trong hệ thống
4	WAF-01/ WAF	Vùng DMZ	Thiết bị tường lửa ứng dụng để kiểm soát các kết nối từ ngoài Internet vào trong hệ thống. Dự phòng 1-1 cho WAF-01
5	AntiVirus/ Windows Server	Vùng quản trị	Thiết bị được cài đặt AV server để kiểm soát thiết bị được cài đặt AV trong hệ thống
II	**Thiết bị máy chủ**		
1	Máy chủ Web 01	Vùng máy chủ ứng dụng	Triển khai ứng dụng Dịch vụ Công
2	Máy chủ Web 02	Vùng máy chủ ứng dụng	Triển khai ứng dụng Dịch vụ Công
3	Máy chủ Agent	Vùng máy chủ 06	Phục vụ kết nối liên thông quốc gia, kết nối tới C06
4	Máy chủ PostgreSQL 01	Vùng Máy chủ CSDL	Chứa các máy chủ CSDL của hệ thống Dịch vụ Công
5	Máy chủ PostgreSQL 02	Vùng Máy chủ CSDL	Chứa các máy chủ CSDL của hệ thống Dịch vụ Công
6	Máy chủ FontEnd 01	Vùng máy chủ ứng dụng	Máy chủ ứng dụng của hệ thống Cổng thông tin.
7	Máy chủ FontEnd 02	Vùng máy chủ ứng dụng	Máy chủ ứng dụng của hệ thống Cổng thông tin.
8	Máy chủ CSDL 01	Vùng Máy chủ CSDL	Chứa các máy chủ CSDL của hệ thống Cổng thông tin.
9	Máy chủ CSDL 02	Vùng Máy chủ CSDL	Chứa các máy chủ CSDL của hệ thống Cổng thông tin.
10	Máy chủ BackEnd 01	Vùng máy chủ ứng dụng	Máy chủ ứng dụng của hệ thống Cổng thông tin.

STT	Tên thiết bị/ chủng loại	Vị trí triển khai	Mục đích sử dụng
11	Máy chủ BackEnd 02	Vùng máy chủ ứng dụng	Máy chủ ứng dụng của hệ thống Cổng thông tin.
12	Máy chủ Transcode	Vùng máy chủ ứng dụng	Máy chủ ứng dụng của hệ thống Cổng thông tin.
13	Máy chủ image	Vùng máy chủ ứng dụng	Máy chủ ứng dụng của hệ thống Cổng thông tin.

1. Yêu cầu đối với dịch vụ hạ tầng điện toán đám mây

Điện toán đám mây cũng giống như nguyên tắc cung cấp máy tính, mạng, thông tin lưu trữ, dịch vụ, nền tảng, ứng dụng cho người dùng có nhu cầu thông qua kết nối mạng. Tất cả các tài nguyên thông tin, dịch vụ và ứng dụng đều đến từ cloud. Cloud này được điều phối bởi phần mềm quản lý và tự động hóa cho các nhóm tài nguyên ảo. Người dùng có thể truy cập (on-site) khi cần thiết thông qua giao diện quản lý. Giao diện được hỗ trợ bởi tính năng tự động thay đổi quy mô và phân bổ tài nguyên rộng, hạ tầng điện toán đám mây được khởi tạo từ một hạ tầng ảo hoá có năng lực xử lý và bảo mật cao. Hạ tầng cần đảm bảo gồm nhiều server vật lý liên kết với nhau, mỗi server (hoặc nhóm server) đóng một chức năng riêng biệt: tính toán, lưu trữ, tường lửa, cân bằng tải, dự phòng, sao lưu dữ liệu…

Dịch vụ hạ tầng điện toán đám mây được thuê cần được thiết kế đểđáp ứng các yêucầu sau:

a) Phải được thiết kế tách riêng, độc lập với các hệ thống khác về lô-gic và có biện pháp quản lý truy cập giữa các hệ thống;

b) Các vùng mạng trong hệ thống phải được thiết kế tách riêng, độc lập với nhau về lô-gic và có biện pháp quản lý truy cập giữa các vùng mạng;

c) Có phân vùng lưu trữ được phân tách độc lập về lô-gic.

d) Cung cấp đủ tài nguyên theo yêu cầu của hệ thống phần mềm Hệ thống thông tin giải quyết thủ tục hành chính.

e) Phân vùng điện toán đám mây phải bảo đảm an toàn hệ thống thông tin theo cấp độ thực hiện theo yêu cầu cơ bản quy định tại Thông tư 12/2022/TT-BTTT, Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - các kỹ thuật an toàn - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ 3, bao gồm thiết lập chính sách, nhân lực, thiết kế, vận hành, quản lý rủi ro, đảm bảo an toàn mạng, máy chủ, ứng dụng, dữ liệu.

Mô hình đảm bảo việc triển khai hệ thống cũng như đảm bảo an toàn thông tin theo cấp độ cũng như đáp ứng các yêu cầu kết nối đến hệ thống CSDL Dân cư Quốc gia do Bộ Công an quản lý.

