CHƯƠNG V. ĐIỀU KHOẢN THAM CHIẾU

I. GIỚI THIỆU :

1.1. Giới thiệu về dự án:

Tên công trình: Giải pháp An toàn, an ninh thông tin cho hệ thống giám sát, điều khiển và tự động hoá tại EVNHANOI.

Địa điểm xây dựng:

- 01 Trung tâm điều khiển
- 01 Hệ thống Điều khiển lưới điện trung thế (cài đặt triển khai trên hệ thống SCADA đã nâng cấp)
- 64 Trạm biến áp không người trực và 12 Công ty Điện lực. (Theo khảo sát thực tế tại thời điểm lập thiết kế thi công dự toán có 64 trạm (chưa tính dự phòng). Khối lượng hồ sơ thiết vẫn đáp ứng khối lượng với thiết kế cơ sở (bao gồm thực tế và dự phòng) đã được duyệt tại quyết định số 6081/QĐ-EVNHANOI ban hành ngày 07/09/2023. Tại thời điểm khảo sát là có 30 Công ty Điện lực, tuy nhiên theo công văn số 3687/EVN-TCNS ban hành ngày 10 tháng 06 năm 2025 về việc triển khai sắp xếp tinh gọn tổ chức, bộ máy quản lý, điều hành của EVNHANOI thì số lượng Công ty điện lực cập nhật là 12 công ty)
- 01 Công ty Lưới điện Cao thế.
- 08 Tổ thao tác lưu động.

Cụ thể như sau:

STT	Đơn vị	Địa điểm
1	Trung tâm điều khiển	Số 69 Đinh Tiên Hoàng, Phường Hoàn Kiếm, Thành phố Hà Nội, Việt Nam
2	Hệ thống Điều khiển lưới điện trung thế	Số 69 Đinh Tiên Hoàng, Phường Hoàn Kiếm, Thành phố Hà Nội, Việt Nam
3	Trạm biến áp không người trực và Công ty Điện lực	
3.1	Trạm biến áp không người trực	E1.1 Đông Anh
		E1.16 Nội Bài
		E1.41 Mai lâm
		E1.42 Sân bay Nội Bài
		E1.49 Đông Anh 2
		E1.17 Bắc Thăng Long
		E1.24 Hải Bối
		E1.36 Quang Minh
		E1.8 Yên Phụ
		E1.9 Nghĩa Đô
		E1.14 Giám
		E1.21 Nhật Tân
		E1.40 Tây Hồ
		E1.63 Bắc Thành Công
		E1.7 Sơn Tây
		E1.28 Phùng Xá
		E1.44 Sơn Tây 2
		E1.48 Quốc Oai
		E10.6 Phúc Thọ

STT	Đơn vị	Địa điểm
		E1.53 Ba Vì
		E1.54 Hòa Lạc
		E1.20- Thanh Xuân
		E1.25- Mỹ Đình
		E1.31 Trôi
		E1.33 Cầu Diễn
		E1.37 Bắc An Khánh
		E1.46 Từ Liêm
		E1.56 Thị Trấn Phùng
		E1.12 Trần Hưng Đạo
		E1.13 Phương Liệt
		E1.18 Bờ Hồ
		E1.22 Thanh Nhàn
		E1.26 Linh Đàm
		E1.52 Thống Nhất
		E1.57 Minh Khai
		E1.64 Hồ Yên Sở
		E1.32 Thường Tín
		E1.39 Thanh Oai
		E10.2 Vân Đình
		E10.4 Tía
		E1.58 Phú Xuyên
		E1.62 Ngọc Hồi
		E1.66 Mỹ Đức
		E1.2 Gia Lâm
		E1.15 Sài Đồng
		E1.38 Gia Lâm 2
		E1.47 Long Biên
		E1.59 Sài Đồng 2
		E1.5 Thượng Đình
		E1.10 Văn Điển
		E1.30 Văn Quán
		E1.43 Mỗ Lao
		E10.9 Xuân Mai
		E1.51 Phú Nghĩa
		E1.61 Dương Nội
		E1.67 CV Thủ Lệ
		E1.69 Trâu Quỳ
		E1.71 Hồng Dương
		E1.73 CNC 2
		E1.74 Thạch Thất 2
3.2	Công ty điện lực	C01 Hoàn Kiếm
		C02 Hai Bà Trưng
		C03 Ba Đình
		C04 Đống Đa
		C05 Nam Từ Liêm

