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

## Mục 1. Yêu cầu về kỹ thuật

### *1.1. Giới thiệu chung về dự án, gói thầu*

#### *1.1.1. Giới thiệu về dự án*

- **Tên dự án:** Thiết bị an ninh mạng IPS/IDS và firewall.

- **Địa điểm đầu tư:** Tổng công ty Quản lý bay Việt Nam

- **Người quyết định đầu tư:** Hội đồng thành viên Tổng công ty Quản lý bay Việt Nam.

- **Chủ đầu tư:** Trung tâm Thông báo tin tức hàng không.

- **Nguồn vốn đầu tư:** Vốn của Tổng công ty Quản lý bay Việt Nam.

- **Thời gian thực hiện dự án**: 16 tháng (từ tháng 12/2025 đến tháng 3/2027)

- **Quy mô đầu tư:**

Quy mô đầu tư hệ thống an toàn thông tin được xác định dựa trên cấp độ bảo mật (3 hoặc 4), tầm quan trọng của từng hệ thống điều hành bay và khả năng mở rộng, tuân thủ pháp luật.

Dự án hướng tới kết hợp giữa đầu tư chiều sâu, công nghệ hiện đại và chuyên gia thuê ngoài, nhằm xây dựng môi trường mạng an toàn, tin cậy, sẵn sàng ứng phó với rủi ro an ninh mạng.

Các giải pháp phải tuân thủ tiêu chuẩn ISO/IEC 27001, 27005, hướng dẫn của Bộ TT&TT, Cục ATTT và ICAO, đồng thời bảo đảm tính đồng bộ, tích hợp và tương thích với hệ thống hiện hữu.

Hệ thống cần dễ nâng cấp, có khả năng mở rộng trong 5-10 năm tới, ưu tiên đầu tư tập trung vào các hệ thống lõi quan trọng để tối ưu chi phí và nâng cao hiệu quả vận hành.

Danh mục vật tư, thiết bị và các phần mềm, giải pháp cần thiết đầu tư mới như sau:

| STT | Danh mục | Đơn vị tính | Số lượng |
|---|---|---|---|
| **A** | **Hệ thống trang thiết bị IPS/IDS/APT và Firewall** | | |
| **I** | **Thiết bị mạng** | | |
| 1 | Thiết bị chuyển mạch cho hệ thống thông tin cấp độ 4 | Thiết bị | 8 |
| 2 | Thiết bị chuyển mạch cho hệ thống thông tin cấp độ 3 | Thiết bị | 6 |
| **II** | **Thiết bị bảo mật** | | |

| | | | |
|---|---|---|---|
| 1 | Thiết bị tường lửa vùng lõi cho hệ thống thông tin cấp độ 4 | Thiết bị | 8 |
| 2 | Thiết bị tường lửa vùng biên cho hệ thống thông tin cấp độ 4 | Thiết bị | 4 |
| 3 | Thiết bị tường lửa cho hệ thống thông tin cấp độ 3 | Thiết bị | 6 |
| 4 | Thiết bị tường lửa cho ứng dụng Web | Thiết bị | 2 |
| 5 | Bản quyền thông lượng WAF (WAF Throughput) | Bộ | 1 |
| **III** | **Hệ thống thiết bị phân tích phát hiện các mối nguy an ninh mạng (IDS/APT)** | | |
| 1 | Thiết bị gom lưu lượng mạng | Thiết bị | 4 |
| 2 | Thiết bị phân tích trung tâm | Thiết bị | 4 |
| 3 | Thiết bị cảm biến trung tâm | Thiết bị | 4 |
| 4 | Thiết bị phân tích mã độc Sandbox | Thiết bị | 4 |
| **IV** | **Phần mềm phân tích phát hiện các mối nguy an ninh mạng (IDS/APT)** | | |
| 1 | Bản quyền cho Hệ thống Phân tích, phát hiện các mối nguy an ninh mạng tại trung tâm chính | Bộ | 1 |
| 2 | Bản quyền cho Hệ thống Phân tích, phát hiện các mối nguy an ninh mạng tại Đài KSKL | Bộ | 1 |
| 3 | Phân tích, phát hiện các mối nguy an ninh mạng - Cảm biến ảo hóa | Bộ | 4 |
| **B** | **Hệ thống quản lý giám sát vận hành** | | |
| **I** | **Hệ thống thiết bị phần cứng phục vụ giám sát, hỗ trợ vận hành** | | |
| 1 | Máy tính quản trị giám sát vận hành | Thiết bị | 4 |
| 2 | Màn hình giám sát | Thiết bị | 4 |
| 3 | Thiết bị chuyển mạch quản lý | Thiết bị | 7 |
| 4 | Máy chủ quản lý giám sát | Thiết bị | 9 |
| 5 | Phụ kiện triển khai | Gói | 4 |
| **II** | **Phần mềm thương mại phục vụ công tác giám sát, hỗ trợ vận hành** | | |
| 1 | Phần mềm Quản lý giám sát mạng (NMS) | Gói | 1 |
| 2 | Phần mềm quản trị CSDL | Bộ | 4 |
| 3 | Hệ điều hành máy chủ quản lý giám sát | Bộ | 9 |
| **C** | **Thiết bị dự phòng** | | |
| 1 | Thiết bị chuyển mạch cho hệ thống thông tin cấp độ 4 (có thể dùng cho HTTT cấp độ 3 nếu cần) | Thiết bị | 3 |
| 2 | Thiết bị chuyển mạch quản lý | Thiết bị | 4 |

| | | | |
|---|---|---|---|
| 3 | Thiết bị tường lửa vùng lõi cho hệ thống thông tin cấp độ 4 (có thể dùng cho vùng biên nếu cần) | Thiết bị | 3 |
| 4 | Thiết bị tường lửa cho hệ thống thông tin cấp độ 3 | Thiết bị | 3 |
| 5 | Thiết bị tường lửa cho ứng dụng Web | Thiết bị | 1 |
| 6 | Máy chủ quản lý giám sát | Thiết bị | 2 |
| 7 | Máy tính quản trị giám sát vận hành | Thiết bị | 2 |
| 8 | Màn hình giám sát | Thiết bị | 2 |

### *1.1.2. Giới thiệu về gói thầu*

**Dự án bao gồm 01 gói thầu:**

- **Tên gói thầu:** Cung cấp thiết bị an ninh mạng IPS/IDS và Firewall
- **Thời gian bắt đầu tổ chức lựa chọn nhà thầu**: Tháng 12/2025
- **Hình thức lực chọn nhà thầu:** Đấu thầu rộng rãi qua mạng trong nước.
- **Phương thức lựa chọn nhà thầu:** Một giai đoạn một túi hồ sơ.
- **Thời gian thực hiện gói thầu:** 10 tháng
- **Loại hợp đồng:** Trọn gói.
- **Địa điểm thực hiện:**

| STT | Tên đơn vị sử dụng | Địa điểm |
|---|---|---|
| 1 | Trung tâm Thông báo tin tức hàng không | Số 5, ngõ 200, đường Nguyễn Sơn, phường Bồ Đề, Thành phố Hà Nội |
| 2 | Công ty Quản lý bay Miền Bắc | Số 5, ngõ 200 đường Nguyễn Sơn, phường Bồ Đề, Thành phố Hà Nội |
| 3 | Công ty Quản lý bay Miền Trung | Số 148 Duy Tân, phường Hòa Cường, Thành phố Đà Nẵng |
| 4 | Công ty Quản lý bay Miền Nam | Số 22 đường Trần Quốc Hoàn, Phường Tân Sơn Nhất, Thành phố Hồ Chí Minh |

### *1.1.3. Mục tiêu*

#### *1.1.3.1. Mục tiêu chung*

Dự án được Tổng công ty Quản lý bay Việt Nam (VATM) triển khai nhằm tăng cường năng lực phòng vệ và bảo vệ hệ thống thông tin điều hành bay - lĩnh vực có ảnh hưởng trực tiếp đến an toàn quốc gia.

Mục tiêu của dự án là trang bị đồng bộ các thiết bị và giải pháp an ninh mạng như Firewall, IDS/IPS, Web Application Firewall (WAF), cùng các phần mềm giám sát, phân tích và phát hiện mối nguy, đáp ứng đầy đủ quy định bảo đảm an toàn thông tin theo cấp độ 3 và 4 theo Nghị định số 85/2016/NĐ-CP ngày

01/7/2016 và Thông tư 12/2022/TT-BTTTT ngày 12/8/2022.

Dự án hướng đến chuẩn hóa kiến trúc bảo mật theo mô hình phòng thủ đa lớp, từng bước xây dựng Trung tâm điều hành mạng (NOC) và Trung tâm điều hành an ninh mạng (SOC) của VATM. Ngoài ra, dự án góp phần nâng cao khả năng giám sát, cảnh báo sớm, phân tách và kiểm soát truy cập mạng, giảm thiểu rủi ro tấn công mạng, bảo vệ an toàn cho các hệ thống thông tin trọng yếu.

Về mặt chiến lược, đầu tư này giúp VATM tuân thủ các tiêu chuẩn pháp lý quốc gia và quốc tế, tiệm cận mô hình bảo mật của ICAO, đồng thời tạo nền tảng hạ tầng bảo mật vững chắc phục vụ chuyển đổi số ngành hàng không. Đây là dự án mang tính nền tảng, lâu dài, góp phần đảm bảo hoạt động an toàn, ổn định và bền vững của hệ thống thông tin hàng không Việt Nam trong giai đoạn chuyển đổi số và hội nhập quốc tế.

*1.1.3.2. Mục tiêu cụ thể*

- Trang bị, nâng cấp và chuẩn hóa các thiết bị an ninh mạng (IPS/IDS, Firewall) cho các trung tâm, hệ thống và đơn vị trực thuộc chưa được trang bị đầy đủ.
- Thiết lập giải pháp giám sát, quản lý tập trung hoạt động của các thiết bị an ninh mạng, bảo đảm khả năng phát hiện và phản ứng nhanh trước các sự cố an toàn thông tin.
- Tăng cường năng lực chủ động phòng thủ mạng, giảm thiểu nguy cơ rủi ro và thiệt hại do các cuộc tấn công mạng gây ra.
- Nâng cao khả năng tuân thủ quy định của pháp luật về bảo đảm an toàn thông tin mạng theo Nghị định 85/2016/NĐ-CP và các tiêu chuẩn kỹ thuật hiện hành.

## *1.2. Yêu cầu về kỹ thuật*

### *1.2.1. Yêu cầu chung về kỹ thuật*

Dự án **"Thiết bị an ninh mạng IPS/IDS và firewall"** cần đáp ứng các yêu cầu cơ bản, tuân thủ và phù hợp với các quy định của Nhà nước, Bộ thông tin và truyền thông, các tiêu chuẩn của ngành hàng không cũng như các tiêu chuẩn quốc tế bao gồm:

- Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015;
- 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;
- Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ trưởng Bộ Thông tin và Truyền thông về việc quy định hoạt động giám sát an toàn hệ thống thông tin;
- Thông tư số 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ trưởng Bộ Thông tin và Truyền thông về việc ban hành danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước;

- Quyết định số 1127/QĐ-BTTTT ngày 30/7/2021 ban hành yêu cầu kỹ thuật cơ bản đối với sản phẩm quản lý và phân tích sự kiện an toàn thông tin;

- Và các tiêu chuẩn, quy định liên quan khác.

Các giải pháp, thiết bị đầu tư sẽ được tích hợp vào các hệ thống của Tổng công ty Quản lý bay Việt Nam nhằm đáp ứng các tiêu chuẩn liên quan cho một hệ thống thông tin cấp độ tương ứng theo Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT và TCVN 11930:2017.

Việc triển khai hệ thống phải đảm bảo không làm ảnh hưởng, không gián đoạn các hệ thống khác hoặc phải có thỏa thuận trước được sự đồng ý của đơn vị quản lý hệ thống liên quan.

Thiết bị có Giấy chứng nhận xuất xứ (CO) và Giấy chứng nhận chất lượng (CQ) đối với hàng hóa nhập khẩu hoặc Phiếu kiểm tra chất lượng xuất xưởng đối với hàng hóa sản xuất, lắp ráp trong nước.

Phần mềm bản quyền trang bị trong dự án phải đảm bảo mới không lỗi thời, và phải có tài liệu chứng minh bản quyền phần mềm.

Thiết bị đồng bộ chính hãng, mới 100%, chưa qua sử dụng, nguyên đai, nguyên kiện và hoạt động tốt. Hàng hóa được giao phải kèm theo đầy đủ bộ chứng từ như: Thông tin xuất xứ nguồn gốc hàng hóa; catalog hàng hóa,…

Năm sản xuất: Sản xuất từ năm 2024 trở về sau.

Tài liệu kỹ thuật, phụ kiện kèm theo và hướng dẫn sử dụng: theo tiêu chuẩn của nhà sản xuất

Hạ tầng kỹ thuật của dự án phải đảm bảo đúng thiết kế đề ra.

### *1.2.2. Danh mục tiêu chuẩn kỹ thuật áp dụng*

*1.2.2.1. Tiêu chuẩn về ứng dụng công nghệ thông tin trong cơ quan nhà nước*

Danh mục tiêu chuẩn và quy chuẩn áp dụng sẽ căn cứ theo Thông tư số 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ trưởng Bộ Thông tin và Truyền thông về việc ban hành danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước.