Căn cứ theo đề xuất số lượng và cấu hình hệ thống máy chủ trong tài liệu thiết kế hệ thống thông tin giải quyết thủ tục hành chính của BDTTG do Văn phòng Bộ vàđơn vị cung cấp, triển khai Hệ thống thông tin giải quyết thủ tục hành chính của Bộ (Công ty CMC), để triển khai Hệ thống thông tin giải quyết thủ tục hành chính và Cổng thông

tin điện tử của BDTTG, hệ thống máy chủ yêu cầu như sau:

STT	ServerRole	Số lượng	Cấu hình
1	Máy chủ Web	02	CPU: 16vCore; RAM: 32GB Network: 10Gbps Disk - OS :50GB mountpoint - DATA: 100GB
2	Máy chủ tích hợp (Agent)	01	CPU: 08vCore; RAM: 16GB Network: 10Gbps Disk - Disk1(OS): 50GB - Disk2(DATA): 100GB
3	Máy chủ PostgreSQL	02	CPU: 16vCore; RAM: 32GB Network: 1Gbps Disk - Disk1(OS): 50GB - Disk2(DATA): 100GB
4	Máy chủ FrontEnd	02	CPU: 6vCore; RAM 32GB Network: 1Gpbs Disk: 800GB
5	Máy chủ CSDL	02	CPU: 12vCore; RAM 64GB Network: 1Gpbs Disk: 2048GB
6	Máy chủ BackEnd	02	CPU: 4vCore; RAM 16GB Network: 1Gpbs Disk: 900GB
7	Máy chủ Transcode	01	CPU: 6vCore; RAM 16GB Network: 1Gpbs Disk: 500GB
8	Máy chủ image	01	CPU: 6vCore; RAM 18GB Network: 1Gpbs Disk: 2048GB

2. Yêu cầu đối với dịch vụ đảm bảo an toàn thông tin

5.1. Các tiêu chí về An toàn thông tin

- Đáp ứng yêu cầu về việc kết nối, tích hợp chia sẻ với CSDLQG về dân cư theo Công văn số 761/VPCP-KSTT ngày 29/01/2022 của Văn phòng Chính phủ về việc hướng dẫn kết nối, tích hợp, chia sẻ với CSDLQG về dân cư, Công văn số 4059/VPCP-KSTT ngày 11/6/2024 của Văn phòng Chính phủ về việc cập nhật lại tài liệu hướng dẫn kết nối, tích hợp, chia sẻ với CSDLQG về dân cư; đồng thời đảm bảo an toàn thông tin cho các máy chủ cho các máy chủ thực hiện kết nối, tích hợp chia sẻ CSDLQG về dân cư theo Công văn số 1834/BCA-C06 ngày 23/5/2024 của Bộ Công an về việc chỉnh sửa hướng dẫn 761/VPCP-KSTT để đảm bảo an toàn thông tin trong việc kết nối, tích hợp, chia sẻ với CSDLQG về dân cư.

-

+Cặp thiết bị này có thể phát hiện và ngăn chặn các tấn công chưa biết và

những hành vi bất thường trên ứng dụng đặc biệt là các website.

+Thiết bị này chống lại các tấn công mức ứng dụng được nêu trong top 10 điểm yếu OWASP như: SQL injection, Cross-Site Scripting (XSS),...

+ Chống được các tấn công tự động như site-scraping, application DDoS,...

- Phương án phòng, chống tấn công mạng cho ứng dụng web: Trang thiết bị tường lửa ứng dụng web được thiết lập để bảo vệ webisite hệ thống dịch vụ công và một cửa điện tử của BDTTG.

- Phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng chính: Các thiết bị network, security, máy chủ đều được thiết kế một cặp để đảm bảo dự phòng cho nhau: như cặp Firewall, cặp WAF, cặp máy chủ ứng dụng, cặp máy chủ CSDL, cặp máy chủ LB làm chức năng cân bằng tải cho ứng dụng

- Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu

-+Máy chủ cơ sở dữ liệu được thiết kế độc lập và tách biệt với các vùng mạng khác trong hệ thống. Chỉ có các máy chủ ứng Đảm bảo hệ thống thông tin được thu thập, đánh giá việc sử dụng thông tin và dịch vụ công trực tuyến theo Công văn số 2278/BTTTT-CĐSQG ngày 12/6/2024 về việc đồng bộ đầy đủ dữ liệu giữa HTTTGQTTHC cấp bộ, cấp tỉnh với Hệ thống giám sát, đo lường mức độ cung cấp và sử dụng dịch vụ Chính phủ số (Hệ thống EMC).

- Đáp ứng yêu cầu về danh mục phương án, thiết bị tối thiểu phục vụ bảo đảm an toàn, an ninh mạng đối với hệ thống thông tin cấp độ 3 để kết nối đến Đề án 06 theo đáp ứng công văn số 1552/BTTTT-THH ngày 26/4/2022 của Bộ TTTT về hướng dẫn kỹ thuật triển khai Đề án 06 (phiên bản 1.0); Công văn số 708/BTTTT-CATTT ngày 02/03/2024 của Bộ Thông tin và Truyền thông về việc sửa đổi, thay thế nội dung về an toàn, an ninh mạng tại Công văn số 1552/BTTTT-THH, Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 Tiêu chuẩn quốc gia TCVN 11930:2017.

Trong đó, tiêu chíkỹ thuật cụ thể về đảm bảo an toàn thông tin:

- Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn: truy cập quản trị hệ thống từ xa, người dùng phải đăng nhập và kết nối qua VPN; người dùng nhập mã pin và passcode đượcgửi đến địa chỉ đã đăng ký (số điện thoại/Mail/…) để thực hiện kết nối VPN.

- Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập: trên cặp Firewall được trang bị cho hệ thống đều được đã cấu hình giải pháp IPS để quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập.

- Phương án phòng, chống tấn công mạng cho ứng dụng web

+Hệ thống được trang bị 01 cặp tường lửa ứng dụng WEB (WAF). Thiết bị được triển khai ở vùng mạng DMZ.

dụng được phép mới được kết nối đến các máy chủ CSDL.

+Các chính sách truy cập được kiểm soát chặt chẽ trên policy của Firewall. Thiết lập cấu hình tường lửa Hệ điều hành máy chủ cơ sở dữ liệu để quản lý truy cập giữa các máy chủ trong cùng một vùng mạng

+Máy chủ CSDL được thiết lập cấu hình tối ưu (hardening) đảm bảo an toàn cho CSDL.