STT	Đơn vị	Địa điểm
		C06 Thanh Trì
		C07 Gia Lâm
		C08 Đông Anh
		C09 Sóc Sơn
		C10 Tây Hồ
		C11 Thanh Xuân
		C12 Cầu Giấy
		C13 Hoàng Mai
		C14 Long Biên
		C15 Mê Linh
		C16 Hà Đông
		C17 Sơn Tây
		C18 Chương Mỹ
		C19 Thạch Thất
		C20 Thường Tín
		C21 Ba Vì
		C22 Đan Phượng
		C23 Hoài Đức
		C24 Mỹ Đức
		C25 Phú Xuyên
		C26 Phúc Thọ
		C27 Quốc Oai
		C28 Thanh Oai
		C29 Ứng Hòa
		C30 Bắc Từ Liêm
4	Công ty Lưới điện Cao thế.	Công ty lưới điện cao thế X6 Phường Yên Hòa, quận Cầu Giấy, TP Hà Nội
5	Tổ thao tác lưu động	Tổ TTLĐ số 1
		Tổ TTLĐ số 2
		Tổ TTLĐ số 3
		Tổ TTLĐ số 4
		Tổ TTLĐ số 5
		Tổ TTLĐ số 6
		Tổ TTLĐ số 7
		Tổ TTLĐ số 8

- Căn cứ Quyết định số 8964/QĐ-EVNHANOI ngày 12/09/2025 của Tổng công ty Điện lực TP Hà Nội về việc phê duyệt thiết kế thi công và dự toán xây dựng công trình;

1.2. Quy mô dự án:

- Trang bị phần cứng (Firewall OT 2 chiều, 1 chiều, thiết bị mạng, máy tính chủ, máy tính trạm, ...) tại Trung tâm Điều khiển, các Trạm biến áp 110kV/220kV và Công ty điện lực. Trong đó các thiết bị firewall tích hợp chức năng IPS để hỗ trợ ngăn chặn các cuộc tấn công mạng.
- Giải pháp quản lý firewall tập trung tại Trung tâm Điều khiển.
- Cổng một chiều tại Trung tâm Điều khiển (chia sẻ dữ liệu một cách an toàn sang

mạng IT).

- Giải pháp xác thực đa lớp (MFA) để tăng cường bảo mật tài khoản người sử dụng.
- Giải pháp SIEM (quản lý Logger) thu thập, lưu trữ, phân tích nhật ký hệ thống, mạng để đưa ra cảnh báo về mối đe dọa an ninh mạng; đồng thời chia sẻ dữ liệu với hệ thống SOC của EVNHANOI và EVN.
- Hệ thống phần mềm bảo vệ điểm cuối (EPS) giúp chống mã độc tại các máy chủ, máy trạm.
- Giải pháp quản lý đặc quyền (PIM/PAM) để quản lý chặt chẽ người dùng, tài khoản có quyền cao trong hệ thống.
- Hệ thống sao lưu và phục hồi dữ liệu tự động (Backup and restore).
- Xây dựng các quy trình, quy định, tài liệu hướng dẫn quản lý vận hành, kiểm tra, bảo trì,... các kịch bản ứng cứu mất an ninh thông tin.
- Xây dựng kịch bản ứng phó với một số sự cố có thể xảy ra và việc ứng dụng các giải pháp công nghệ được trang bị trong dự án để ngăn chặn, giảm thiểu rủi ro.
- Đào tạo và chuyển giao công nghệ về hệ thống ATTT được trang bị nhằm nâng cao nhận thức về ATTT ở 3 cấp độ (nhận thức, hiểu biết và thực thi).