*1.2.2.2. Tiêu chuẩn về an toàn an ninh thông tin*

| STT | Mã số | Tên Tiêu chuẩn |
|---|---|---|
| 1 | TCVN ISO/IEC 27002:2011 | Công nghệ thông tin-Các kỹ thuật an toàn-Quy tắc thực hành Quản lý an toàn thông tin |
| 2 | TCVN 8709-1:2011 ISO/IEC 15408-1:2009 | Công nghệ thông tin- Các kỹ thuật an toàn-Các tiêu chí đánh giá an toàn CNTT- Phần 1: Giới thiệu và mô hình tổng quát |

| STT | Mã số | Tên Tiêu chuẩn |
|---|---|---|
| 3 | TCVN 8709-2:2011<br>ISO/IEC 15408-2:2008 | Công nghệ thông tin- Các kỹ thuật an toàn- Các tiêu chí đánh giá an toàn CNTT- Phần 2: Các thành phần chức năng an toàn |
| 4 | TCVN 8709-3:2011<br>ISO/IEC 15408-3:2008 | Công nghệ thông tin- Các kỹ thuật an toàn- Các tiêu chí đánh giá an toàn CNTT- Phần 3: Các thành phần đảm bảo an toàn |
| 5 | TCVN 9250:2012 | Trung tâm kỹ thuật - Yêu cầu về hạ tầng kỹ thuật viễn thông |
| 6 | TCVN 10295:2014<br>ISO/IEC 27005:2011 | Công nghệ thông tin-Các kỹ thuật an toàn- Quản lý rủi ro an toàn thông tin |
| 7 | TCVN 10541:2014<br>ISO/IEC 27003:2010 | Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn triển khai hệ thống quản lý an toàn thông tin |
| 8 | TCVN 10542:2014<br>ISO/IEC 27004:2009 | Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý an toàn thông tin - Đo lường |
| 9 | TCVN 10543:2014<br>ISO/IEC 27010:2012 | Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý an toàn trao đổi thông tin liên tổ chức, liên ngành |
| 10 | TCVN 9801-3:2014<br>ISO/IEC 27033-3:2010 | Công nghệ thông tin - Kỹ thuật an toàn - 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 |
| 11 | TCVN 9801-2:2015 | Công nghệ thông tin - Các kỹ thuật an toàn - An toàn mạng - Phần 2: Hướng dẫn thiết kế và triển khai an toàn mạng |
| 12 | TCVN 11238:2015 | Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng |
| 13 | TCVN 11239:2015 | Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý sự cố an toàn thông tin |
| 14 | TCVN 11385:2016 | Công nghệ thông tin - Các kỹ thuật an toàn - Đánh giá an toàn sinh trắc học |

| STT | Mã số | Tên Tiêu chuẩn |
|---|---|---|
| 15 | TCVN 11386:2016 | Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp đánh giá an toàn công nghệ thông tin |
| 16 | TCVN 11393-1:2016<br>ISO/IEC 13888-1:2009 | Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 1: Tổng quan |
| 17 | TCVN 11393-2:2016<br>ISO/IEC 13888-2:2009 | Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 2: Các cơ chế sử dụng kỹ thuật đối xứng |
| 18 | TCVN 11393-3:2016<br>ISO/IEC 13888-3:2009 | Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 3: Các cơ chế sử dụng kỹ thuật bất đối xứng |
| 19 | 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 |

### *1.2.3. Yêu cầu về triển khai, cấu hình hệ thống*

*1.2.3.1. Tổng hợp Danh mục thiết bị phần cứng, phần mềm theo vị trí lắp đặt*

Danh mục thiết bị phần cứng, phần mềm sẽ được phân bổ triển khai lắp đặt tới các vị trí như sau:

| STT | Danh mục hàng hóa | Đơn vị tính | Tổng | Phân bổ thiết bị theo đơn vị | | | |
|---|---|---|---|---|---|---|---|
| | | | | TT TB TTHK | Cty QLB MB | Cty QLB MT | Cty QLB MN |
| **A** | **Hệ thống trang thiết bị IPS/IDS/APT và Firewall** | | | | | | |
| **I** | **Thiết bị mạng** | | | | | | |
| 1 | Thiết bị chuyển mạch cho hệ thống thông tin cấp độ 4 | Thiết bị | 8 | 2 | 2 | 0 | 4 |
| 2 | Thiết bị chuyển mạch cho hệ thống thông tin cấp độ 3 | Thiết bị | 6 | 0 | 0 | 2 | 4 |
| **II** | **Thiết bị bảo mật** | | | | | | |
| 1 | Thiết bị tường lửa vùng lõi cho hệ thống thông tin cấp độ 4 | Thiết bị | 8 | 4 | 2 | 0 | 2 |
| 2 | Thiết bị tường lửa vùng biên cho hệ thống thông tin cấp độ 4 | Thiết bị | 4 | 2 | 2 | 0 | 0 |
| 3 | Thiết bị tường lửa cho hệ thống thông tin cấp độ 3 | Thiết bị | 6 | 0 | 0 | 2 | 4 |
| 4 | Thiết bị tường lửa cho ứng dụng Web | Thiết bị | 2 | 2 | 0 | 0 | 0 |

| STT | Danh mục hàng hóa | Đơn vị tính | Tổng | Phân bổ thiết bị theo đơn vị | | | |
|---|---|---|---|---|---|---|---|
| | | | | TT TB TTHK | Cty QLB MB | Cty QLB MT | Cty QLB MN |
| 5 | Bản quyền thông lượng WAF (WAF Throughput) | Bộ | 1 | 1 | 0 | 0 | 0 |
| **III** | **Hệ thống thiết bị phân tích phát hiện các mối nguy an ninh mạng (IDS/APT)** | | | | | | |
| 1 | Thiết bị gom lưu lượng mạng | Thiết bị | 4 | 1 | 1 | 1 | 1 |
| 2 | Thiết bị phân tích trung tâm | Thiết bị | 4 | 1 | 1 | 1 | 1 |
| 3 | Thiết bị cảm biến trung tâm | Thiết bị | 4 | 1 | 1 | 1 | 1 |
| 4 | Thiết bị phân tích mã độc Sandbox | Thiết bị | 4 | 1 | 1 | 1 | 1 |
| **IV** | **Phần mềm phân tích phát hiện các mối nguy an ninh mạng (IDS/APT)** | | | | | | |
| 1 | Bản quyền cho Hệ thống Phân tích, phát hiện các mối nguy an ninh mạng tại trung tâm chính | Bộ | 1 | 1 | 0 | 0 | 0 |
| 2 | Bản quyền cho Hệ thống Phân tích, phát hiện các mối nguy an ninh mạng tại Đài KSKL | Bộ | 1 | 1 | 0 | 0 | 0 |
| 3 | Phân tích, phát hiện các mối nguy an ninh mạng - Cảm biến ảo hóa | Bộ | 4 | 1 | 1 | 1 | 1 |
| **B** | **Hệ thống quản lý giám sát vận hành** | | | | | | |
| **I** | **Hệ thống thiết bị phần cứng phục vụ giám sát, hỗ trợ vận hành** | | | | | | |
| 1 | Máy tính quản trị giám sát vận hành | Thiết bị | 4 | 1 | 1 | 1 | 1 |
| 2 | Màn hình giám sát | Thiết bị | 4 | 1 | 1 | 1 | 1 |
| 3 | Thiết bị chuyển mạch quản lý | Thiết bị | 7 | 1 | 2 | 2 | 2 |
| 4 | Máy chủ quản lý giám sát | Thiết bị | 9 | 2 | 3 | 1 | 3 |
| 5 | Phụ kiện triển khai | Gói | 4 | 1 | 1 | 1 | 1 |
| **II** | **Phần mềm thương mại phục vụ công tác giám sát, hỗ trợ vận hành** | | | | | | |
| 1 | Phần mềm Quản lý giám sát mạng (NMS) | Gói | 1 | 1 | 0 | 0 | 0 |
| 2 | Phần mềm quản trị CSDL | Bộ | 4 | 2 | 0 | 0 | 2 |
| 3 | Hệ điều hành máy chủ quản lý giám sát | Bộ | 9 | 2 | 3 | 1 | 3 |
| **C** | **Thiết bị dự phòng** | | | | | | |
| 1 | Thiết bị chuyển mạch cho hệ thống thông tin cấp độ 4 (có thể dùng cho HTTT cấp độ 3 nếu cần) | Thiết bị | 3 | 1 | 1 | 0 | 1 |

| STT | Danh mục hàng hóa | Đơn vị tính | Tổng | Phân bổ thiết bị theo đơn vị | | | |
|---|---|---|---|---|---|---|---|
| | | | | TT TB TTHK | Cty QLB MB | Cty QLB MT | Cty QLB MN |
| 2 | Thiết bị chuyển mạch quản lý | Thiết bị | 4 | 1 | 1 | 1 | 1 |
| 3 | Thiết bị tường lửa vùng lõi cho hệ thống thông tin cấp độ 4 (có thể dùng cho vùng biên nếu cần) | Thiết bị | 3 | 1 | 1 | 0 | 1 |
| 4 | Thiết bị tường lửa cho hệ thống thông tin cấp độ 3 | Thiết bị | 3 | 0 | 1 | 1 | 1 |
| 5 | Thiết bị tường lửa cho ứng dụng Web | Thiết bị | 1 | 1 | 0 | 0 | 0 |
| 6 | Máy chủ quản lý giám sát | Thiết bị | 2 | 1 | 0 | 0 | 1 |
| 7 | Máy tính quản trị giám sát vận hành | Thiết bị | 2 | 1 | 0 | 0 | 1 |
| 8 | Màn hình giám sát | Thiết bị | 2 | 1 | 0 | 0 | 1 |

*1.2.3.2. Yêu cầu về thiết bị Switch, Firewall, IPS, Thiết bị tường lửa ứng dụng Web (Web Application Firewall - WAF) cho các hệ thống*

Dựa vào hiện trạng các hệ thống thiết bị, triển khai bổ sung các thiết bị Firewall, IPS, Web Application Firewall, Switch như sau:

| STT | Hệ thống thông tin | Cấp độ | Switch cấp độ 4 | Firewall vùng lõi cấp độ 4 | Firewall vùng biên cấp độ 4 | Thiết bị tường lửa ứng dụng Web (WAF) | Switch cấp độ 3 | Firewall vùng lõi cấp độ 3 |
|---|---|---|---|---|---|---|---|---|
| **Trung tâm Thông báo tin tức hàng không** | | | | | | | | |
| 1 | Hệ thống thông báo tin tức hàng không tự động (AIS) | 4 | | 2 | | | | |
| 2 | Hệ thống quản lý tin tức hàng không (AIM) | 4 | 2 | 2 | 2 | 2 | | |
| **Công ty Quản lý bay Miền bắc** | | | | | | | | |
| 3 | Hệ thống thiết bị quản lý không lưu tự động (ATM) | 4 | 2 | 2 | 2 | | | |

| STT | Hệ thống thông tin | Cấp độ | Switch cấp độ 4 | Firewall vùng lõi cấp độ 4 | Firewall vùng biên cấp độ 4 | Thiết bị tường lửa ứng dụng Web (WAF) | Switch cấp độ 3 | Firewall vùng lõi cấp độ 3 |
|---|---|---|---|---|---|---|---|---|
| 4 | Hệ thống VCCS ATCC Hà Nội | 3 | | | | | 2 | 2 |
| **Công ty quản lý bay Miền Trung** | | | | | | | | |
| 5 | Hệ thống xử lý dữ liệu ra đa (RDP) Aircon APP/TWR Đà Nẵng | 3 | | | | | 2 | 2 |
| **Công ty Quản lý bay Miền nam** | | | | | | | | |
| 6 | Hệ thống xử lý điện văn dịch vụ không lưu AMHS | 4 | 4 | 2 | | | | |
| 7 | Hệ thống VCCS ACC/HCM | 3 | | | | | 2 | 2 |
| | **Cộng** | | **8** | **8** | **4** | **2** | **6** | **6** |

*1.2.3.3. Yêu cầu về giải pháp phân tích phát hiện các mối nguy an ninh mạng*

*1.2.3.3.1. Yêu cầu về mô hình giải pháp phân tích, phát hiện các mối nguy an ninh mạng*

Hệ thống phân tích được triển khai tại các đầu mối gồm:

+ Đài KSKL Nội Bài, Đà Nẵng, Tân Sơn Nhất;

+ Phòng thiết bị trung tâm ATCC HCM, ATCC HAN và Trung tâm TBTTHK (đặt tại ATCC HAN);

Tại các đầu mối thu thập dữ liệu các thiết bị của các hệ thống theo từng khu vực sẽ gồm:

+ Các **Thiết bị cảm biến** chuyên dụng, có khả năng xử lý đáp ứng yêu cầu lưu lượng mạng tổng hợp của các hệ thống và;

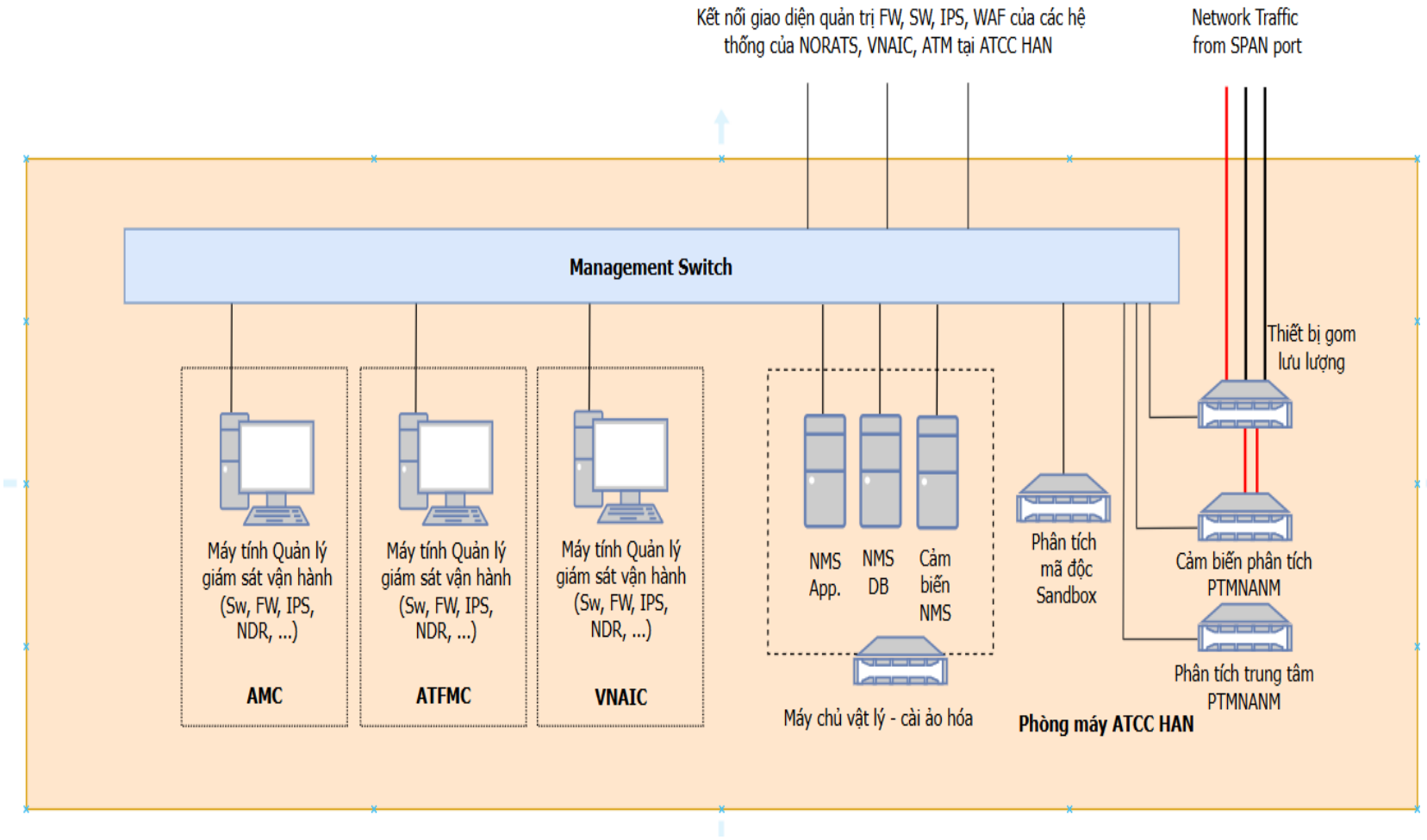
+ Các **Thiết bị gom lưu lượng mạng** chuyên dụng.

Lưu lượng mạng từ các chuyển mạch chính của các hệ thống được đầu tư trong dự án được cấu hình SPAN port đẩy ra một cổng. Thiết bị thu gom lưu lượng chuyên dụng sẽ kết nối vào cổng SPAN, thu gom lưu lượng và đẩy vào thiết bị Thiết bị cảm biến Phân tích phát hiện các mối nguy an ninh mạng.