+ Máy chủ CSDL được cài đặt EDR, toàn bộ log, bao gồm cả Audit log được đẩy về SIEM.

+ Trên SIEM có cấu hình các tập luật liên quan đến máy chủ CSDL

- Phương án chặn lọc phần mềm độc hại trên môi trường mạng: Sử dụng phần mềm diệt virus (Anti Virus).

- Phương án phòng chống tấn công từ chối dịch vụ

+Sử dụng chức năng phòng, chống tấn công từ chối dịch vụ được tích hợp trên các thiết bị bảo mật WAF, Firewall: Layer 7 triển khai Web Application Firewall (WAF) giúp lọc và chặn những đợt tấn công có đặc điểm của các cuộc tấn công DDOS ở mức ứng dụng, bảo vệ hệ thống khỏi các mối đe dọa tới các ứng dụng web.

+Sử dụng dịch vụ Anti-DDoS từ 02 ISP khi hệ thống bị tấn công

- Phương án quản lý truy cập lớp mạng

+Toàn bộ hệ thống được triển khai trong một VPC (Virtual Private Cloud) với các subnet tương ứng với VXLAN.

+Các VXLAN của hệ thống hoàn toàn riêng biệt với các hệ thống khác trên Cloud của nhà cung cấp dịch vụ, do đó không có các thiết bị lạ truy cập.

+ Người quản trị hệ thống khi muốn truy cập cần thực hiện VPN, tài khoản VPN này được quản lý

- Phương án giám sát hệ thống thông tin tập trung: Hệ thống sẽ giám sát tình trạng hoạt động của thiết bị như: CPU, RAM,…

- Phương án giám sát hệ thống thông tin tập trung

+Sử dụng giám sát an toàn hệ thống thông tin tập trung SIEM

+Tích hợp log: log Firewall (cảnh báo, và outbound connection, audit logs, IPS,…), log server (thu thập các thông tin security logs, message logs, audit logs), logs WAF (thu thập các logs cảnh báo và access logs từ hệ thống).

- Phương án quản lý sao lưu dự phòng tập trung: hệ thống backup VM ứng dụng/mã nguồn trên Cloud (tự động), các thiết bị máy chủ, mạng được backup định kỳ thường xuyên.

- Phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung: Sử dụng giải pháp Antivirus để phòng chống mã độc trên các máy chủ, có chức năng quản lý tập trung

- Phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung: Toàn bộ các máy chủ, máy trạm trong hệ thống được cài đặt Sản phẩm Antivirus và được quản lý trên hệ thống quản lý tập trung

- Phương án phòng, chống thất thoát dữ liệu: Sử dụng giải pháp phòng chống thất thoát dữ liệu chuyên dụng.

- Phương án duy trì ít nhất 2 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau: sử dụng 02 đường truyền kết nối Internet của 2 nhà mạng

khác nhau, đồng thời kênh truyền đảm bảo có kết nối đa hướng để dự phòng các hướng kết nối cho nhau

5.2. Tính toán yêu cầu về thông số chính của các giải pháp, thiết bị

Để tính toán thông số kỹ thuật của hệ thống đảm bảo an toàn an ninh cho hệ thốngDVC dựa vào tài liệu thiết kế hệ thống thông tin giải quyết thủ tục hành chínhvà sự đánh giá của tổ thẩm định về tài liệu thiết kế hệ thống của đơn vị thường trực CNTT thuộc BDTTG, các tổ tư vấn cho các hệ thống thông tin trên,như sau:

Hệ thống được thiết kế nhằm phục vụ người dùng với các thông số kỹ thuật như sau:

STT	Thông số kỹ thuật	
1	Số lượng người dùng đồng thời của hệ thống	150 người dùng
2	Số lượng phiên làm việc trung bình mà mỗi người dùng thực hiện	1.4 phiên
3	Số lượng trang được mở với mỗi phiên làm việc	4 trang
4	Thời gian truy cập trung bình của người dùng	90 giây

Từ đó tính ra được số lượng bản tin (message) mỗi giây: =150x1.4x4/90=9.3 message/s.

Với tính toán kích thước mỗi bản tin (message) trong tài liệu thiết kế hệ thống như sau:

Dung lượng message	Phân loại message	Trên hệ thống (dự kiến)
Từ 50 KB	Nhỏ	35%
Từ 50 KB đến 1 MB	Trung bình	40%
Từ 1 MB đến 5 MB	Lớn	15%
Trên 5 MB	Rất lớn	10%

Thông lượng của hệ thống để đáp ứng 9.3 message/s:

Dung lượng message	Trên hệ thống (dự kiến)	Thông lượng
Từ 50 KB **(0.4Mb)**	35%	= 9.3 x 35% x 0.4 Mb = **1.3 Mbps**
Từ 50 KB đến 1 MB (Trung bình: 0.5MB **÷4Mb)**	40%	= 9.3 x 40% x 4 Mb = **14.9 Mbps**
Từ 1 MB đến 5 MB **(Trung bình: 2.5MB ÷ 20 Mb)**	15%	= 9.3 x 15% x 20 Mb = **28 Mbps**
Trên 5 MB **(Trung bình: 7MB ÷ 56Mb)**	15%	= 9.3 x 15% x 56 Mb = **52.3 Mbps**
Tổng thông lượng trung bình		**96.5 Mbps**

Căn cứ theo tính toán ở trên, cấu hình các trang thiết bị đảm bảo an toàn an ninh thông tin cần đáp ứng mức thông lượng tối thiểu 100 Mbps. Bên cạnh đó Hệ thống có thể thiết kế để đáp ứng 150 người dùng, trung bình file 25Mb và có khả năng mở rộng,

nâng cấp cấu hình trong tương lai.