II. THUYẾT MINH THIẾT KẾ

1.1 Căn cứ pháp lý

- Căn cứ theo Nghị định 85/2016/NĐ-CP, ngày 01/07/2016 Về đảm bảo an toàn hệ thống thông tin theo cấp độ;
- Chỉ thị số 09/CT-TTg về tuân thủ quy định pháp luật và tang cường bảo đảm an toàn hệ thống thông tin theo cấp độ
- Căn cứ theo Thông tư số 12/2022/TT-BTTTT, ngày 12/08/2022 về quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP của Chính phủ về đảm bảo an toàn Hệ thống thông tin theo cấp độ. Cụ thể Phụ lục III Yêu cầu cơ bản đảm bảo an toàn hệ thống thông tin đối với Hệ thống thông tin cấp độ 3;
- Quyết định số 168/QĐ-EVN ngày 23/02/2023 của Tập đoàn Điện lực Việt Nam về việc phê duyệt Đề án "Đảm bảo an toàn thông tin cho hệ thống thông tin của Tập đoàn Điện lực quốc gia Việt Nam giai đoạn 2023 – 2028"
- Căn cứ quyết định 6679/QĐ-EVNHANOI ngày 29/12/2017 về việc thành lập Trung tâm Điều khiển thuộc Trung tâm Điều độ Hệ thống TP Hà Nội;
- Căn cứ quyết định 4951/QĐ-EVNHANOI, ngày 02/07/2019 về việc chuyển đổi hệ thống Điều khiển trung tâm sang kết nối mạng WAN-HTĐ để sử dụng giao thức IEC 60870-5-104;
- Căn cứ văn bản số 2465/BTL-AT, ngày 14/08/2019 của Bộ Tư lệnh 86 - Bộ Quốc Phòng về việc thông báo kết quả kiểm tra an toàn thông tin tại EVNHANOI;
- Căn cứ quyết định 10634/QĐ-EVNHANOI, ngày 16/12/2019 về việc ban hành quy trình An toàn an ninh thông tin, sao lưu và khôi phục dữ liệu trong Tổng công ty Điện lực TP Hà Nội;
- Căn cứ 2184/Tr-B11, ngày 24/04/2020 về việc chủ trương thực hiện công tác triển khai các giải pháp an toàn, an ninh thông tin đối với hệ thống giám sát, điều khiển và tự động hóa tại EVNHANOI;
- Căn cứ văn bản 1785/EVN VT-CNTT, ngày 26/03/2020 về việc tăng cường triển khai các giải pháp đảm bảo an toàn thông tin trong Tập đoàn Điện lực Việt Nam;
- Căn cứ quyết định số 5866/QĐ-EVNHANOI ngày 20/7/2020 về việc ban hành đề án “Bổ sung các trạm biến áp vào Trung tâm Điều khiển giai đoạn 2020 - 2021”;
- Căn cứ văn bản số 1856/NVĐT-EVNHANOILDC ngày 12/11/2020 về Nhiệm vụ đầu tư cho công trình “Giải pháp An toàn, an ninh thông tin cho hệ thống giám sát, điều khiển và tự động hóa tại EVNHANOI”;
- Căn cứ vào Quyết định số 6081/QĐ-EVNHANOI ngày 07/09/2023 về việc Phê duyệt báo cáo nghiên cứu khả thi đầu tư xây dựng Công trình: Giải pháp an toàn, an ninh thông tin cho hệ thống giám sát, điều khiển và tự động hóa tại EVNHANOI;
- Căn cứ hợp đồng số 43/2023/HĐ-EVNHANOIPMB ngày 17/11/2023 giữa Ban Quản lý dự án lưới điện Hà Nội và Công ty Cổ phần Giải pháp Công nghệ cao Việt Sifo về việc thực hiện Gói thầu 2: Tư vấn lập hồ sơ thiết kế thi công – dự

toán, lập hồ sơ mời thầu Công trình: Giải pháp an toàn, an ninh thông tin cho hệ thống giám sát, điều khiển và tự động hóa tại EVNHANOI;

- Căn cứ vào Báo cáo kết quả khảo sát;
- Căn cứ vào Quyết định số 717/QĐ-EVN ngày 31/05/2025 về việc ban hành Quy định Đảm bảo An ninh mạng và An toàn thông tin trong Tập đoàn Điện lực Việt Nam;
- Căn cứ văn bản số 4032/EVN-KHCNCĐS ngày 23/6/2025 về việc bảo đảm ANM&ATTT trong quá trình thực hiện ĐTXD các dự án.