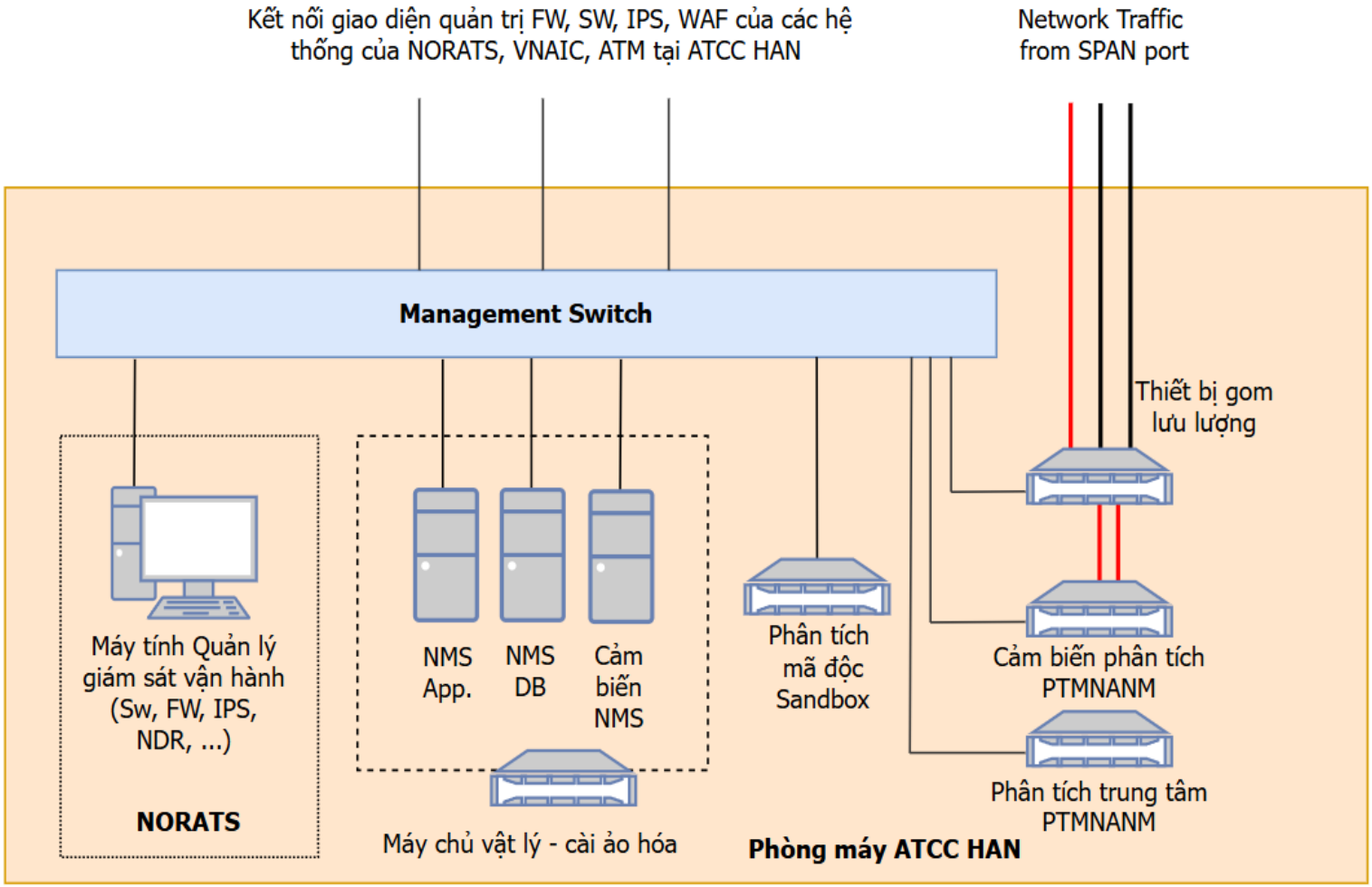
Thiết bị thu gom lưu lượng mạng hỗ trợ các loại cổng 1/10Gbps RJ45 cáp đồng và 1/10/25Gbps SFP+ cáp quang cho phép thu nhận từ các mạng trong khoảng cách lên tới 300m.

Đối với hệ thống hoặc điểm thu lưu lượng ở xa  sử dụng Cảm biến ảo hóa.

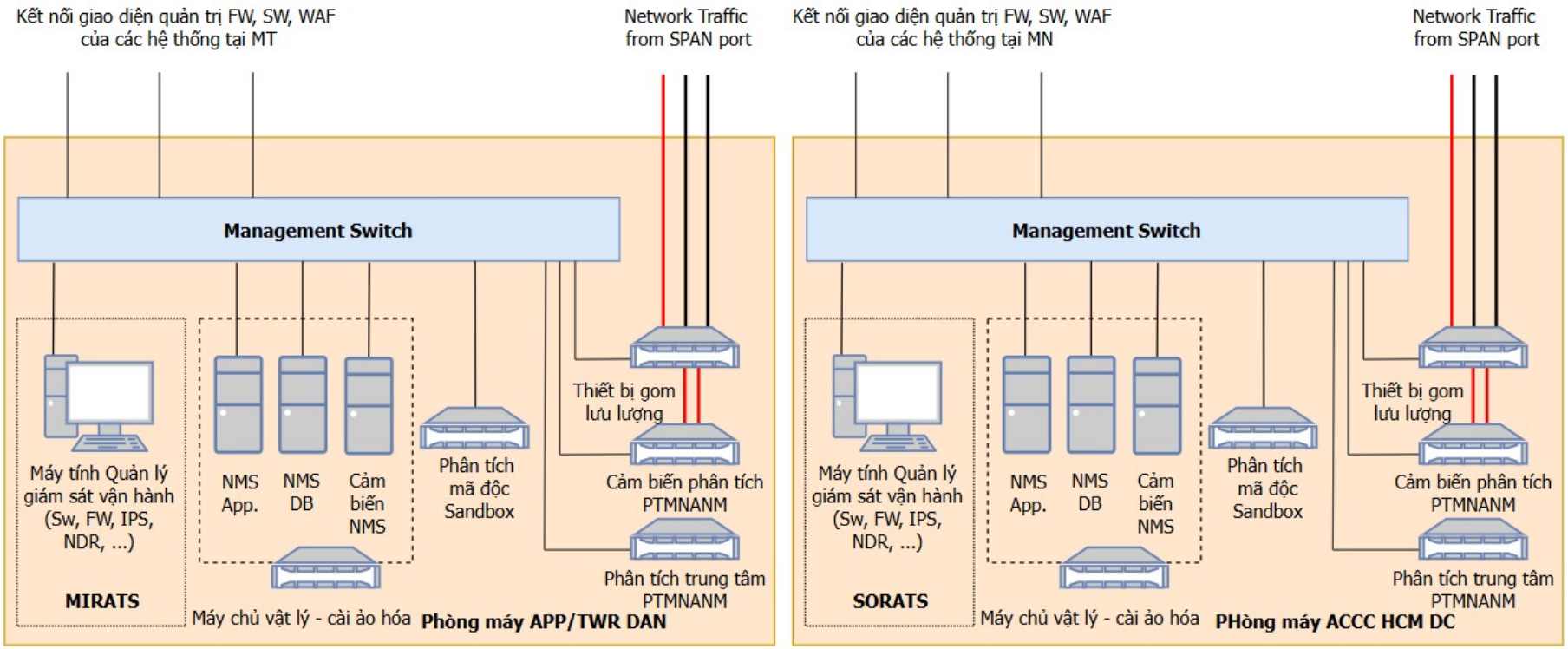
*1.2.3.3.2. Yêu cầu chi tiết về mô hình hệ thống phân tích, phát hiện các mối nguy an ninh mạng tại các trung tâm*




*Hình V-1: Mô hình hệ thống do Trung tâm TBTTHK quản lý vận hành tại phòng máy tại ATCC HAN*




*Hình V-2: Mô hình hệ thống do Công ty QLB Miền Bắc quản lý vận hành tại phòng máy tại ATCC HAN*




*Hình V-3: Mô hình hệ thống tại phòng máy tại ACCC HCM và APP/TWR DAN*

Tại các miền, lưu lượng từ nhiều hệ thống, hệ thống cần sử dụng thiết bị phần cứng để đảm bảo tải, hiệu năng xử lý, tính ổn định.

***1- Thiết bị gom lưu lượng mạng:***

- Tiếp nhận, gom lưu lượng mạng (aggregate traffic) từ nhiều hệ thống, gửi lưu lượng đã thu gom vào Thiết bị cảm biến phân tích phát hiện mối nguy an ninh mạng.

- Lưu lượng thu gom về có thể điều hướng, nhân bản (duplicate/copy) gửi tới các giao diện khác nhau để kết nối với các thiết bị phân tích khác nhau. Khi lưu lượng hệ thống tăng lên có thể tăng thêm các Thiết bị cảm biến phân tích phát hiện mối nguy an ninh mạng và gửi các nhóm lưu lượng mạng khác nhau tới các cảm biến phân tích khác nhau, để chia tải, tăng năng lực xử lý tổng của hệ thống.

***2- Thiết bị phân tích trung tâm:***

- Tiếp nhận các cảnh báo, phát hiện và siêu dữ liệu (metadata) mạng từ các Cảm biến phân tích phát hiện mối nguy an ninh mạng triển khai tại miền và các Đài KSKL.

- Phát hiện các tài sản xuất hiện trên mạng, tính toán các đường cơ sở về hoạt động, phát hiện các hành vi bất thường và mối nguy an ninh mạng, kết nối mạng có nguy cơ.

- Tích hợp với các giải pháp như Endpoint Security, IPS, … để tiếp nhận thêm thông tin, làm giàu thông tin cho các tài sản và mối nguy an ninh mạng.

- Tích hợp với các giải pháp như đo quét điểm yếu để xác định các điểm có rủi ro và con đường các mối nguy, tội phạm mạng có thể khai thác tấn công mạng.

- Sử dụng các công nghệ ML/AI để phát hiện các tấn công lây lan, đi ngang trong hệ thống, các tấn công nâng cao, có chủ đích, sử dụng các kỹ thuật trốn tránh tinh vi.

- Sử dụng trí tuệ nhân tạo tạo sinh (GenAI) để tổng hợp thông tin, vẽ sơ đồ trực quan, hỗ trợ điều tra nhanh chóng, gợi ý các hành động phản ứng cần thực hiện với sự cố đang được phân tích, dẫn hướng và nâng cao năng lực phân tích của đội ngũ vận hành.

***3- Thiết bị cảm biến trung tâm phát hiện mối nguy an ninh mạng:***

- Phát hiện các tấn công khai thác điểm yếu, phát hiện các file có chứa virus / mã độc truyền nhận trên mạng sử dụng công nghệ phân tích mã độc thực thi ảo hóa, phân tích nâng cao, sử dụng công nghệ học máy và trí tuệ nhân tạo (ML/AI), phát hiện các tấn công lan truyền trong hệ thống.

- Hỗ trợ nhiều cổng để phân tích cho nhiều hệ thống / phân mạng khác nhau.

- Hỗ trợ chế độ triển khai ngoại tuyến (TAP/SPAN) và chế độ nội tuyến (Inline) có khả năng ngăn chặn các mối nguy, các kết nối độc hại.

- Hỗ trợ phân tích mã độc Sandbox tích hợp sẵn trong thiết bị hoặc thiết bị phân tích mã độc Sandbox ngoài để tăng năng lực xử lý.

***4- Thiết bị phân tích mã độc Sandbox:***

- Phân tích mã độc nâng cao sử dụng công nghệ thực thi ảo hóa (Virtual Execution – Sandboxing), phân tích mã (Code Analysis), quét mã độc, học máy/trí tuệ nhân tại (ML/AI), phát hiện Riskware, YARA.

- Hỗ trợ thực thi ảo hóa, phân tích trong các hệ điều hành Windows, MacOS, Linux với các bản vá, phiên bản hệ điều hành khác nhau, tổ hợp thành hàng trăm môi trường.

- Tích hợp với các cảm biến ảo hóa, và cả vật lý để cung cấp năng lực phân tích file, URL nâng cao, phát hiện các tấn công APT, mã độc mới, chưa từng biết tới.

***5- Máy chủ quản lý giám sát:***

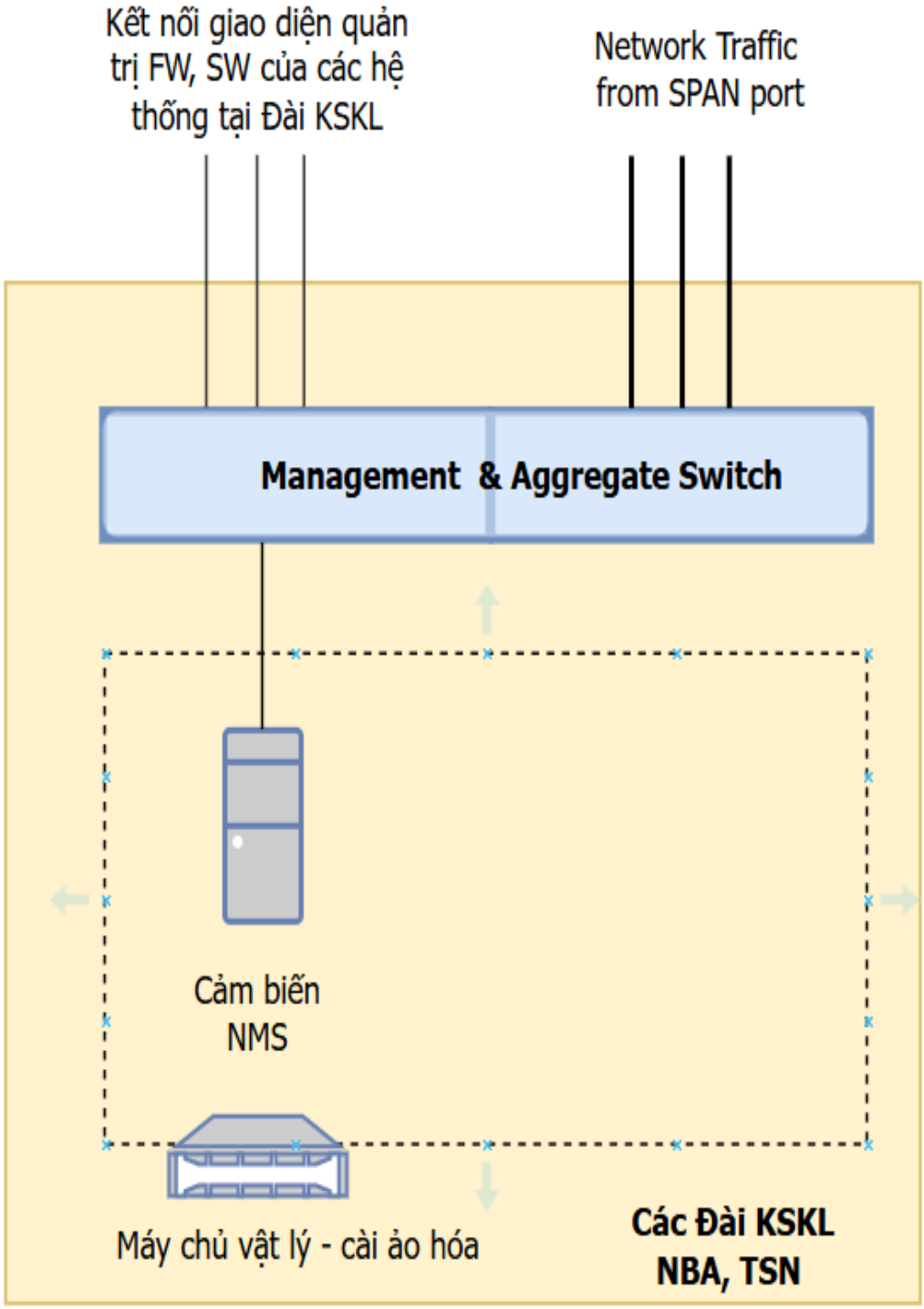
- Quản lý tập trung các cảm biến phân tích mối nguy an ninh mạng bao gồm cả thiết bị phần cứng tại các miền và cảm biến ảo hóa triển khai tại các Đài KSKL

- Tích hợp các cảm biến ảo hóa tại các Đài KSKL với thiết bị phân tích mã độc Sandbox tại các miền để phân tích các file, URL nâng cao, phát hiện các mã độc mới.