Vì vậy cấu hình thiết bị/giải pháp yêu cầu:

5.2.1. Tường lửa tích hợp IPS

STT	Tính năng	
1	**Thông số kỹ thuật**	Yêu cầu tối thiểu
	Thông lượng IPS	100 Mbps
	Thông số NGFW	100 Mbps
	Thông số phần cứng yêu cầu cài đặt	CPU ≥ 1 Core Ram ≥ 2 GB
2	**Tính năng tường lửa cơ bản**	
	Tính năng quản trị	Hỗ trợ quản trị thông qua giao diện web GUI, CLI và Cloud Central
		Hỗ trợ xác thực 2 nhân tố cho truy cập quản trị, kết nối IPSec và SSL VPN.
		Có hỗ trợ trang quản trị cho người dùng cuối User Portal
		Hỗ trợ sao lưu và Phục hồi cấu hình theo theo nhu cầu hàng ngày, hàng tuần, hàng tháng tại local, qua FTP hoặc Email
		Thông báo qua email hoặc SNMP
		Thông báo bản cập nhật mới
		Hỗ trợ tích hợp API của bên thứ 3
		Hỗ trợ đổi tên giao diện
		Hỗ trợ quản trị tập trung Firewall trên nền tảng điện toán đám mây miễn phí
		Cho phép cấu hình chính sách theo nhóm các thiết bị tường lửa
	Kiến trúc xử lý thông minh	Là tường lửa Stateful
		Sử dụng kiến trúc xử lý gói tin thông minh để phát hiện mã độc và bảo vệ hệ thống
		Hỗ trợ giải mã lưu lượng TLS 1.3 mà không hạ bậc giao thức
		Hỗ trợ tăng tốc các lưu lượng đáng tin cậy
	Tính năng mạng	Ngăn chặn các tấn công DoS, DDoS và portscan
		Chặn lưu lượng theo vùng địa lý
		Chính sách theo mạng/người dùng/thời gian/vùng mạng
		Cân bằng tải nhiều đường Internet
		Hỗ trợ giao thức định tuyến tĩnh, multicast (PIM-SM) và động (RIP, BGP, OSPF)
		Hỗ trợ giao thức 802.3ad (LAG)
		Hỗ trợ Jumbo frame
	Tính năng QoS	Giới hạn băng thông theo network, user
	Tính năng VPN cơ bản	Hỗ trợ giao thức VPN site-to-site
		Truy cập từ xa bằng giao thức VPN
		Hỗ trợ Route-based VPN

STT	Tính năng	
		Hỗ trợ khả năng chia tách đường hầm thông minh để định tuyến lưu lượng tối ưu
	Tính năng SD-WAN	Hỗ trợ nhiều kết nối WAN, các tùy chọn bao gồm VDSL, DSL, cáp, LTE/Cellular, và MPLS
		Hỗ trợ chọn đường và định tuyến theo ứng dụng
3	**Network Protection (bảo mật mạng)**	
		Hỗ trợ tích hợp hệ thống chống xâm nhập IPS
		Hỗ trợ phòng chống các mối đe dạo nâng cao
		Chống xâm nhập: theo mẫu dấu hiệu & hỗ trợ tùy chỉnh mẫu dấu hiệu IPS
		Hỗ trợ VPN không cần cài Agent: HTML5 hỗ trợ các giao thức RDP, SSH, Telnet, VNC
4	**Web Protection (Bảo vệ truy cập Web)**	
		Hỗ trợ tích hợp hệ thống chống xâm nhập IPS
		Hỗ trợ phòng chống các mối đe dạo nâng cao
		Chống xâm nhập: theo mẫu dấu hiệu & hỗ trợ tùy chỉnh mẫu dấu hiệu IPS
		Hỗ trợ VPN không cần cài Agent: HTML5 hỗ trợ các giao thức RDP, SSH, Telnet, VNC
		Hỗ trợ quét mã độc trên giao thức HTTP/S, FTP và webmail
		Hỗ trợ cơ sở dữ liệu bộ lọc URL với hơn 92 loại trang web
		Hỗ trợ chính sách định mức truy cập web theo người dùng/nhóm người dùng
		Hỗ trợ Đánh giá mức độ nguy hại của người dùng (UTQ)
		Hỗ trợ Giới hạn băng thông theo ứng dụng, theo danh mục Web
		Hỗ trợ Ngăn chặn các ứng dụng không mong muốn
		Hỗ trợ nhận dạng và định danh các ứng dụng cloud
		Hỗ trợ Quản lý ứng dụng theo category, characteristics, technology, risk level
		Hỗ trợ Quản lý chính sách ứng dụng theo User và Network
5	**Zero-Day Protection (Bảo vệ kỹ thuật hộp cát)**	
		Kiểm tra các tệp thực thi và tài liệu chứa thực thi như (.exe, .com, .dll, .doc, docx, docm, .rtf, pdf)
		Kiểm tra được các định dạng nén, lưu trữ như: zip, bzip, gzip, rar, tar, LHA/LZH, 7Z, Microsoft Cabinet

STT	Tính năng	
		Phân tích hành vi, mạng và phân tích bộ nhớ
		Công nghệ Machine Learning sử dụng Deep learning quét tất cả file thực thi đã bị loại bỏ
		Công nghệ chống khai thác lỗ hổng
		Công nghệ trên hộp cát giám sát ghi tệp. Nếu phát hiện thấy các hành động giống như ransomware, nó sẽ khôi phục các tệp bị ảnh hưởng và ngừng thực thi quy trình được phát hiện
		Xác định hành vi lẩn tránh hộp cát
		Kiểm tra và phân tích tất cả tập tin bất thường bằng tính năng Threat Intelligence