1.2 Yêu cầu thiết kế

1.2.1 Nguyên tắc thiết kế

Các nội dung thiết kế các hạng mục trong phần thiết kế thi công của dự án ngoài việc phải tuân thủ các yêu cầu về tính năng, chức năng kỹ thuật như đã yêu cầu trong thiết kế sơ bộ được duyệt còn phải đảm bảo tuân thủ theo các nội dung như sau:

- Tuân thủ theo các tiêu chí cấp độ 3 theo Nghị định 85/2016/NĐ-CP và Thông tư 12/2022/TT-BTTTT.

  Cấp độ 3: Hệ thống thông tin phục vụ một trong những tiêu chí sau:

  - Thông tin bí mật nhà nước hoặc quốc phòng, an ninh quốc gia;
  - Thông tin và dịch vụ công trực tuyến từ mức độ 3 trở xuống, có xử lý thông tin cá nhân từ 10.000 người dùng trở lên;
  - Cơ sở hạ tầng thông tin dùng chung của các cơ quan, tổ chức trong phạm vi một ngành/tỉnh.
  - Hệ thống thông tin điều khiển, vận hành hoạt động bình thường của các công trình xây dựng cấp II/III/IV theo phân cấp của pháp luật về xây dựng.
- Tuân thủ theo Đề án "Đảm bảo ATTT cho hệ thống thông tin của Tập đoàn Điện lực Quốc gia Việt Nam giai đoạn 2023 – 2028" ban hành tại Quyết định số 168/QĐ-EVN ngày 23/02/2023;
- Phù hợp với kết quả khảo sát, đặc trưng của từng đơn vị.
- Phù hợp với Nhiệm vụ thiết kế.
- Đáp ứng mục tiêu của Dự án.
- Phù hợp với phạm vi của Dự án.
- Đảm bảo đủ điều kiện để triển khai thi công đáp ứng mục tiêu kế hoạch tiến độ.
- Đảm bảo kết nối, tích hợp và đồng bộ giữa các hạng mục trong hệ thống tổng thể.
- Đáp ứng yêu cầu kế thừa, tối ưu hóa các nguồn tài nguyên, yêu cầu nâng cấp và nhu cầu mở rộng trong tương lai.
- Phải tuân thủ các quy chuẩn, tiêu chuẩn được áp dụng đối với các hạng mục của dự án.
- Phải thể hiện được các thông số chủ yếu của hệ thống hạ tầng kỹ thuật và các hạng mục đầu tư của dự án;
- Phải đảm bảo xác định được tổng dự toán.

1.2.2 Các chỉ tiêu kỹ thuật áp dụng

1.2.2.1 Tiêu chuẩn về công nghệ thông tin

- Giao diện kết nối mạng - Yêu cầu kỹ thuật TCN 68-172:1998
- Chuẩn kết nối truyền thông hệ thống theo mô hình tham chiếu OSI;
- Tiêu chuẩn mạng máy tính cục bộ Ethernet LAN;
- Tiêu chuẩn mạng máy tính diện rộng IP WAN;
- Tiêu chuẩn giao diện truyền thông mạng máy tính TCP/IP;
- Tiêu chuẩn công nghệ mạng lưu trữ trong máy tính SAN, NAS;
- Tiêu chuẩn hệ điều hành máy tính đa nhiệm/ Multi-task, đa người dùng/ multi-user;