- Chia sẻ thông tin về các mối nguy giữa các cảm biến để nhanh chóng phối hợp, hiệp đồng phát hiện các mối nguy phát hiện trên toàn mạng.

*1.2.3.3.3. Yêu cầu chi tiết về mô hình hệ thống phân tích, phát hiện các mối nguy an ninh mạng tại các đài KSKL*

Mô hình hệ thống tại các Đài KSKL Nội Bài, Tân Sơn Nhất:




*Hình V-4: Mô hình hệ thống tại các Đài KSKL Nội Bài, Tân Sơn Nhất*

***1- Thiết bị gom lưu lượng mạng***

Lưu lượng mạng được thu thập thông qua các thiết bị chuyển mạch được đầu tư trong dự án, các trung tâm của các hệ thống. Lưu lượng các vùng mạng cần được phân tích sẽ được SPAN port, tổng hợp gửi về một cổng của chuyển mạng trong hệ thống. Cổng này sẽ được kết nối và gửi lưu lượng tới phân vùng gom lưu lượng của Chuyển mạch vùng quản lý và gom lưu lượng (Management & Aggregate Switch).

Trên Management & Aggregate Switch, thực hiện SPAN port thêm một lần nữa để gom lưu lượng gửi vào Cảm biến phân tích phát hiện mối nguy an ninh mạng ảo hóa.

***2- Cảm biến phân tích phát hiện mối nguy an ninh mạng:***

Cảm biến phân tích phát hiện mối nguy an ninh mạng được triển khai dạng ảo hóa trên máy chủ ảo hóa VMware, KVM, Hyper-V.

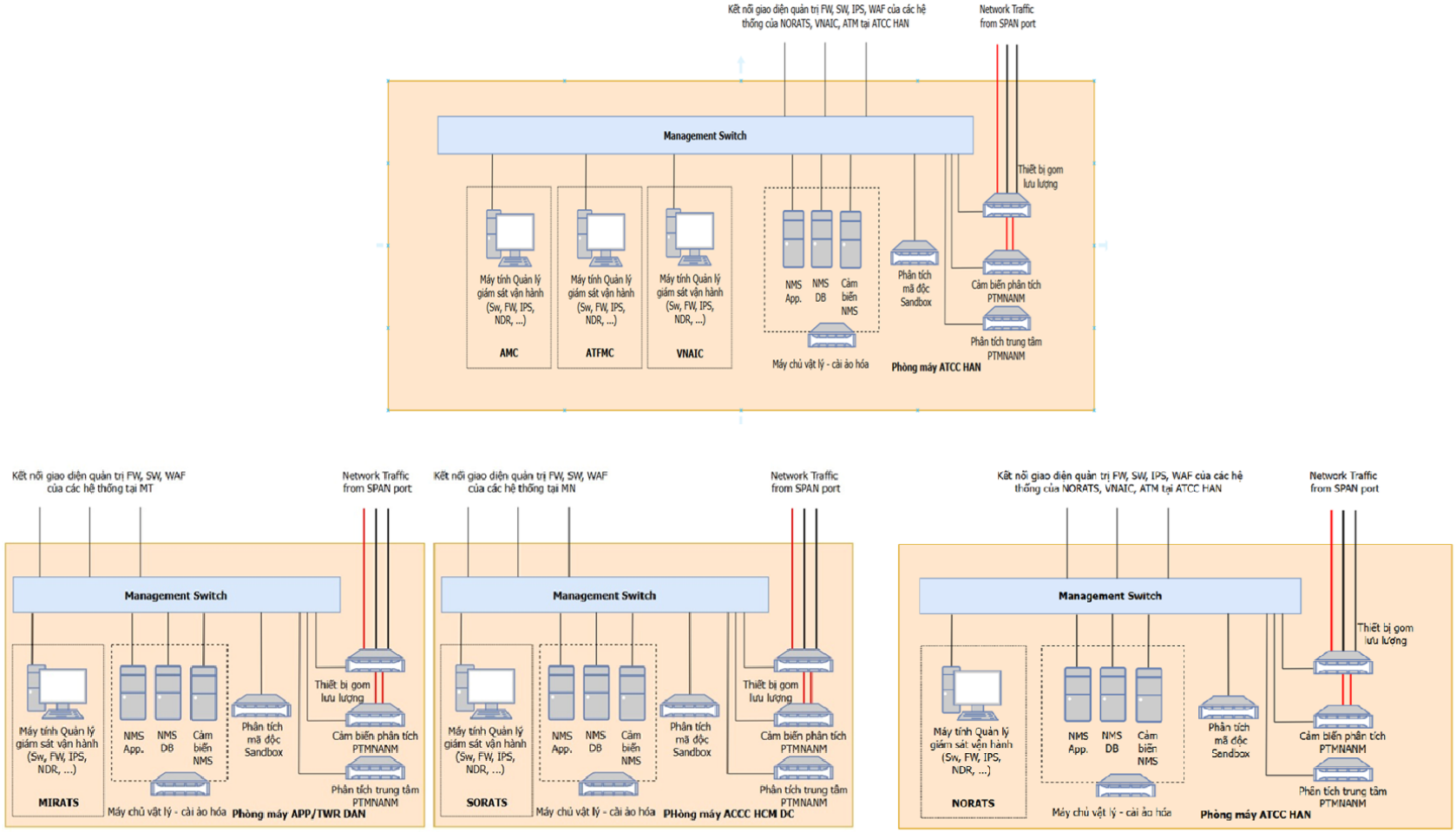
Cảm biến có thể hỗ trợ lưu lượng phân tích với 500Mbps. Cảm biến cần tích hợp với Thiết bị phân tích mã độc Sandbox ở các Trung tâm miền.

Cảm biến được quản lý tập trung, chia sẻ thông tin các mối nguy từ hệ thống Quản lý tập trung các cảm biến ở các Trung tâm miền.

*1.2.3.4. Yêu cầu về giải pháp quản lý giám sát vận hành*

*1.2.3.4.1. Yêu cầu về mô hình hệ thống quản lý giám sát vận hành*

Mô hình logic cho Hệ thống Quản lý giám sát vận hành như sau:




*Hình V-5: Mô hình logic Hệ thống Quản lý giám sát vận hành*

Hệ thống Quản lý giám sát vận hành được đầu tư tại các Công ty quản lý bay Miền Bắc (ATCC HAN và Đài KSKL Nội Bài), Miền Trung (Đài KSKL Đà Nẵng), Miền Nam (ATCC HCM và Đài KSKL TSN), Trung tâm Thông báo tin tức hàng không (TBTTHK).

Tại mỗi Công ty quản lý bay khu vực sẽ được trang bị các hệ thống máy chủ được cài đặt phần mềm quản lý giám sát, thu thập thông tin của hệ thống APT, các thiết bị chuyển mạch quản lý để kết nối port quản trị của các thiết bị và kết nối span để chuyển tiếp lưu lượng mạng, máy tính quản trị giám sát và màn hình hiển thị thông tin. Phần mềm hỗ trợ triển khai trong môi trường Private Cloud hoặc on-premises. Về bản quyền phần mềm, hệ thống sử dụng một giấy phép linh hoạt cho tất cả các thiết bị giám sát bao gồm thiết bị mạng và máy chủ vật lý/ảo hóa.

Phần mềm Quản lý giám sát mạng (Network Monitoring System - NMS) sẽ có các chức năng chính như:

- Giám sát tình trạng sức khỏe của toàn bộ các thiết bị đang có trong hệ thống. Có thể hiển thị các thông tin như CPU, RAM, Disk, Interface, latency, …

- Giám sát hạ tầng mạng (end to end) trên toàn bộ hệ thống mạng của đơn vị, cung cấp cái nhìn sâu sắc về các tác động của hiệu suất mạng đến dịch vụ và người dùng.

- Giám sát ứng dụng toàn diện và chi tiết, cho phép đánh giá hiệu suất, phân tích lỗi và xử lý sự cố trong quá trình vận hành.

- Hỗ trợ quản lý log đa nguồn, đa lớp (full-stack) với khả năng mở rộng linh hoạt, được tích hợp chặt chẽ với các thành phần observability trong cả ứng dụng và hạ tầng.

- Giám sát Cơ sở dữ liệu chuyên sâu để chẩn đoán và phân tích hiệu suất cơ sở dữ liệu với công nghệ phân tích nguyên nhân gốc rễ (root cause analysis). Hỗ trợ nhiều nền tảng Cơ sở dữ liệu khác nhau như MySQL, PostgreSQL, Microsoft SQL Server, MongoDB, Redis,…

- Cung cấp Dashboard quản lý lỗ hổng (Vulnerability Dashboard) giúp tăng khả năng quan sát, rút ngắn thời gian phát hiện – cảnh báo – xử lý sự cố bảo mật cho đội ngũ vận hành.

- Hỗ trợ giám sát đa dạng các loại thiết bị như Router, Switch, Firewall, Wireless, Server, các thiết bị hỗ trợ giao thức SNMP và từ nhiều các nhà cung cấp phổ biến như Cisco, Dell, F5, Juniper, HP…

*1.2.3.4.2. Yêu cầu chi tiết về hệ thống quản lý giám sát trung tâm*

Hệ thống quản lý giám sát vận hành tập trung được triển khai tại Phòng thiết bị trung tâm Công ty QLB Miền Bắc, Miền Trung, Miền Nam và Trung tâm Thông báo tin tức hàng không, bao gồm:

***1- Thiết bị chuyển mạch quản lý (management switch):*** Toàn bộ các kết nối giao diện quản trị của những thiết bị mới được trang bị sẽ kết nối đến thiết bị switch này, thông qua cổng management người quản trị có thể truy cập vào cấu hình, quản lý và vận hành các thiết bị được kết nối. Ngoài ra thông qua cổng management của mỗi thiết bị cũng có thể truy xuất một số thông tin sử dụng làm dữ liệu đầu vào cho hệ thống NMS.

Nhiều hệ thống công nghệ thông tin độc lập, thuộc các đơn vị và chức năng khác nhau, mỗi hệ thống được thiết lập vùng mạng và tường lửa (firewall) riêng biệt, đảm bảo nguyên tắc phân tách, độc lập trong vận hành.

Thiết bị **Management Switch** được bố trí nhằm phục vụ việc **quản lý, giám sát và cấu hình tập trung các thiết bị an ninh mạng (Firewall/IPS/IDS)**. Tuy nhiên, do đặc thù của thiết bị này sẽ **kết nối đến các cổng quản trị (Management Port)** của nhiều thiết bị firewall thuộc các hệ thống khác nhau (bao gồm cả các hệ thống trong Tòa nhà Trung tâm Kiểm soát không lưu Hà Nội - ATCC HAN), nên phải có giải pháp kỹ thuật đảm bảo rằng việc triển khai không tạo ra nguy cơ liên thông hoặc xâm nhập chéo giữa các hệ thống. Cụ thể, phải áp dụng các giải pháp:

***+ Phân vùng mạng quản trị bằng VLAN độc lập:***

Mỗi hệ thống (ví dụ: AIM, ATFM, VCCS, v.v.) sẽ có một VLAN quản trị riêng biệt trên thiết bị Management Switch. Các VLAN này không được định tuyến với nhau, chỉ cho phép truy cập từ máy chủ quản trị được phân quyền riêng của từng hệ thống, đảm bảo tính độc lập hoàn toàn.

***+ Áp dụng cơ chế Access Control List (ACL):***

Trên Management Switch cấu hình danh sách kiểm soát truy cập (ACL) để giới hạn IP, MAC và giao thức quản trị được phép đi qua từng VLAN. Chỉ các kết nối từ thiết bị giám sát trung tâm (hoặc SOC) đã được định danh mới được phép truy cập đến từng thiết bị firewall cụ thể.

***+ Không định tuyến lớp 3 giữa các VLAN:***

Thiết bị Management Switch hoạt động ở lớp 2 (Layer 2 switch mode), không có chức năng định tuyến IP, đảm bảo cách ly hoàn toàn các miền quản trị. Các tác vụ giám sát tập trung được thực hiện thông qua giao diện quản lý được thiết kế "read-only", không có quyền can thiệp cấu hình.

***+ Triển khai giám sát và cảnh báo truy cập quản trị:***

Hệ thống quản lý tập trung (Security Management/Monitoring System) ghi log và cảnh báo mọi truy cập đến các cổng quản trị của firewall để đảm bảo kiểm soát tuyệt đối truy cập quản trị.

***2- Máy tính quản trị giám sát vận hành:*** Sẽ được kết nối trực tiếp vào Management Switch, từ thiết bị này người vận hành có thể thực hiện các tác vụ quản trị như cấu hình, chỉnh sửa, thiết lập chính sách, troubleshooting, …

***3- Màn hình giám sát:*** Sẽ được sử dụng để hiển thị các thông tin từ hệ thống NMS giúp đội ngũ quản trị, vận hành nắm được thông tin tổng thể về tình trạng sức khỏe của thiết bị, các vấn đề mà hệ thống đang gặp phải hoặc những thống kê về ứng dụng/người dùng/IP đang hoạt động trong hệ thống.

***4- Máy chủ quản lý giám sát:*** Các máy chủ được triển khai tại các Trung tâm chính tại Công ty QLB Miền Bắc, Công ty QLB Miền Nam, Trung tâm TBTTHK theo mô hình host-stanby (1+1) sẽ gồm 02 máy chủ và 01 tại Đài KSKL Đà Nẵng (Công ty QLB Miền Trung) để cài đặt các ứng dụng phục vụ cho các thành phần quản lý, giám sát hay thu thập thông tin của hệ thống.