5.2.2. Tường lửa ứng dụng Web (WAF)

STT	Thông số kỹ thuật
1	**Thông số hiệu năng tối thiểu**
	Số lượng kết nối HTTP đồng thời: 150
	Số lượng kết nối HTTPS đồng thời: 150
	Thông lượng HTTP: 100Mbps
	Thông lượng HTTPS: 100Mbps
	vCPU: 1
	RAM: 2GB
	Hỗ trợ các nền tảng Hyper-V, VMware, Xen server, KVM
2	**Tính năng bảo vệ tấn công Web**
	Chống tấn công XSS
	Chống giả mạo yêu cầu liên trang
	Chống lỗ hổng OS command
	Chống tấn công truy cập tập tin máy chủ
	Chống tấn công vét cạn
	Chống cài mã độc trên cơ sở dữ liệu
	Chống đánh cắp lệnh
	Chống tấn công lỗ hổng XXE
	Chống Include Injection
	Công nghệ phát hiện tấn công dựa trên logic (Logic Based Detection Engine COCEP)
	Hỗ trợ virtual patching
	Hỗ trợ mã hóa URL
	Hỗ trợ bảo vệ web socket
	Ngăn chặn dữ liệu kết nối tới Tor Proxy
	Chống LDAP Injection
	Chống Xpath Injection
	Chống tấn công từ chối dịch vụ tầng ứng dụng (Application Level DDoS)
3	**Tính năng bảo mật ứng dụng**
	Chống tấn công đầu độc Cookie
	Kiểm tra IP tin cậy
	Chống liệt kê thư mục

STT	Thông số kỹ thuật
	Hỗ trợ xác thực & quản lý phiên
	Hỗ trợ xử lí lỗi
	Hỗ trợ chống chuyển hướng trang không hợp lệ
	Hỗ trợ lưu trữ dấu vết thiết bị
	Chống tấn công lỗ hổng File Inclusion
	Chống botnet
	Chống truy cập URL không hợp lệ
	Xác thực tuân thủ HTTP
	Chống giả mạo tham số
	Chống lỗi tràn bộ đệm
	Chống upload tập tin độc hại
	Chống thay đổi giao diện website
	Chống tấn công Webshell
	Chống thu thập thông tin web
4	**Tính năng Chống thất thoát dữ liệu**
	Bộ lọc tệp tin riêng tư
	Chọn lọc dữ liệu đầu ra
	Xác minh hợp lệ với thuật toán Luhn
	Bảo mật thông tin nhạy cảm trong logs
5	**Tính năng hỗ trợ SSL/TLS**
	Hỗ trợ SSL Offload
	Hỡ trợ SSL/TLS Cipher control
	Hỗ trợ SSL Profiling
	Hỗ trợ SSL Termination
6	**Tính năng quản lý và báo cáo**
	Hỗ trợ tích hợp các hệ thống SIEM
	Hỗ trợ cá nhân hóa báo cáo, gửi báo cáo tự động qua E-mail, v.v.
	Hỗ trợ báo cáo theo chuẩn PCI-DSS
	Hỗ trợ các định dạng báo cáo PDF, CSV, WORD,…
	Hỗ trợ REST API trên nền web
	Hỗ trợ giám sát SNMP, Syslog và E-mail
	Hỗ trợ đo lưu lượng, bảng giám sát trong thời gian thực
	Quản lý báo cáo
	Hỗ trợ HA Active/Active, Active/Passive Clustering
	Ghi nhật ký và giám sát dựa trên vị trí địa lý
7	**Tính năng kiểm soát**
	Bộ lọc Header của Request
	Lọc IP
	Bộ lọc mở rộng
	Hỗ trợ lọc dữ liệu đầu vào cá nhân
	Chọn lọc Request Header
	Chọn lọc Response Header
	Chọn lọc Request Method
	Chọn lọc nội dung dữ liệu đầu vào
	kiểm soát truy cập URL
	Ngăn chặn theo khu vực địa lí

STT	Thông số kỹ thuật
	URL/HTML/Base64 Deco
8	**Các tính năng nâng cao**
	Hỗ trợ tự chẩn đoán và cảnh báo
	Hỗ trợ tích hợp LDAP/ Active Directory
	Khôi phục dữ liệu dương tính giả (false positive)
	Lưu trữ khóa SSL an toàn
	Hỗ trợ mạng HSM

5.2.3. Phòng chống tấn công DDoS (Anti-DDoS)

TT	Nội dung	Yêu cầu kỹ thuật
1	Phòng chống tấn công từ chối dịch vụ DDoS	Phát hiện và ngăn chặn các loại hình tấn công DDoS Volume-Based. Làm sạch lưu lượng tấn công để trả về lưu lượng sạch cho khách hàng. Chống tấn công volume lớn, lên đến 01Gbps.