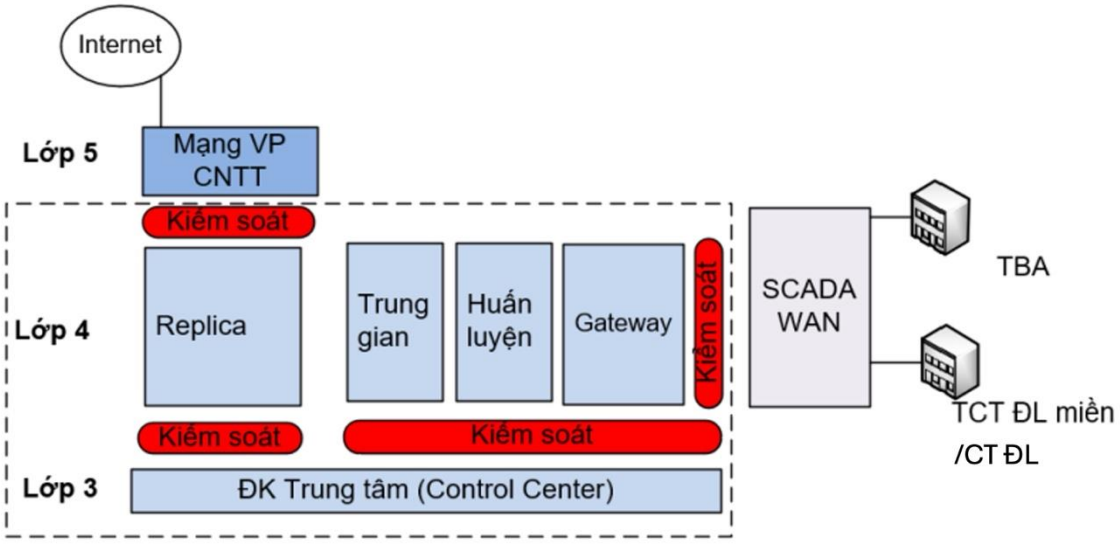
1.2.2.2 Tiêu chuẩn về an toàn thông tin

- An toàn giao vận SSL v3.0;
- An toàn truyền tệp tin (HTTPS): sử dụng cho việc thiết lập SSL Certificate.
- An toàn giải thuật mã hóa (RSA, SHA-2): sử dụng giải thuật mã hóa công khai để thiết lập các giao dịch an toàn;
- An toàn trao đổi bản tin XML (XML Signature Syntax and Processing): sử dụng cho việc đồng bộ dữ liệu;
- Tiêu chuẩn Oauth 2.0 (OAuth2 là một chuẩn mở để ủy quyền/phân quyền (authorization), OAuth2 cũng là nền tảng của OpenID Connect, nó cung cấp OpenID (xác thực - authentication) ở phía trên của OAuth2 (ủy quyền - authorization) để có một giải pháp bảo mật hoàn chỉnh hơn;
- Tiêu chuẩn 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";
- TCVN ISO/IEC 27001:2009 Công nghệ thông tin - Hệ thống quản lý an toàn thông tin – Các yêu cầu;
- TCVN ISO/IEC 27002:2011 Công nghệ thông tin-Các kỹ thuật an toàn- Quy tắc thực hành Quản lý an toàn thông tin;
- 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;
- TCVN 8709-2:2011 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;
- TCVN 8709-3:2011 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;
- TCVN 10295:2014 ISO/IEC 27005:2011 Công nghệ thông tin-Các kỹ thuật an toàn-Quản lý rủi ro an toàn thông tin;
- TCVN 10541:2014 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;

- TCVN 10543:2014 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;
- TCVN 11239:2015 Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý sự cố an toàn thông tin;
- TCVN 11386:2016 Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp đánh giá an toàn công nghệ thông tin;

1.3 Thiết kế tổng quan

Quyết định số 168/QĐ-EVN ngày 23/02/2023 của Tập đoàn Điện lực Việt Nam về việc phê duyệt Đề án "Đảm bảo an toàn thông tin cho hệ thống thông tin của Tập đoàn Điện lực quốc gia Việt Nam giai đoạn 2023 – 2028", tại mục III.4.2.d có đề cập đến phương pháp thiết kế ATTT cho trung tâm điều khiển xa cụm nhà máy trực thuộc TCTĐL/CTĐL như sau:



TKTC-BV 1 Thiết kế ATTT cho TTĐK xa cụm nhà máy trực thuộc TCTĐL/CTĐL

Tham khảo: Quyết định số 168/QĐ-EVN ngày 23/02/2023 của Tập đoàn Điện lực Việt Nam, mục III.4.2.d. Trung tâm điều khiển xa cụm nhà máy trực thuộc TCTĐL/CTĐL, trang 94, Hình 21. Phương pháp thiết kế hệ thống TTĐKX thuộc TCTĐL/CTĐL

Kiến trúc thiết kế theo nguyên tắc phân tầng và phòng thủ theo chiều sâu (Defense in Depth) tham khảo các hướng dẫn IEC 62443, DHS ICS-CERT như hình trên.