Máy chủ vật lý được trang bị tại các Trung tâm này sẽ được cài đặt các Máy chủ ảo hóa cho các ứng dụng khác nhau gồm:

+ Máy ảo cài đặt Phần mềm Quản lý giám sát mạng (NMS Application);

+ Máy ảo cài đặt CSDL cho Hệ thống Quản lý giám sát mạng (NMS Database);

+ Máy ảo cài đặt Cảm biến NMS;

+ Máy ảo cài đặt Hệ thống Cảm biến Phân tích mối nguy an ninh mạng (PTMNANM);

+ Máy ảo cài đặt thành phần thu nhận log của SIEM (dự tính cho tương lai);

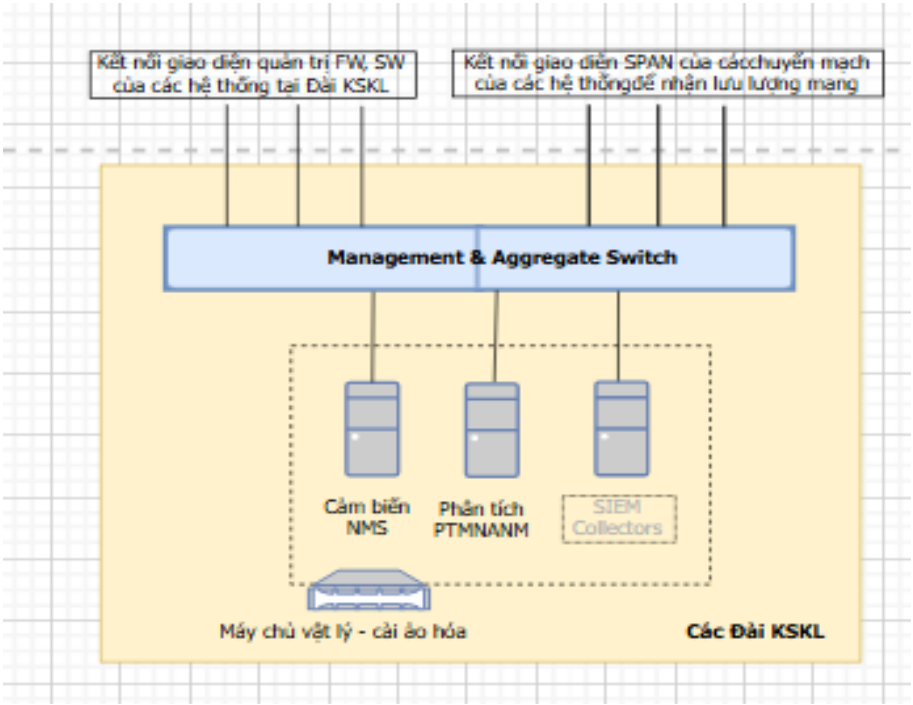
+ Máy ảo cài đặt Cảm biến NMS;

+ Máy ảo cài đặt Hệ thống Cảm biến Phân tích mối nguy an ninh mạng (PTMNANM);

+ Máy ảo cài đặt thành phần thu nhận log của SIEM (dự tính cho tương lai);

*1.2.3.4.3. Yêu cầu chi tiết về hệ thống quản lý giám sát tại Đài KSKL Nội Bài, Tân Sơn Nhất*

Mô hình hệ thống tại các Đài KSKL:




*Hình V-6: Mô hình logic cho Hệ thống Quản lý giám sát vận hành tại Đài KSKL*

Hệ thống quản lý giám sát vận hành tại các Đài KSKL sẽ bao gồm:

- Thiết bị chuyển mạch quản lý (management switch) sẽ đảm nhận 2 vai trò chính:

+ Kết nối toàn bộ cổng quản trị của các thiết bị để phục vụ cho tác vụ quản lý, cấu hình, vận hành và thu thập thông tin thông qua cổng Management.

+ Kết nối vào cổng nhận lưu lượng SPAN port của các thiết bị chuyển mạch trong hệ thống, để tiếp nhận lưu lượng mạng. SPAN lưu lượng sẽ gửi thông tin đến Cảm biến phân tích và gom tổng hợp đến các thiết bị phân tích tại Công ty quản lý bay khu vực .

- Máy chủ: Hệ thống máy chủ tại các Đài KSKL sẽ được sử dụng để cài đặt các ứng dụng phục vụ cho các thành phần quản lý, giám sát hay thu thập thông tin của hệ thống. Mỗi máy chủ vật lý được trang bị tại các Đài KSKL sẽ được ảo hóa thành các máy chủ như Cảm biến NMS, Cảm biến phân tích APT (Phân tích phát hiện các

mối nguy an ninh mạng) hay SIEM Collectors (phục vụ thu thập thông tin log cho hệ thống SOC).

Cụ thể các máy chủ ảo sẽ được cài đặt tại các Đài KSKL như sau:

+ Máy ảo cài đặt Cảm biến NMS
+ Máy ảo cài đặt Cảm biến Phân tích mối nguy an ninh mạng (PTMNANM)
+ Máy ảo cài đặt thành phần thu nhận log của SIEM (dự tính cho tương lai).