5.2.4. Dịch vụ Phần mềm diệt virus (Anti Virus)

TT	Nội dung	Yêu cầu kỹ thuật
1	**Công nghệ phòng chống mã độc**	
	Khả năng bảo vệ	Tự động quét lọc mã độc, bảo vệ máy tính theo thời gian thực
		Công nghệ quét tối ưu, không quét lại các file đã quét trước đó
		Phòng chống giả mạo (anti-phishing)
		Tường lửa bảo vệ máy tính
		Bảo vệ và tự động ngăn chặn quyền truy cập tới thư mục chia sẻ khi phát hiện hành vi mã hóa dữ liệu từ máy tính bị nhiễm mã độc.
		Tạo các khu vực tin cậy (Trust-zone) giúp tăng hiệu suất an ninh và giảm tiêu tốn tài nguyên cho quá trình quét virus
		Phát hiện và ngăn chặn các thiết bị USB nhiễm mã độc thực hiện mô phỏng giả mạo như thiết bị bàn phím. Cho phép người dùng nhập mã số để bàn phím được kết nối theo nhu cầu.
		Tính năng cho phép điều khiển xóa dữ liệu trên máy trạm từ xa trong trường hợp cần thiết
	Kiểm soát ứng dụng:	Quản lý ứng dụng được khởi chạy, ngăn chặn các ứng dụng không mong muốn
		Kiểm soát quyền của ứng dụng được phép truy cập vào hệ thống, giám sát và phân loại ứng dụng
	Kiểm soát thiết bị ngoại vi	Kiểm soát theo công nghệ truyền dữ liệu/bus kết nối (ổ cứng, thiết bị lưu trữ gắn ngoài, máy in, ổ đĩa CD/DVD, …)
		Có khả năng ghi lại báo cáo, theo dõi các hoạt động của tập tin được tạo, xóa trên thiết bị lưu trữ di động
	Kiểm soát truy cập web	Thiết lập chính sách hạn chế truy cập web, ngăn chặn việc truy cập các trang web không mong muốn, kiểm soát việc truy cập theo danh mục website, theo loại dữ liệu hoặc địa chỉ web chỉ định
		Kiểm soát linh hoạt theo nhóm người dùng, theo lịch tùy chọn
	Khả năng	Hỗ trợ mã hóa mức Full disk và file-level

TT	Nội dung	Yêu cầu kỹ thuật
	mã hóa dữ liệu	Module phục vụ tính năng mã hóa được tích hợp mà không cài thêm phần mềm mã hóa riêng biệt
	Khả năng dò quét và vá lỗ hổng	Khả năng dò quét và vá lỗ hổng hệ điều hành, ứng dụng trên máy tính người dùng thông qua thành phần quản trị tập trung (Vulnerability and Patch Management)
	Ngôn ngữ hỗ trợ	Hỗ trợ giao diện tiếng Anh và giao diện tiếng Việt
	Nền tảng hỗ trợ bảo vệ	Hỗ trợ các hệ điều hành máy chủ: Windows Server 2016, 2019, 2022; Linux
2	**Khả năng quản trị tập trung**	
	Tính năng quản trị	Giám sát và báo cáo tập trung từ công cụ quản trị, cung cấp thông tin tổng quan và các số liệu thống kê trạng thái bảo vệ của hệ thống
		Phần mềm kết nối tương tác giữa máy chủ quản trị và các thiết bị hoạt động riêng
		Cho phép cài đặt từ xa phần mềm diệt virus từ công cụ quản trị
		Hỗ trợ quản lý, cài đặt từ xa phần mềm của hãng khác trên công cụ quản trị
		Tự động kích hoạt chính sách bảo vệ nâng cao khi bùng phát mã độc. Chính sách này được thiết lập riêng so với chính sách hiện hành
		Có cơ chế Out-of-Office cho phép thực thi một chính sách bảo vệ phù hợp khi người sử dụng mang máy tính ra khỏi mạng công ty
		Thực thi tác vụ rà soát lỗ hổng bảo mật trên hệ thống, có báo cáo cung cấp danh sách các lỗ hổng bảo mật được phát hiện và các bản cập nhật cho phần mềm của bên thứ ba được cài đặt trên các máy tính.
		Khả năng thiết lập mô hình quản lý phân cấp Primary Manager/ secondary Manager
		Hỗ trợ đồng thời cả giao diện quản lý Web Console và MMC-based console. Có cơ chế xác thực hai bước để tăng cường bảo mật.
		Cho phép tùy chỉnh, trích xuất lưu trữ các báo cáo theo các định dạng XML, HTML, PDF
	Nền tảng hỗ trợ triển khai thành phần quản trị tập trung	Hỗ trợ triển khai máy chủ quản trị theo chế độ cluster, đảm bảo tính sẵn sàng cao cho máy chủ.
		Quản trị tập trung hỗ trợ các cơ sở dữ liệu: Microsoft SQL, MySQL hoặc cơ sở dữ liệu quan hệ tương đương

5.2.5. Dịch vụ phòng chống thất thoát dữ liệu (DLP)

STT	Yêu cầu kỹ thuật
1	**Chống thất thoát dữ liệu (Data Loss Prevention - DLP)**
	Giải pháp cho phép thiết lập, quản lý chính sách tập trung.
	Thành phần quản lý hỗ trợ quản trị thông qua giao diện Web hoặc GUI