### *1.2.4. Yêu cầu chi tiết về kỹ thuật*

#### *1.2.4.1. Yêu cầu chi tiết về thông số kỹ thuật*

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| **A** | **Hệ thống trang thiết bị IPS/IDS/APT và Firewall** | | | |
| **I** | **Thiết bị mạng** | | | |
| 1 | Thiết bị chuyển mạch cho hệ thống thông tin cấp độ 4 | - Thiết kế dạng rackmount hoặc tương đương; | Thiết bị | 8 |
| | | - Số cổng kết nối tối thiểu: | | |
| | | + ≥24 cổng tốc độ 1G/10G SFP+ hoặc tương đương; | | |
| | | + ≥02 cổng QSFP28 tốc độ ≥40Gbps hoặc tương đương; | | |
| | | - Module kèm theo: | | |
| | | + Tối thiểu 14 module đồng 1000BASE-T hoặc tương đương; | | |
| | | + Tối thiểu 10 module quang tốc độ 10Gbps chuẩn SR hoặc tương đương; | | |
| | | - Tốc độ chuyển mạch (Switching capacity): ≥ 1000 Gbps; | | |
| | | - Tốc độ chuyển tiếp dữ liệu (Forwarding rate): ≥ 800 Mpps; | | |
| | | - Số lượng địa chỉ MAC hoặc bảng MAC: ≥ 32,000; | | |
| | | - Số lượng mạng lan ảo (VLANs): ≥ 4094; | | |
| | | - Khung jumbo (Jumbo Frames): ≥ 9198 Bytes; | | |
| | | - Số nhóm LAG (LAG groups): ≥ 128 | | |
| | | - Đáp ứng các tiêu chuẩn quốc tế: IEEE 802.1d, IEEE 802.1w, IEEE 802.1p, IEEE 802.1Q, IEEE 802.3ad, IEEE 802.1s; | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Có sẵn tính năng truyền tải Audio/Video qua môi trường Ethernet theo thời gian thực; | | |
| | | - Hỗ trợ khả năng xếp chồng; | | |
| | | - Hỗ trợ các giao thức định tuyến: RIPv1/v2, BGP, EVPN, VXLAN, Định tuyến theo chính sách (PBR) cho IPV4 và IPV6; | | |
| | | - Có sẵn các giao thức định tuyến: Tĩnh, OSPF, IS-IS; | | |
| | | - Giao diện dòng lệnh CLI, giao thức SSH và SNMP và giao diện web (GUI) | | |
| | | - Nguồn điện: ≥02 nguồn dự phòng với dải điện áp 220V-240V; | | |
| | | - Bảo hành: ≥3 năm theo tiêu chuẩn của nhà sản xuất. | | |
| 2 | Thiết bị chuyển mạch cho hệ thống thông tin cấp độ 3 | - Thiết kế dạng rackmount hoặc tương đương; | Thiết bị | 6 |
| | | - Số cổng kết nối tối thiểu: | | |
| | | + ≥24 cổng 10/100/1000 Mbps hoặc tương đương; | | |
| | | + ≥8 cổng 1/10Gbps SFP+ hoặc tương đương; | | |
| | | - Tốc độ chuyển mạch (Switching capacity): ≥ 208Gbps; | | |
| | | - Tốc độ chuyển tiếp dữ liệu (Forwarding rate): ≥ 150Mpps; | | |
| | | - Số lượng địa chỉ MAC hoặc bảng MAC: ≥ 32,000; | | |
| | | - Số nhóm LAG có thể tạo (LAG groups): ≥ 128 | | |
| | | - Hỗ trợ khả năng xếp chồng; | | |
| | | - Có sẵn tính năng truyền tải Audio/Video qua môi trường Ethernet theo thời gian thực; | | |
| | | - Giao thức định tuyến: RIPv1/v2, Định tuyến theo chính sách (PBR), OSPF, IS-IS, Tĩnh; | | |
| | | - Giao diện dòng lệnh CLI, giao thức SSH và SNMP và giao diện web (GUI). | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Nguồn điện: ≥1 nguồn cấp với dải điện áp 220V-240V; | | |
| | | - Bảo hành: ≥3 năm theo tiêu chuẩn của nhà sản xuất. | | |
| **II** | **Thiết bị bảo mật** | | | |
| 1 | Thiết tường lửa vùng lõi cho hệ thống thông tin cấp độ 4 | - Thiết kế dạng rackmount hoặc tương đương; | Thiết bị | 8 |
| | | - Thông lượng Threat Prevention/Threat Protection đo với traffic hỗn hợp appmix/enterprisemix ≥ 4.5 Gbps; | | |
| | | - New session per second/connection per second ≥ 90.000; | | |
| | | - Số cổng kết nối tối thiểu: | | |
| | | + Cổng đồng 1Gbps: ≥8; | | |
| | | + Cổng quang 1 Gbps SFP: ≥6; | | |
| | | + Cổng quang 10Gbps SFP+: ≥4 cổng (trang bị sẵn ≥02 transceiver tốc độ ≥10Gbps chuẩn SR); | | |
| | | + Cổng high availability (HA): ≥01; | | |
| | | - Nguồn điện: | | |
| | | + Tối thiểu 02 nguồn, hỗ trợ dự phòng redundant; | | |
| | | + Dải điện áp 220V-240V; | | |
| | | - Giao thức định tuyến: OSPF, BGP, static routing; | | |
| | | - Có sẵn tính năng High availability cấu hình Active/Active hoặc Active/Passive; | | |
| | | - Có tính năng tường lửa, kiểm soát theo ứng dụng Application Control/App-ID, phòng chống xâm nhập (IPS), Antivirus/Antimalware; | | |
| | | - Có tính năng lọc web URL-Filtering theo các danh mục (category); | | |
| | | - Có khả năng tuỳ biến các IPS signature, cho phép chuyển đổi / import cú pháp signature từ Snort sang ngay trên Firewall; | | |
| | | - Có menu riêng để cấu hình chính sách giải mã SSL, độc lập với menu cấu hình chính sách kiểm soát truy cập | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Có khả năng kéo thả, di chuyển các đối tượng object (address, application…) giữa các Security Rule; | | |
| | | - Có khả năng chuyển tiếp các yêu cầu DNS request đến tên miền độc hại (malicious domain) tới một địa chỉ IP đích định nghĩa trước (DNS sinkhole/DNS trap), áp dụng cho mọi loại ứng dụng; | | |
| | | - Giao diện quản trị đồ hoạ web, CLI và qua API để quản trị thiết bị; | | |
| | | - Có chức năng phân tích log và báo cáo tổng hợp; | | |
| | | - Yêu cầu trang bị sẵn tối thiểu các tính năng IPS, Application Control, Antivirus, URL Filtering hoặc tương đương có hiệu lực ≥03 năm; | | |
| | | - Bảo hành: ≥3 năm theo tiêu chuẩn của nhà sản xuất. | | |
| 2 | Thiết bị tường lửa vùng biên cho hệ thống thông tin cấp độ 4 | - Thiết kế dạng rackmount hoặc tương đương; | Thiết bị | 4 |
| | | - Thông lượng Threat Prevention/Threat Protection đo với traffic hỗn hợp appmix/enterprisemix ≥ 4.5 Gbps | | |
| | | - Số lượng phiên kết nối mới mỗi giây: ≥ 90.000; | | |
| | | - Cổng kết nối tối thiểu: | | |
| | | + Cổng đồng 1Gbps: ≥8; | | |
| | | + Cổng quang 1 Gbps SFP: ≥6; | | |
| | | + Cổng quang 10Gbps SFP+: ≥4 cổng (trang bị sẵn ≥02 transceiver tốc độ ≥10Gbps chuẩn SR); | | |
| | | + Cổng high availability (HA): ≥01; | | |
| | | - Nguồn điện: | | |
| | | + Tối thiểu 2 nguồn, hỗ trợ dự phòng redundant; | | |
| | | + Dải điện áp 220V-240V; | | |
| | | - Giao thức định tuyến: OSPF, BGP, static routing; | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Có sẵn tính năng High availability cấu hình Active/Active hoặc Active/Passive; | | |
| | | - Có sẵn tính năng Firewall, kiểm soát theo ứng dụng Application Control/App-ID, phòng chống xâm nhập (IPS), Antivirus/Antimalware có hiệu lực ≥03 năm; | | |
| | | - Có khả năng tuỳ biến các IPS signature, cho phép chuyển đổi / import cú pháp signature từ Snort sang ngay trên Firewall; | | |
| | | - Có menu riêng để cấu hình chính sách giải mã SSL, độc lập với menu cấu hình chính sách kiểm soát truy cập | | |
| | | - Có khả năng kéo thả, di chuyển các đối tượng object (address, application…) giữa các Security Rule; | | |
| | | - Có khả năng chuyển tiếp các yêu cầu DNS request đến tên miền độc hại (malicious domain) tới một địa chỉ IP đích định nghĩa trước (DNS sinkhole/DNS trap), áp dụng cho mọi loại ứng dụng; | | |
| | | - Giao diện quản trị đồ hoạ web, CLI và qua API để quản trị thiết bị; | | |
| | | - Có chức năng phân tích log và báo cáo tổng hợp; | | |
| | | - Bảo hành: ≥3 năm theo tiêu chuẩn của nhà sản xuất. | | |
| 3 | Thiết bị tường lửa cho hệ thống thông tin cấp độ 3 | - Thiết kế dạng rackmount hoặc tương đương; | Thiết bị | 6 |
| | | - Thông lượng Threat Prevention/Threat Protection đo với traffic hỗn hợp appmix/enterprisemix ≥ 1 Gbps | | |
| | | - Số lượng phiên kết nối mới mỗi giây: ≥ 30.000; | | |
| | | - Số cổng kết nối tối thiểu: | | |
| | | + Cổng đồng 1Gbps: ≥6; | | |
| | | + Cổng quang 1 Gbps SFP: ≥01; | | |
| | | - Dung lượng lưu trữ: ≥ 128 GB; | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Nguồn điện: Nguồn AC có dải điện áp 100V-240V; | | |
| | | - Giao thức định tuyến: OSPF, BGP, static routing; | | |
| | | - Có sẵn tính năng High availability cấu hình Active/Active hoặc Active/Passive; | | |
| | | - Có tính năng Firewall, kiểm soát theo ứng dụng Application Control/App-ID, phòng chống xâm nhập (IPS), Antivirus/Antimalware; | | |
| | | - Có tính năng lọc web URL-Filtering theo các danh mục (category); | | |
| | | - Có menu riêng để cấu hình chính sách giải mã SSL, độc lập với menu cấu hình chính sách kiểm soát truy cập | | |
| | | - Có khả năng kéo thả, di chuyển các đối tượng object (address, application…) giữa các Security Rule; | | |
| | | - Có khả năng chuyển tiếp các yêu cầu DNS request đến tên miền độc hại (malicious domain) tới một địa chỉ IP đích định nghĩa trước (DNS sinkhole/DNS trap), áp dụng cho mọi loại ứng dụng; | | |
| | | - Giao diện quản trị đồ hoạ web, CLI, và qua API để quản trị thiết bị; | | |
| | | - Có chức năng phân tích log và báo cáo tổng hợp; | | |
| | | - Yêu cầu trang bị sẵn các tính năng IPS, Application Control, Antivirus, URL Filtering hoặc tương đương có hiệu lực ≥03 năm; | | |
| | | - Bảo hành: ≥3 năm theo tiêu chuẩn của nhà sản xuất. | | |
| 4 | Thiết bị tường lửa cho ứng dụng Web | - Thiết kế dạng rackmount hoặc tương đương | Thiết bị | 2 |
| | | - Băng thông ứng dụng (Application Throughput): ≥10 Gbps; | | |
| | | - Cổng kết nối 1Gbps đồng (RJ45) hoặc tương đương: ≥6; | | |
| | | - Cổng kết nối 10Gbps quang SFP+: ≥4; | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Bộ nhớ (RAM) ≥ 24 GB; | | |
| | | - Số lượng kết nối SSL mỗi giây (SSL CPS/TPS) sử dụng thuật toán mã hóa RSA: ≥ 7500; | | |
| | | - Thiết bị có tối thiểu 2 nguồn AC; | | |
| | | - Có sẵn tính năng cấu hình HA (Active/Active hoặc Active/Standby); | | |
| | | - Có sẵn tính năng cân bằng tải ứng dụng lớp 4/lớp 7 (Advanced Layer 4/Layer7 server load balancing) | | |
| | | - Chống tấn công OWASP Top 10 (OWASP Top 10 Protection); | | |
| | | - Chống tấn công Bot độc hại (Malicious bots Protection); | | |
| | | - Giới hạn số lượng truy cập (Advanced Rate Limiting) | | |
| | | - Phần cứng hỗ trợ SSL Offloading/Offloading TLS; | | |
| | | - Chống tấn công chiếm quyền tài khoản (Account takeover (ATO) protection); | | |
| | | - Tích hợp khả năng chống DDoS (Integrated DDoS protection); | | |
| | | - Ngăn chặn truy cập theo vị trí địa lý (Geolocation-based Blocking); | | |
| | | - Hỗ trợ quản trị GUI, CLI, SSH, SNMP; | | |
| | | - Thời gian bảo hành theo tiêu chuẩn của nhà sản xuất: ≥3 năm | | |
| 5 | Bản quyền thông lượng WAF (WAF Throughput) | - Tổng thông lượng (WAF Throughput): ≥20GB;<br>- Khả năng phân bổ thông lượng: Có khả năng phân bổ thông lượng linh hoạt cho tối thiểu 15 thiết bị WAF.<br>- Thời gian sử dụng: ≥3 năm | Bộ | 1 |
| **III** | **Hệ thống thiết bị phân tích phát hiện các mối nguy an ninh mạng (IDS/APT)** | | | |
| 1 | Thiết bị gom lưu lượng mạng | - Thiết kế dạng rack mount; | Thiết bị | 4 |
| | | - Số lượng cổng quang tốc độ 1G/10G/25G hoặc tương đương: ≥48; | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Số lượng cổng quang tốc độ 40G/100G hoặc tương đương: ≥8; | | |
| | | - Thông lượng thiết bị: ≥2 Tbps; | | |
| | | - Có sẵn tính năng lọc ≥256 quy tắc Flow mapping filter hoặc filter rule; | | |
| | | - Có sẵn tính năng tổng hợp nhiều luồng SPAN, TAP vào các đường liên kết tốc độ cao hơn; | | |
| | | - Có sẵn tính năng lọc gói tin từ lớp 2 đến lớp 4; | | |
| | | - Có sẵn tính năng cân bằng tải dựa theo mã băm; | | |
| | | - Hỗ trợ tối ưu hóa phân phối lưu lượng mạng tới các công cụ bảo mật trong hệ thống; | | |
| | | - Phần mềm quản trị: Có sẵn phần mềm để thực hiện cấu hình quản trị thiết bị; | | |
| | | - Khả năng kích hoạt thêm các tính năng (license mở rộng) nếu có nhu cầu:<br>1.Clustering với các thiết bị tổng hợp lưu lượng khác<br>2. Giải đóng gói (Decapsulation) L2GRE/VXLAN Tunnelling<br>3. Đóng gói (Encapsulation) L2GRE/VXLAN Tunnelling<br>4. Loại bỏ header MPLS/VXLAN (Header Stripping) | | |
| | | - Nguồn thiết bị: ≥02 nguồn AC. | | |
| | | - Bảo hành: ≥3 năm theo tiêu chuẩn của nhà sản xuất. | | |
| 2 | Thiết bị phân tích trung tâm | - Thiết kế dạng rack mount hoặc tương đương; | Thiết bị | 4 |
| | | - Có khả năng chạy cluster, hoặc mua thêm bản quyền để tăng năng lực lưu trữ, xử lý; | | |
| | | - Tổng dung lượng lưu trữ của hệ thống: ≥80TB metadata; | | |
| | | - Cổng kết nối: ≥02 cổng 1GigE RJ45 hoặc ≥02 cổng SFP+; | | |
| | | - Thiết bị có sẵn ≥02 nguồn AC 240V; | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Liên tục giám sát, phát hiện, điều tra và ngăn chặn các mối đe dọa mới trên mạng theo thời gian thực; | | |
| | | - Quan trắc các tài sản, các sự kiện, cảnh báo liên quan; | | |
| | | - Có sẵn tính năng tích hợp nhận metadata từ các cảm biến NDR Sensor/Network APT, IPS, Network Packet Capture; | | |
| | | - Có sẵn tính năng tích hợp nhận thông tin làm giàu từ Endpoint Security, Vulnerability Management, Threat Intelligence; | | |
| | | - Tích hợp sẵn GenAI để hỗ trợ phân tích và làm giảm các cảnh báo sai; tổng hợp, tóm tắt các vấn đề chính và các chi tiết quan trọng của cảnh báo; | | |
| | | - Có sẵn GenAI hiển thị các thực thể bị ảnh hưởng nhiều nhất, thể hiện trực quan dạng biểu đồ tình huống các thực thể liên quan tới cảnh báo; | | |
| | | - Có sẵn GenAI khuyến nghị các bước khắc phục, phản ứng, hành động có thể để xử lý, khắc phục cảnh báo; | | |
| | | - Hiển thị bảng tham chiếu MITRE: các kỹ/chiến thuật liên quan tới cảnh báo; | | |
| | | - Bảo hành và hỗ trợ kỹ thuật: ≥36 tháng. | | |
| 3 | Thiết bị cảm biến trung tâm | - Thiết bị phần cứng chuyên dụng, rackmount; | Thiết bị | 4 |
| | | - Năng lực xử lý ≥5Gbps và có khả năng mở rộng lên ≥10Gbps; | | |
| | | - Cổng kết nối: ≥2 ports 1/10GigE RJ45 hoặc tương đương, ≥4 ports 10GigE SFP+ hoặc tương đương, ≥2 ports 40G QSFP+ hoặc ≥2 port 100G QSFP28 hoặc tương đương; | | |
| | | - Cổng quản lý: ≥02 1GigE RJ45 hoặc tương đương; | | |
| | | - Dung lượng lưu trữ: cấu hình RAID hỗ trợ dự phòng khi xảy ra sự cố hỏng ổ cứng, dung lượng lưu trữ khả dụng ≥8 TB; | | |
| | | - Số lượng Sanbox tích hợp sẵn hoặc ghép nối với tổng Sandbox: ≥160VM; | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Thiết bị có sẵn ≥02 nguồn AC; | | |
| | | - Chế độ hoạt động: In-line monitor, fail-open (bypass) or TAP/ SPAN; | | |
| | | - Sử dụng các công nghệ phân tích phát hiện mối nguy hệ thống mạng, file, Web, sử dụng công nghệ sandbox, có công nghệ Machine Learning; | | |
| | | - Phát hiện, ngăn chặn các kiểu tấn công nâng cao (zero-day), làm rối (obfuscated), có chủ đích (targeted), ngăn chặn các kết nối C&C; | | |
| | | - Phát hiện và cảnh báo đối với các hành vi tấn công qua mạng nội bộ như: Internal Reconnaissance, Privilege Escalation,Lateral Movement of Malware, Data Exfiltration Detection; | | |
| | | - Các cảm biến cung cấp metadata và nhật ký phát hiện để thực hiện liên kết dữ liệu và phân tích mối đe dọa nâng cao; | | |
| | | - Hỗ trợ nền tảng thực thi ảo ngay trên thiết bị và cho phép tích hợp với thiết bị Sandbox chuyên dụng của cùng hãng; | | |
| | | - Các cảm biến được quản lý tập trung, chia sẻ thông tin tri thức tình báo mối nguy thời gian thực để nhận diện và ngăn chặn các tấn công nâng cao; | | |
| | | - Bảo hành và hỗ trợ kỹ thuật: ≥36 tháng. | | |
| 4 | Thiết bị phân tích mã độc Sandbox | - Thiết bị phần cứng chuyên dụng, rackmount; | Thiết bị | 4 |
| | | - Năng lực xử lý: ≥15.000 mẫu/ngày; | | |
| | | - Cổng kết nối song hành/nhận mẫu: ≥02 ports 1Gbps RJ45 hoặc tương đương; | | |
| | | - Cổng quản lý: ≥01 ports 1Gbps RJ45 hoặc tương đương; | | |
| | | - Dung lượng lưu trữ: ≥2 ổ cứng ≥4TB, RAID1; | | |
| | | - Nguồn: ≥02 khối nguồn AC, dự phòng nóng hot-swap; | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Hỗ trợ chạy song hành (cluster/grid) hoặc gồm nhiều thiết bị để mở rộng số lượng sandbox; | | |
| | | - Phân tích mã độc sử dụng nhiều cơ chế phân tích tĩnh, phân tích động (sandboxing) không dùng mẫu bảo mật, sử dụng ML/AI. Phát hiện các tấn công zero-day, APT có chủ đích, phát hiện các mã độc, khai thác chưa từng thấy trước đó; | | |
| | | - Môi trường phân tích thực thi ảo: Hỗ trợ trên các hệ điều hành Sandbox gồm tối thiểu Windows, MacOS; | | |
| | | - Cho phép phân tích các URL được nhúng trong email hoặc file; | | |
| | | - Có sẵn tính năng phân tích nhiều định dạng file khác nhau, tối thiểu bao gồm: portable executables (PEs), web content, archives, images, Java, Microsoft; | | |
| | | - Có sẵn tính năng phân tích các loại file tối thiểu bao gồm: chm, class, dll, doc, docx, exe, jar, js, jse, jtd, lnk, mov, pdf, ppt, pptx, ps1, rtf, swf, vbs, xls, xlsx, xml; | | |
| | | - Bảo hành và hỗ trợ kỹ thuật: ≥36 tháng. | | |
| **IV** | **Phần mềm phân tích phát hiện các mối nguy an ninh mạng (IDS/APT)** | | | |
| 1 | Bản quyền cho Hệ thống Phân tích, phát hiện các mối nguy an ninh mạng tại trung tâm chính | - Bản quyền cho Hệ thống Phân tích, phát hiện các mối nguy an ninh mạng; | Bộ | 1 |
| | | - Bản quyền xử lý ≥1Gbp băng thông mạng, có khả năng nâng cấp mở rộng; | | |
| | | - Phát hiện và ngăn chặn các mối nguy mới, zero day sử dụng công nghệ không sử dụng mẫu, tương quan nhiều chiều, phát hiện các lây lan đi ngang trong hệ thống; | | |
| | | - Có sẵn tính năng triển khai bắt gói tin và điều tra sâu (Forensics), săn tìm mối nguy; | | |
| | | - Có sẵn tính năng các khả năng phản ứng: xem xét ngữ cảnh, tổng hợp thông tin điều tra, phân loại ưu tiên, điều tra sâu; | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Dịch vụ bảo hành, hỗ trợ kỹ thuật: ≥36 tháng. | | |
| 2 | Bản quyền cho Hệ thống Phân tích, phát hiện các mối nguy an ninh mạng tại Đài KSKL | - Bản quyền cho Hệ thống Phân tích, phát hiện các mối nguy an ninh mạng;<br>- Bản quyền xử lý ≥1Gbp băng thông mạng, có khả năng nâng cấp mở rộng;<br>- Phân tích thời gian thực, phát hiện và ngăn chặn tức thời các tấn công nâng cao, có chủ đích, khai thác điểm yếu của hệ điều hành và ứng dụng;<br>- Phát hiện các mã độc nâng cao, ransomware, Callback (C&C) connection, khai thác điểm yếu, các hành vi trốn tránh, phát hiện các lây lan đi ngang;<br>- Dịch vụ bảo hành, hỗ trợ kỹ thuật: ≥36 tháng. | Bộ | 1 |
| 3 | Phân tích, phát hiện các mối nguy an ninh mạng - Cảm biến ảo hóa | - Cảm biến ảo hóa chuyên dụng (virtual appliance);<br>- Năng lực xử lý lên tới ≥8Gbps;<br>- Số lượng cổng giám sát: ≥4;<br>- Chế độ hoạt động: ngoại tuyến (Out-of-Band of SPAN);<br>- Tích hợp với Thiết bị phân tích trung tâm tại Công ty miền, Thiết bị phân tích mã độc nâng cao tại Công ty miền;<br>- Hỗ trợ các nền tảng ảo hóa, tối thiểu gồm: ESXi, KVM, Hyper-V. | Bộ | 4 |
| **B** | **Giải pháp quản lý giám sát vận hành** | | | |
| **I** | **Hệ thống thiết bị phần cứng phục vụ giám sát, hỗ trợ vận hành** | | | |
| 1 | Máy tính quản trị giám sát vận hành | - Khuôn dạng: Tower;<br>- Bộ vi xử lý: ≥ Intel Core i3-14100 hoặc tương đương;<br>- Bộ nhớ: ≥16 GB Up to 64 GB RAM;<br>- Ổ cứng: ≥512GB SSD;<br>- Cổng kết nối tối thiểu: 2 USB; 02 x HDMI port; 1 x RJ45 Port;<br>- Hệ điều hành: Windows 11 Pro; | Thiết bị | 4 |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Keyboard + Mouse; | | |
| | | - Bảo hành ≥12 tháng theo tiêu chuẩn hãng. | | |
| 2 | Màn hình giám sát | - Hiển thị: ≥ 55 inches | Thiết bị | 4 |
| | | - Độ phân giải: ≥ 3,840 x 2,160 | | |
| | | - Kết Nối: ≥ 3 HDMI | | |
| | | - Độ sáng: ≥ 500 cd/m2 | | |
| | | - Góc nhìn: ≥ 178 x 178 | | |
| | | - Thời gian hoạt động (Giờ/ Ngày): 24/7 | | |
| | | - Đèn nền: E-LED hoặc tương đương | | |
| | | - Thời gian bảo hành: ≥ 24 tháng | | |
| 3 | Thiết bị chuyển mạch quản lý | - Thiết kế dạng rackmount; | Thiết bị | 7 |
| | | - Cổng kết nối tối thiểu: ≥48 cổng 10/100/1000 Mbps hoặc tương đương; ≥8 cổng 1/10Gbps SFP+ hoặc tương đương; | | |
| | | - Tốc độ chuyển mạch (Switching capacity): ≥ 256Gbps; | | |
| | | - Tốc độ chuyển tiếp dữ liệu (Forwarding rate): ≥ 190Mpps; | | |
| | | - Số lượng địa chỉ MAC hoặc bảng MAC: ≥ 32,000; | | |
| | | - Số nhóm LAG tối đa có thể tạo (LAG groups): ≥ 128 | | |
| | | - Hỗ trợ khả năng xếp chồng; | | |
| | | - Có sẵn tính năng AVB: Có khả năng truyền tải Audio/Video qua môi trường Ethernet theo thời gian thực; | | |
| | | - Giao thức định tuyến:; | | |
| | | - Khả năng quản lý: giao diện dòng lệnh CLI, giao thức SSH, SNMP và giao diện web (GUI); | | |
| | | - Bảo hành: ≥3 năm theo tiêu chuẩn của nhà sản xuất. | | |
| 4 | | - Kiểu dáng: Rack mounted ≥ 1U; | Thiết bị | 9 |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | Máy chủ quản lý giám sát | - Bộ vi xử lý: 02 x Intel Xeon Gold 32 Cores, xung nhịp ≥2.5GHz thế hệ 5 hoặc tương đương; | | |
| | | - Bộ nhớ: ≥ 256GB; Khả năng nâng cấp mở rộng lên tới 32 khe cắm DIMMM, dung lượng tối đa lên tới ≥8 TB; | | |
| | | - Ổ cứng: ≥04 ổ cứng dung lượng ≥1.92TB SSD; Khả năng nâng cấp mở rộng lên tới ≥ 12 ổ cứng SAS/SATA; | | |
| | | - Bộ điều khiển RAID: Hỗ trợ tối thiểu RAID 1, 5, 6; 8 GB Cache; | | |
| | | - Kết nối mạng: ≥04 x 1GbE; | | |
| | | - PCIe slot: ≥3; | | |
| | | - OS hỗ trợ tối thiểu: Windows Server; Red Hat Enterprise Linux; VMware ESXi; | | |
| | | - Nguồn cấp: ≥02 nguồn AC; | | |
| | | - Bảo hành: ≥3 năm theo tiêu chuẩn của nhà sản xuất. | | |
| 5 | Phụ kiện triển khai | Có các phụ kiện triển khai kèm theo: cáp điện, cáp mạng, hạt mạng, dây thít, phụ kiện khác (đầy đủ để lắp đặt các thiết bị trong dự án). | Gói | 4 |
| **II** | **Phần mềm thương mại phục vụ công tác giám sát, hỗ trợ vận hành** | | | |
| 1 | Phần mềm Quản lý giám sát mạng (NMS) | - Có khả năng giám sát hệ thống hạ tầng CNTT: thiết bị mạng/bảo mật, máy chủ, phần mềm hệ thống, website URL…; | Gói | 1 |
| | | - License phần mềm: 100 nodes | | |
| | | + Không giới hạn thành phần được quản lý trên từng thiết bị như CPU, RAM, volume, interface, fan, temperature...; | | |
| | | + Không giới hạn thành phần xử lý và hiển thị cho hệ thống giám sát; | | |
| | | + Cho phép triển khai theo mô hình High Availability. Triển khai HA cho toàn bộ các thành phần thu thập, xử lý trong hệ thống; | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | + Cho phép triển khai theo mô hình multi-tenant, tối thiểu là 3 tenants tương ứng với 3 miền; dữ liệu tại các khu vực được lưu trữ riêng biệt, một số thông tin có thể được cấu hình đồng bộ về trung tâm; | | |
| | | - Giải pháp có khả năng giám sát nhiều loại thiết bị như Router, Switch, Firewall, Wireless, Server và các thiết bị hỗ trợ giao thức SNMP; | | |
| | | - Có khả năng tìm kiếm và khắc phục sự cố đường mạng theo hop-by-hop cho môi trường On-Premise và Cloud; | | |
| | | - Có khả năng giám sát sức khỏe phần cứng của các nhà cung cấp phổ biến như: Cisco, Dell, F5, Juniper, HP, Fortinet, Juniper, Extreme, Palo Alto,…; | | |
| | | - Có khả năng thu thập và phân tích dữ liệu Flow từ nhiều hãng bao gồm Netflow v5, v9, Juniper® J-Flow™, sFlow®, Huawei® NetStream™…; | | |
| | | - Xác định các người dùng, ứng dụng, và giao thức mạng đang tiêu thụ nhiều băng thông nhất; hiển thị Top các địa chỉ IP tiêu thụ băng thông và tìm ra việc sử dụng băng thông không mong muốn; | | |
| | | - Giám sát theo thời gian thực các tiến trình chạy trong hệ thống và thống kê hiệu suất ứng dụng; | | |
| | | - Khả năng thu thập, hợp nhất và phân tích các thông tin từ nhiều môi trường như Syslog, SNMP traps, Windows, Vmware; | | |
| | | - Khả năng xem log theo thời gian thực; | | |
| | | - Cung cấp bảng điều khiển động (dynamic dashboard) có khả năng kéo thả các metric từ nhiều nguồn để so sánh và trực quan hóa số liệu trên một chế độ xem duy nhất, giúp giám sát chuyên sâu và tương quan các dữ liệu lịch sử trên các thành phần khác nhau của cơ sở hạ tầng; | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Cho phép xuất báo cáo qua các định dạng Excel, PDF, XML, Html, và hình ảnh;<br>- Tích hợp sẵn công nghệ AIOps (Artificial Intelligence for IT Operations);<br>- Bản quyền và hỗ trợ kỹ thuật ≥3 năm. | | |
| 2 | Phần mềm quản trị CSDL | Bản quyền Microsoft SQL Server 2022 Standard (hoặc tương thích với giải pháp) | Bộ | 4 |
| 3 | Hệ điều hành máy chủ quản lý giám sát | - Bản quyền Microsoft Windows Server 2025 Standard dạng 2 core pack (cho các máy chủ loại 2CPUx32 cores)<br>- Bản quyền Microsoft Windows Server 2025 Standard (CAL) (một bộ gồm 5 CAL)<br>(hoặc tương thích với giải pháp) | Bộ | 9 |
| **C** | **Thiết bị dự phòng** | | | |
| 1 | Thiết bị chuyển mạch cho hệ thống thông tin cấp độ 4 (có thể dùng cho HTTT cấp độ 3 nếu cần) | - Thiết kế dạng rackmount hoặc tương đương;<br>- Số cổng kết nối tối thiểu:<br>+ ≥24 cổng tốc độ 1G/10G SFP+ hoặc tương đương;<br>+ ≥02 cổng QSFP28 tốc độ ≥40Gbps hoặc tương đương;<br>- Module kèm theo:<br>+ Tối thiểu 14 module đồng 1000BASE-T hoặc tương đương;<br>+ Tối thiểu 10 module quang tốc độ 10Gbps chuẩn SR hoặc tương đương;<br>- Tốc độ chuyển mạch (Switching capacity): ≥ 1000 Gbps;<br>- Tốc độ chuyển tiếp dữ liệu (Forwarding rate): ≥ 800 Mpps;<br>- Số lượng địa chỉ MAC hoặc bảng MAC: ≥ 32,000;<br>- Số lượng mạng lan ảo (VLANs): ≥ 4094;<br>- Khung jumbo (Jumbo Frames): ≥ 9198 Bytes;<br>- Số nhóm LAG (LAG groups): ≥ 128 | Thiết bị | 3 |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Đáp ứng các tiêu chuẩn quốc tế: IEEE 802.1d, IEEE 802.1w, IEEE 802.1p, IEEE 802.1Q, IEEE 802.3ad, IEEE 802.1s; | | |
| | | - Có sẵn tính năng truyền tải Audio/Video qua môi trường Ethernet theo thời gian thực; | | |
| | | - Hỗ trợ khả năng xếp chồng; | | |
| | | - Hỗ trợ các giao thức định tuyến: RIPv1/v2, BGP, EVPN, VXLAN, Định tuyến theo chính sách (PBR) cho IPV4 và IPV6; | | |
| | | - Có sẵn các giao thức định tuyến: Tĩnh, OSPF, IS-IS; | | |
| | | - Giao diện dòng lệnh CLI, giao thức SSH và SNMP và giao diện web (GUI) | | |
| | | - Nguồn điện: ≥02 nguồn dự phòng với dải điện áp 220V-240V; | | |
| | | - Bảo hành: ≥3 năm theo tiêu chuẩn của nhà sản xuất. | | |
| 2 | Thiết bị chuyển mạch quản lý | - Thiết kế dạng rackmount; | Thiết bị | 4 |
| | | - Cổng kết nối tối thiểu: ≥48 cổng 10/100/1000 Mbps hoặc tương đương; ≥8 cổng 1/10Gbps SFP+ hoặc tương đương; | | |
| | | - Tốc độ chuyển mạch (Switching capacity): ≥ 256Gbps; | | |
| | | - Tốc độ chuyển tiếp dữ liệu (Forwarding rate): ≥ 190Mpps; | | |
| | | - Số lượng địa chỉ MAC hoặc bảng MAC: ≥ 32,000; | | |
| | | - Số nhóm LAG tối đa có thể tạo (LAG groups): ≥ 128 | | |
| | | - Hỗ trợ khả năng xếp chồng; | | |
| | | - Có sẵn tính năng AVB: Có khả năng truyền tải Audio/Video qua môi trường Ethernet theo thời gian thực; | | |
| | | - Giao thức định tuyến: RIPv1/v2, Định tuyến theo chính sách (PBR) cho IPV4 và IPV6; Có sẵn các giao thức định tuyến: OSPF, IS-IS, Tĩnh (Static); | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Khả năng quản lý: giao diện dòng lệnh CLI, giao thức SSH, SNMP và giao diện web (GUI); | | |
| | | - Nguồn điện: tối thiểu 1 nguồn cấp AC; | | |
| | | - Bảo hành: ≥3 năm theo tiêu chuẩn của nhà sản xuất. | | |
| 3 | Thiết bị tường lửa vùng lõi cho hệ thống thông tin cấp độ 4 (có thể dùng cho vùng biên nếu cần) | - Thiết kế dạng rackmount hoặc tương đương; | Thiết bị | 3 |
| | | - Thông lượng Threat Prevention/Threat Protection đo với traffic hỗn hợp appmix/enterprisemix ≥ 4.5 Gbps; | | |
| | | - New session per second/connection per second ≥ 90.000; | | |
| | | - Số cổng kết nối tối thiểu: | | |
| | | + Cổng đồng 1Gbps: ≥8; | | |
| | | + Cổng quang 1 Gbps SFP: ≥6; | | |
| | | + Cổng quang 10Gbps SFP+: ≥4 cổng (trang bị sẵn ≥02 transceiver tốc độ ≥10Gbps chuẩn SR); | | |
| | | + Cổng high availability (HA): ≥01; | | |
| | | - Nguồn điện: | | |
| | | + Tối thiểu 02 nguồn, hỗ trợ dự phòng redundant; | | |
| | | + Dải điện áp 220V-240V; | | |
| | | - Giao thức định tuyến: OSPF, BGP, static routing; | | |
| | | - Có sẵn tính năng High availability cấu hình Active/Active hoặc Active/Passive; | | |
| | | - Có tính năng tường lửa, kiểm soát theo ứng dụng Application Control/App-ID, phòng chống xâm nhập (IPS), Antivirus/Antimalware; | | |
| | | - Có tính năng lọc web URL-Filtering theo các danh mục (category); | | |
| | | - Có khả năng tuỳ biến các IPS signature, cho phép chuyển đổi / import cú pháp signature từ Snort sang ngay trên Firewall; | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Có menu riêng để cấu hình chính sách giải mã SSL, độc lập với menu cấu hình chính sách kiểm soát truy cập | | |
| | | - Có khả năng kéo thả, di chuyển các đối tượng object (address, application…) giữa các Security Rule; | | |
| | | - Có khả năng chuyển tiếp các yêu cầu DNS request đến tên miền độc hại (malicious domain) tới một địa chỉ IP đích định nghĩa trước (DNS sinkhole/DNS trap), áp dụng cho mọi loại ứng dụng; | | |
| | | - Giao diện quản trị đồ hoạ web, CLI và qua API để quản trị thiết bị; | | |
| | | - Có chức năng phân tích log và báo cáo tổng hợp; | | |
| | | - Yêu cầu trang bị sẵn tối thiểu các tính năng IPS, Application Control, Antivirus, URL Filtering hoặc tương đương có hiệu lực ≥03 năm; | | |
| | | - Bảo hành: ≥3 năm theo tiêu chuẩn của nhà sản xuất. | | |
| 4 | Thiết bị tường lửa cho hệ thống thông tin cấp độ 3 | - Thiết kế dạng rackmount hoặc tương đương; | Thiết bị | 3 |
| | | - Thông lượng Threat Prevention/Threat Protection đo với traffic hỗn hợp appmix/enterprisemix ≥ 1 Gbps | | |
| | | - Số lượng phiên kết nối mới mỗi giây: ≥ 30.000; | | |
| | | - Số cổng kết nối tối thiểu: | | |
| | | + Cổng đồng 1Gbps: ≥6; | | |
| | | + Cổng quang 1 Gbps SFP: ≥01; | | |
| | | - Dung lượng lưu trữ: ≥ 128 GB; | | |
| | | - Nguồn điện: Nguồn AC có dải điện áp 100V-240V; | | |
| | | - Giao thức định tuyến: OSPF, BGP, static routing; | | |
| | | - Có sẵn tính năng High availability cấu hình Active/Active hoặc Active/Passive; | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Có tính năng Firewall, kiểm soát theo ứng dụng Application Control/App-ID, phòng chống xâm nhập (IPS), Antivirus/Antimalware; | | |
| | | - Có tính năng lọc web URL-Filtering theo các danh mục (category); | | |
| | | - Có menu riêng để cấu hình chính sách giải mã SSL, độc lập với menu cấu hình chính sách kiểm soát truy cập | | |
| | | - Có khả năng kéo thả, di chuyển các đối tượng object (address, application…) giữa các Security Rule; | | |
| | | - Có khả năng chuyển tiếp các yêu cầu DNS request đến tên miền độc hại (malicious domain) tới một địa chỉ IP đích định nghĩa trước (DNS sinkhole/DNS trap), áp dụng cho mọi loại ứng dụng; | | |
| | | - Giao diện quản trị đồ hoạ web, CLI, và qua API để quản trị thiết bị; | | |
| | | - Có chức năng phân tích log và báo cáo tổng hợp; | | |
| | | - Yêu cầu trang bị sẵn các tính năng IPS, Application Control, Antivirus, URL Filtering hoặc tương đương có hiệu lực ≥03 năm; | | |
| | | - Bảo hành: ≥3 năm theo tiêu chuẩn của nhà sản xuất. | | |
| 5 | Thiết bị tường lửa cho ứng dụng Web | - Thiết kế dạng rackmount hoặc tương đương | Thiết bị | 1 |
| | | - Băng thông ứng dụng (Application Throughput): ≥10 Gbps; | | |
| | | - Cổng kết nối 1Gbps đồng (RJ45) hoặc tương đương: ≥6; | | |
| | | - Cổng kết nối 10Gbps quang SFP+: ≥4; | | |
| | | - Bộ nhớ (RAM) ≥ 24 GB; | | |
| | | - Số lượng kết nối SSL mỗi giây (SSL CPS/TPS) sử dụng thuật toán mã hóa RSA: ≥ 7500; | | |
| | | - Thiết bị có tối thiểu 2 nguồn AC; | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Có sẵn tính năng cấu hình HA (Active/Active hoặc Active/Standby); | | |
| | | - Có sẵn tính năng cân bằng tải ứng dụng lớp 4/lớp 7 (Advanced Layer 4/Layer7 server load balancing) | | |
| | | - Chống tấn công OWASP Top 10 (OWASP Top 10 Protection); | | |
| | | - Chống tấn công Bot độc hại (Malicious bots Protection); | | |
| | | - Giới hạn số lượng truy cập (Advanced Rate Limiting) | | |
| | | - Phần cứng hỗ trợ SSL Offloading/Offloading TLS; | | |
| | | - Chống tấn công chiếm quyền tài khoản (Account takeover (ATO) protection); | | |
| | | - Tích hợp khả năng chống DDoS (Integrated DDoS protection); | | |
| | | - Ngăn chặn truy cập theo vị trí địa lý (Geolocation-based Blocking); | | |
| | | - Hỗ trợ quản trị GUI, CLI, SSH, SNMP; | | |
| | | - Bảo hành thiết bị ≥3 năm theo tiêu chuẩn của nhà sản xuất. | | |
| 6 | Máy chủ quản lý giám sát | - Kiểu dáng: Rack mounted ≥ 1U; | Thiết bị | 2 |
| | | - Bộ vi xử lý: 02 x Intel Xeon Gold 32 Cores, xung nhịp ≥2.5GHz thế hệ 5 hoặc tương đương; | | |
| | | - Bộ nhớ: ≥ 256GB; Khả năng nâng cấp mở rộng lên tới 32 khe cắm DIMMM, dung lượng tối đa lên tới ≥8 TB; | | |
| | | - Ổ cứng: ≥04 ổ cứng ≥1.92TB SSD; Khả năng nâng cấp mở rộng lên tới ≥ 12 ổ cứng SAS/SATA; | | |
| | | - Bộ điều khiển RAID: Hỗ trợ tối thiểu RAID 1, 5, 6; 8 GB Cache; | | |
| | | - Kết nối mạng: ≥04 x 1GbE; | | |
| | | - PCIe slot: ≥3; | | |
| | | - OS hỗ trợ tối thiểu: Windows Server; Red Hat Enterprise Linux; VMware ESXi; | | |

| STT | Danh mục hàng hóa | Thông số kỹ thuật | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | - Nguồn cấp: ≥02 nguồn AC; | | |
| | | - Bảo hành: ≥3 năm theo tiêu chuẩn của nhà sản xuất. | | |
| 7 | Máy tính quản trị giám sát vận hành | - Khuôn dạng: Tower; | Thiết bị | 2 |
| | | - Bộ vi xử lý: ≥ Intel Core i3-14100 hoặc tương đương; | | |
| | | - Bộ nhớ: ≥16 GB Up to 64 GB RAM; | | |
| | | - Ổ cứng: ≥512GB SSD; | | |
| | | - Cổng kết nối tối thiểu: 2 USB; 02 x HDMI port; 1 x RJ45 Port; | | |
| | | - Hệ điều hành: Windows 11 Pro; | | |
| | | - Keyboard + Mouse; | | |
| | | - Bảo hành ≥12 tháng theo tiêu chuẩn hãng. | | |
| 8 | Màn hình giám sát | - Hiển thị: ≥ 55 inches | Thiết bị | 2 |
| | | - Độ phân giải: ≥ 3,840 x 2,160 | | |
| | | - Kết Nối: ≥ 3 HDMI | | |
| | | - Độ sáng: ≥ 500 cd/m2 | | |
| | | - Góc nhìn: ≥ 178 x 178 | | |
| | | - Thời gian hoạt động (Giờ/ Ngày): 24/7 | | |
| | | - Đèn nền: E-LED hoặc tương đương | | |
| | | - Thời gian bảo hành: ≥ 24 tháng | | |