STT	Yêu cầu kỹ thuật
	Có khả năng phát hiện các loại tệp tin đa dạng, cho phép nhận dạng và phát hiện tối thiểu 500 loại tệp tin khác nhau
	Hỗ trợ kiểm soát dữ liệu qua các kênh như: Cloud, Email, Web…
	Báo cáo các sự kiện vi phạm
	Hỗ trợ tính năng phân quyền truy cập cho người dùng
	Khả năng tích hợp hệ thống domain (Active Directory)
	Giải pháp cho phép ẩn tiến trình và dịch vụ hoặc thiết lập mật khẩu phần mềm DLP nhằm ngăn chặn can thiệp vào phần mềm
	Hỗ trợ xuất báo cáo ra tối thiểu 01 loại định dạng sau: CSV, XML, PDF, XLSX, HTML
	Nền tảng cơ sở dữ liệu hỗ trợ Microsoft SQL hoặc PostgreSQL hoặc tương đương
	Nền tảng Endpoint hỗ trợ phổ biến như: Windows 10/11; Windows Server 2016, 2019; Ubuntu
2	**Chống thất thoát dữ liệu qua thiết bị ngoại vi**
	Kiểm soát các thiết bị ngoại vi ngăn chặn thất thoát dữ liệu
	Kiểm soát dữ liệu nhạy cảm thông qua in ấn
	Hỗ trợ mã hóa dữ liệu file khi sao chép ra thiết bị ngoại vi
	Hỗ trợ kiểm soát thiết bị ngoại vi, gồm các kiểu kết nối như: USB, LPT/COM Port, FDD, DVD/CD, PCMCIA, IrDA, Modem, Máy in, HDD, Các ổ cứng ngoài khác, Tape drives, FireWire
3	**Chống thất thoát dữ liệu qua mạng**
	Hỗ trợ kiểm soát thất thoát dữ liệu qua Email
	Hỗ trợ kiểm soát dữ liệu qua kênh qua Web: HTTP/HTTPS và FTP
	Hỗ trợ kiểm soát dữ liệu sử dụng trên nền tảng Cloud như: OneDrive, Office 365, DropBox, WeTransfer, Box.com, Google Drive, Google Docs
4	**Tính năng khám phá, phân loại dữ liệu**
	Hỗ trợ phát hiện dữ liệu nhạy cảm lưu trữ không đúng cách
	Giải pháp trang bị hoặc cho phép tích hợp nhiều công nghệ khác nhau để phát hiện dữ liệu nhạy cảm, tối thiểu hỗ trợ 03 công nghệ sau: Machine learning, từ khóa, từ điển, fingerprints, OCR, AI-based image templates
	Hỗ trợ cảnh báo đến người dùng và quản trị viên bảo mật

5.2.6. Dịch vụ phát hiện và phản hồi các mối nguy hại (EDR)

STT	Yêu cầu kỹ thuật	
1	Nền tảng hoạt động	Windows Server 2016, Windows Server 2019,Windows Server 2022; Ubuntu 18/20/22, RHEL8/9, Oracle 7/8
		Danh sách ứng dụng được phép hoạt động
		Bảo mật truy cập web, độ tin cậy khi download.
		Kiểm soát web / ngăn chặn URL theo danh mục.
		Kiểm soát thiết bị ngoại vi (USB…)
		Kiểm soát ứng dụng
2	Ngăn chặn trước khi mã độc hoạt động	Phát hiện phần mềm độc hại bằng công nghệ Deep Learning
		Quét tập tin để ngăn chặn mã độc.
		Bảo vệ thời gian thực.
		Phân tích hành vi trước khi thực thi tập tin (HIPS).

STT	Yêu cầu kỹ thuật	
		Ngăn chặn ứng dụng tiềm tàng không mong muốn (PUA).
3	Ngăn chặn mối nguy không mong muốn	Chống thất thoát dữ liệu (DLP)
		Ngăn chặn các kỹ thuật khai thác lỗ hổng: tối thiểu 20 kỹ thuật tấn công khai thác lỗ hổng.
		Phân tích hành vi hoạt động theo thời gian chạy (HIPS)
		Giảm thiểu hoạt động nguy hại (Active Adversary Mitigations) + Credential Theft Protection +Code Cave Mitigation +Man-in-the-Browser Protection (Safe Browsing) +Malicious Traffic Detection + Meterpreter Shell Detection
		Khóa ứng dụng tăng cường: + Web Browsers + Web Browser Plugins + Java + Media Applications + Offce Applications
		Bảo vệ tấn công Man-in-the-Brower
		Bảo vệ bản ghi khởi động và ổ đĩa
		Ngăn chặn Ransomware + Ransomware File Protection + Automatic file recovery + Disk and Boot Record Protection
4	Tính năng phát hiện và điều tra hành vi mã độc	Tìm kiếm mối đe dọa trực tiếp (giúp săn tìm mối đe dọa, duy trì và cải thiện hệ thống bảo mật CNTT)
		Thư viện truy vấn SQL giúp săn tìm mối nguy hại (các truy vấn được viết sẵn, hoàn toàn có thể tùy chỉnh), có thể đặt lịch truy vấn
		Truy cập nhanh, lưu trữ dữ liệu trên đĩa cục bộ (lên đến 90 ngày)
		Truy cập chéo các nguồn dữ liệu từ các hệ thống máy tính, tường lửa, email
		Lưu trữ đám mây Data Lake
5	Tính năng điều tra	Phân tích nguyên nhân (Root Case) với các mối đe dọa (Threat Case)
		Phân tích mã độc với công nghệ Deep learning chuyên sâu
		Phân tích Threat Intelligence nâng cao theo yêu cầu
		Xuất dữ liệu điều tra Forensic
		Điều tra sử dụng AI
6	Tính năng khắc phục sự cố	Loại bỏ phần mềm độc hại tự động
		Đồng bộ bảo mật với thiết bị tường lửa cùng hãng
		Làm sạch mã độc
		Khả năng phản hồi trực tiếp (điều tra từ xa và thực hiện phản hồi)
		Cách ly máy chủ theo yêu cầu
		Loại bỏ và ngăn chặn nhanh bằng 1 cú click chuột
7	Điều khiển	Cập nhật cache và chuyển tiếp gói tin
		Tự động loại trừ vùng quét