*1.2.4.2. Yêu cầu về sơ đồ và thuyết minh quy hoạch địa chỉ mạng IP*

Nhà thầu phải thực hiện quy hoạch địa chỉ mạng IP trong quá trình triển khai thực tế tại mỗi hệ thống, với mỗi quy hoạch IP hiện có và thiết kế mới được xây dựng sẽ quy hoạch địa chỉ mạng IP phù hợp, đáp ứng nhu cầu sử dụng.

*1.2.4.3. Yêu cầu về Sơ đồ lắp đặt thiết bị*

Toàn bộ trang thiết bị, giải pháp được trang bị trong dự án sẽ được phân bổ về các hệ thống được đặt tại các Trung tâm, Đài kiểm soát không lưu và các Công ty quản lý bay Miền (theo điểm 1.1.6. Phạm vi cung cấp). Dựa theo tình trạng lắp đặt thực tế, các trang thiết bị/giải pháp bổ sung sẽ được lắp đặt hợp lý tại các Rack đặt tại các Phòng máy của từng đơn vị, đảm bảo quá trình vận hành và khai thác ổn định.

*1.2.4.4. Chỉ dẫn biện pháp triển khai*

*1.2.4.4.1. Nhận thiết bị và kiểm tra thiết bị*

Nhà thầu phải cam kết và cung cấp hồ sơ tài liệu chứng minh tính đáp ứng, thực hiện đầy đủ các yêu cầu về việc nhận thiết bị và kiểm tra thiết bị như sau:

- Chứng nhận xuất xứ (nếu có); Chứng chỉ chất lượng; Số lượng; Kích thước; Tài liệu kỹ thuật; Thông số kỹ thuật.
- Trước khi lắp đặt: Kiểm tra mặt bằng tại vị trí lắp đặt thiết bị.
- Sau khi lắp đặt: Kiểm tra đối chiếu với bản vẽ thiết kế và hồ sơ tài liệu, hướng dẫn của Nhà sản xuất; kiểm tra kết nối (nếu có).
- Quá trình chạy thử: Kiểm tra đối chiếu các tính năng và thông số kỹ thuật thiết bị.
- Khi vật tư, thiết bị không có số liệu, không có chứng chỉ chất lượng hoặc có các sai biệt thì sẽ lập biên bản về khác biệt để xử lý.

*1.2.4.4.2. Yêu cầu về an toàn lao động, đảm bảo an ninh bảo mật*

Về an toàn lao động, lắp đặt hệ thống: phải đảm bảo chống cháy, nổ, điện giật, sét, tránh rơi hỏng, rơi rớt thiết bị xuống mặt đất làm hư hại thiết bị, an toàn cho người khi xảy ra sự cố.

Nhà thầu phải tuân thủ các quy định hiện hành và Quy định đã ban hành của Tổng công ty Quản lý bay Việt Nam. Nhà thầu phải tổ chức thi công cùng các biện pháp bảo vệ môi trường ở trong và ngoài khu vực thi công nhằm tránh gây thiệt hại về tài sản và người ở khu vực thi công và khu vực lân cận.

*1.2.4.4.3. Biện pháp đảm bảo an toàn lao động*

Trong quá trình xây dựng, triển khai và đưa vào vận hành, khai thác sử dụng, Nhà thầu phải đảm bảo thực hiện đúng các biện pháp đảm bảo an toàn lao động, bảo vệ môi trường và các quy định hiện hành của Nhà nước.

## *1.3. Các yêu cầu khác*

### *1.3.1. Yêu cầu về Biện pháp an toàn vận hành, phòng, chống cháy, nổ*

Nhà thầu phải tuân thủ các Quy định đã ban hành của Tổng công ty Quản lý bay Việt Nam về an toàn vận hành, phòng, chống cháy, nổ.

### *1.3.2. Yêu cầu về dịch vụ triển khai, dịch vụ huấn luyện khai thác, quản trị hệ thống*

*1.3.2.1. Yêu cầu về triển khai, hỗ trợ, quản trị, vận hành sản phẩm hoặc hạng mục công việc của dự án trước khi nghiệm thu bàn giao*

Nhà thầu căn cứ trên danh mục thiết bị, phân bổ thiết bị, giải pháp, yêu cầu về

tiến độ lên trình bày phương pháp luận, phương án, kế hoạch cung cấp dịch vụ lắp đặt, cài đặt, triển khai công nghệ, tích hợp hệ thống đối với các thiết bị mạng, thiết bị bảo mật, triển khai các hệ thống phân tích phát hiện các mối nguy an ninh mạng (IDS/APT), hệ thống quản lý giám sát vận hành (NMS) hợp lý, khả thi.

Hạ tầng kỹ thuật, phần mềm thương mại được mua sắm sẽ được triển khai lắp đặt, cài đặt theo phạm vi quy mô đầu tư của dự án tại các hệ thống thành phần của các đơn vị thuộc Tổng công ty Quản lý bay Việt Nam quy định tại điểm 1.1.1 và điểm 1.1.2. thuộc mục 1.1 của E-HSMT.

Yêu cầu về quy trình triển khai:

- Chuẩn bị triển khai:

+ Xây dựng Tài liệu giải pháp triển khai, quy trình triển khai, bảng tiến độ thi công tổng thể, chi tiết các hạng mục và được chủ đầu tư chấp thuận;

+ Xây dựng gói cài đặt hoặc thông số (nếu cần).

- Thực hiện triển khai:

+ Lắp đặt thiết bị, cài đặt cấu hình hạ tầng kỹ thuật, phần mềm thương mại, cài đặt phân chia hệ thống thiết kế.

+ Cài đặt, cấu hình thông số an toàn thông tin và các cấu hình theo thiết kế đã có để hình thành môi trường theo thiết kế.

+ Kiểm tra tích hợp với các hệ thống liên quan;

- Nghiệm thu, bàn giao.

*1.3.2.2. Yêu cầu về dịch vụ huấn luyện khai thác, quản trị hệ thống*

Nhà thầu phải cung cấp dịch vụ huấn luyện khai thác, quản trị hệ thống qua hai hình thức:

- Huấn luyện tập trung;
- Huấn luyện trực tiếp trong quá trình triển khai (on-job training).

*1.3.2.2.1. Hình thức huấn luyện tập trung*

- Địa điểm: Huấn luyện tập trung tại Công ty Quản lý bay Miền Bắc, Công ty Quản lý bay Miền Trung và Công ty Quản lý bay Miền Nam
- Số lớp và đối tượng được huấn luyện tập trung: 3 lớp, cụ thể:

+ Công ty Quản lý bay Miền Bắc, Trung tâm Thông báo tin tức hàng không, Trung tâm Khí tượng hàng không: 1 lớp

+ Công ty Quản lý bay Miền Trung: 1 lớp

+ Công ty Quản lý bay Miền Nam: 1 lớp

- Thời lượng và nội dung huấn luyện mỗi lớp: 14 buổi

+ Quản trị hệ thống (tổng quan cho dự án) (2 buổi)

+ Hệ thống thiết bị mạng (2 buổi)

+ Hệ thống thiết bị bảo mật (3 buổi)

+ Hệ thống phân tích phát hiện các mối nguy an ninh mạng (IDS/APT) (4 buổi)

+ Hệ thống quản lý giám sát vận hành (3 buổi)

- Nhân sự thực hiện: Tối thiểu 01 giảng viên và 02 trợ giảng cho mỗi lớp.

*1.3.2.2.2. Hình thức huấn luyện trực tiếp trong quá trình triển khai (on-job training)*

Cán bộ phụ trách Tổng công ty Quản lý bay Việt Nam cùng tham gia quá trình lắp đặt, cài đặt vừa để giám sát vừa để học tập, trao đổi làm rõ các thông tin thiết bị và lưu ý khi được bàn giao, quản trị vận hành sau này. Nội dung huấn luyện các tính năng liên quan tới từng hệ thống, thiết bị, cụ thể:

- Huấn luyện về hệ thống chuyển mạch (Switch);
- Huấn luyện về hệ thống tường lửa (Firewall);
- Huấn luyện về hệ thống tường lửa ứng dụng web (Web Application Firewall);
- Huấn luyện về hệ thống phân tích phát hiện các mối nguy an ninh mạng (IDS/APT);
- Huấn luyện về hệ thống quản lý giám sát vận hành (NMS).

Các tài liệu/sản phẩm bàn giao phải được chủ đầu tư hoặc đơn vị thụ hưởng phê duyệt, bao gồm:

- Tài liệu đào tạo;
- Tài liệu thiết kế;
- Tài liệu triển khai hệ thống;
- Tài liệu quản trị vận hành hệ thống;

### *1.3.3. Yêu cầu về tính sẵn sàng với Ipv6*

Nhà thầu phải đảm bảo các giải pháp lựa chọn, thiết bị sẵn sàng tương thích với Ipv6 khi có yêu cầu về nâng cấp hệ thống. Hệ thống sẵn sàng nâng cấp, tích hợp

IPv6 theo kế hoạch chuyển đổi IPv6 của Bộ TTTT và theo kế hoạch cấp phát tài nguyên.

### *1.3.4. Yêu cầu về bảo hành, bảo trì*

Nhằm đảm bảo hệ thống thiết bị khi đưa vào vận hành được hỗ trợ, bảo hành bảo trì an toàn, nhanh chóng, hiệu quả, các hạng mục thiết bị chính (thiết bị mạng, thiết bị tường lửa, thiết bị tường lửa ứng dụng WAF, thiết bị gom lưu lượng mạng, thiết bị phân tích phát hiện các mối nguy an ninh mạng IDS/APT, máy chủ, phần mềm quản lý giám sát mạng NMS), cần thiết phải được xác nhận bởi chính hãng sản xuất (đối với các hãng nước ngoài) với đầy đủ các nội dung:

- Cam kết và xác nhận có văn phòng đại diện hoặc Nhà phân phối chính thức và có Trung tâm bảo hành hoặc đơn vị ủy quyền tiếp nhận bảo hành tại Việt Nam.

- Cam kết và xác nhận về việc hàng hóa, thiết bị tại thời điểm chào thầu, không có kế hoạch End-of-Sales (EOS) hoặc End-of-Life (EOL).

- Cam kết và xác nhận về việc thiết bị chào thầu không chứa bất kỳ phần mềm độc hại nào như virus, trojan, backdoor và sẽ chịu trách nhiệm nếu phát hiện thiết bị chứa mã độc sau khi trúng thầu.

Nhà thầu phải cam kết cung cấp các dịch bảo hành, bảo trì, hỗ trợ kỹ thuật chính hãng miễn phí tối thiểu 36 tháng (1096 ngày) kể từ ngày nghiệm thu bàn giao, đưa vào sử dụng đối với hàng hóa được cung cấp.

### *1.3.5. Yêu cầu về an toàn thông tin*

Các hệ thống đã được phê duyệt hồ sơ cấp độ 3 và 4 về an toàn thông tin của Tổng công ty Quản lý bay Việt Nam phải tuân theo các tiêu chuẩn trong Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết, 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 và TCVN 11930:2017 về Thiết lập chính sách an toàn thông tin, Tổ chức đảm bảo an toàn thông tin, Đảm bảo nguồn lực, Quản lý thiết kế, xây dựng hệ thống, vận hành, Đảm bảo về mặt thiết kế hệ thống, giải pháp an toàn thông tin đảm bảo an toàn (mạng, máy chủ, ứng dụng, dữ liệu).

## Mục 2. Bản vẽ

Không có bản vẽ.

## Mục 3. Kiểm tra và thử nghiệm

Các kiểm tra và thử nghiệm cần tiến hành gồm có:

- Hệ thống trước khi đưa vào cài đặt sẽ được kiểm tra, nghiệm thu về số lượng, chủng loại, tiêu chuẩn và xuất xứ;

- Các hạng mục bổ sung sau khi cài đặt tại mỗi vị trí sẽ được kiểm tra, nghiệm thu thông điện, cấu hình, kết nối, tình trạng hoạt động của thiết bị.

- Nhà thầu phải cử nhân sự phối hợp với Bên mời thầu để thực hiện nghiệm thu và chịu các chi phí liên quan đối với phía Nhà thầu.

- Sau khi hoàn thành việc cài đặt tại các địa điểm sẽ tiến hành nghiệm thu khối lượng, chất lượng, tiến độ thực hiện Gói thầu.