STT	Yêu cầu kỹ thuật	
		Giám sát tính toàn vẹn của tệp tin

5.2.7. Dịch vụ sao lưu dự phòng tập trung

STT	Tính năng	
1	Sao lưu dự phòng tập trung	- Gói 2TB lưu trữ tập trung

5.2.8. Dịch vụ giám sát ATTT (SOC)

STT	Tính năng
1	+ Thu thập và quản lý log theo thời gian thực: từ các thiết bị mạng, thiết bị an ninh mạng, các dịch vụ mạng, các máy chủ và các thiết bị đầu cuối. Hệ thống tự động chuẩn hóa các dạng log khác nhau. + Phát hiện tấn công mạng nhanh chóng: Hệ thống có thể phát hiện tấn mạng dựa trên phân tích log, truy vấn tên miền độc hại, kết nối tới các địa chỉ IP độc hại… + Xử lý phân tích tương quan: Cho phép thiết lập các luật nhằm tự động phân tích tương quan nhiều nguồn log khác nhau + Tích hợp Vulnerability management: Tích hợp chức năng quản lý điểm yếu ATTT, tự động cảnh báo khi phát hiện điểm yếu ATTT. + Cảnh báo và tự động ngăn chặn tấn công mạng: Tự động cảnh báo tấn công mạng. + Điều tra và phân tích sự cố: Hệ thống hỗ trợ điều tra và phân tích log mức sâu theo từng trường thông tin, điều tra sự cố thông qua giao diện tương quan.

3. Yêu cầu đối với dịch vụ vận hành hệ thống

Giám sát 24/7 và vận hành, đảm bảo hoạt động của hạ tầng thuê, bao gồm các máy chủ, thiết bị an toàn thông tin và các giải pháp đi kèm:

- 02 Máy chủ web
- 01 Máy chủ tích hợp (Agent)
- 02 Máy chủ PostgreSQL
- 02 Máy chủ Fontend
- 02 Máy chủ Backend
- 02 Máy chủ CSDL
- 01 Máy chủ Transcode
- 01 Máy chủ Image

Trách nhiệm của nhà cung cấp dịch vụ vận hành:

- Bố trí các nhân sự có chuyên môn trong lĩnh vực điện toán đám mây và an toàn thông tin phù hợp, đảm bảo tính an toàn, tính sẵn sàng, tính khả dụng 24/7 của hệ thống thông tin trong suốt quá trình thuê dịch vụ.

- Đảm bảo tính bảo mật, vẹn toàn và tính khả dụng của thông tin trong suốt quá trình thuê dịch vụ.

- Có quy trình vận hành, giám sát, xử lý sự cố hệ thống thông tin đảm khả năng vận hành an toàn và xuyên suốt.

- Sẵn sàng hỗ trợ kỹ thuật phục vụ việc bảo trì, tích hợp dịch vụ đối với các phần phần mềm của đơn vị thuê dịch vụ.

- Thực hiện các báo cáo định kỳ về tình trạng hoạt động của hệ thống, các thay đổi hoặc sự cố xảy ra đối với các thiết bị trong quá trình vận hành.

- Nhật ký giám sát hệ thống phải được lưu trữ toàn bộ trong thời gian thuê dịch vụ.

- Bàn giao toàn bộ dữ liệu cho đơn vị thuê dịch vụ khi hợp đồng chấm dứt.

4. Yêu cầu đối với dịch vụ đường truyền kết nối tới mạng truyền số liệu chuyên dùng

Đáp ứng các yêu cầu của Công văn số 1552/BTTTT-THH ngày 26/4/2022 của Bộ TTTT về hướng dẫn kỹ thuật triển khai Đề án 06 (phiên bản 1.0); Công văn số 708/BTTTT-CATTT ngày 02/03/2024 của Bộ Thông tin và Truyền thông về việc sửa đổi, thay thế nội dung về an toàn, an ninh mạng tại Công văn số 1552/BTTTT-THH.

Đáp ứng yêu cầu của Công văn số 273/BTTTT-CBĐTW ngày 31/01/2020 V/v hướng dẫn mô hình tham chiếu về kết nối mạng cho bộ, ngành, địa phương.

Cung cấp đủ băng thông đường truyền theo yêu cầu của Hệ thống thông tin giải quyết thủ tục hành chính.

5. Xác định yêu cầu về khả năng kết nối, liên thông với ứng dụng, hệ thống thông tin khác

Hệ thống dịch vụ CNTT được thuê cần có khả năng kết nối Hệ thống thông tin giải quyết thủ tục hành chính của BDTTGvới Đề án 06 nhằm tích hợp, chia sẻ dữ liệu đối với CSDLQG về dân cư, Hệ thống định danh và xác thực điện tử.

6. Xác định yêu cầu về công tác vận hành thử trước khi đưa dịch vụ vào khai thác và sử dụng.

Hệ thống dịch vụ CNTT sẽ được vận hành thử (nếu có) trước khi đưa vào vận hành và khai thác sử dụng. Mọi công việc và chi phí vận hành thử sẽ do Đơn vị cung cấp dịch vụ đảm nhận theo đúng qui định hướng dẫn hiện hành.

4. GIẢI PHÁP VÀ PHƯƠNG PHÁP LUẬN

Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Chương này, gồm các phần như sau:

1. Giải pháp và phương pháp luận;

2. Kế hoạch công tác.

5. QUY ĐỊNH VỀ KIỂM TRA, NGHIỆM THU SẢN PHẨM :

Chủ đầu tư phối hợp với nhà thầu thực hiện kiểm tra, nghiệm thu chất lượng theo trình tự và nguyên tắc sau:

- Kiểm tra và nghiệm thu khối lượng các dịch vụ mà nhà thầu cung cấp;
- Kiểm tra, đánh giá chất lượng các dịch vụ nhà thầu cung cấp;
- Xác định giá trị khối lượng công việc hoàn thành của nhà thầu thực hiện.