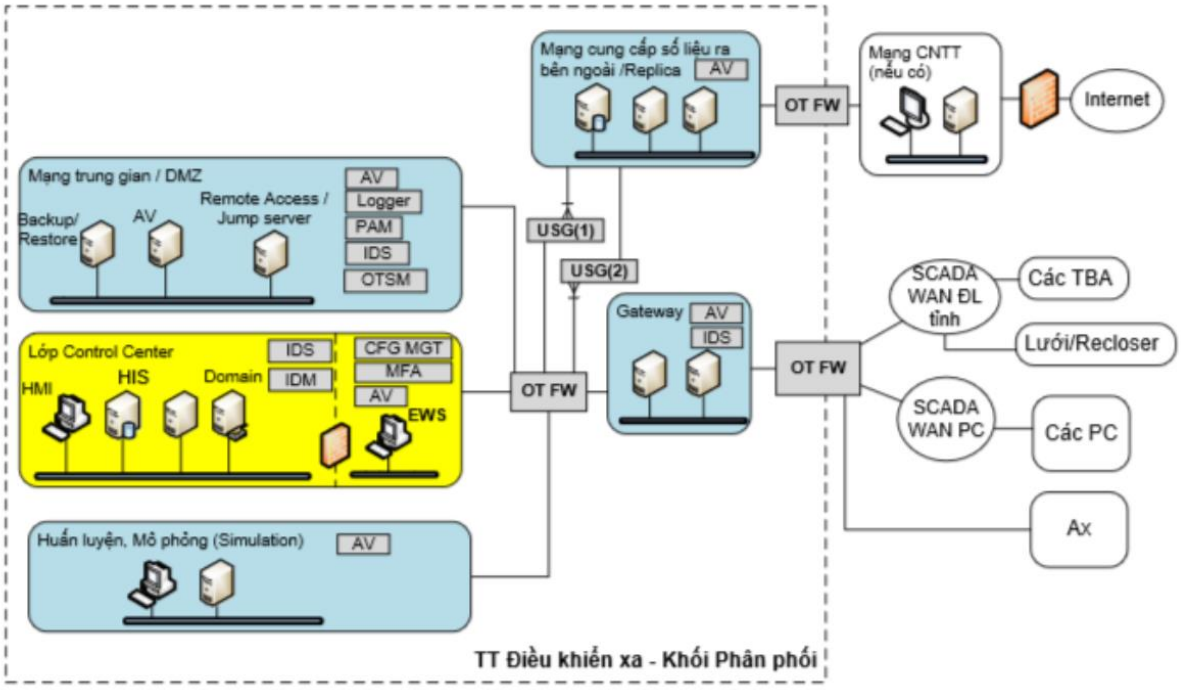
Ở trên là mô hình kiến trúc đảm bảo an toàn, an ninh thông tin cho hệ thống mini SCADA của Tổng công ty Điện lực TP Hà Nội và TP Hồ Chí Minh.

Các phân vùng mạng trong hệ thống mini SCADA bao gồm:

- Lớp 3:
  - Khối điều khiển trung tâm bao gồm các máy chủ (HMI/Application/HIS Servers), các máy chủ giao diện người dùng (HMI Server), máy chủ ứng dụng (Application Server), máy chủ lưu trữ dữ liệu quá khứ (Historian Server).
- Lớp 4:

- Khối huấn luyện: Bao gồm các máy tính phục vụ mô phỏng đào tạo điều độ viên thực hành điều khiển (DTS – Dispatcher Training Simulator).
- Khối trung gian gồm: máy kỹ sư (EWS – Engineering Workstation) cấu hình hệ thống, các máy tính của kỹ sư vận hành.
- Vùng đệm cung cấp số liệu ra bên ngoài (Replica): Dữ liệu được đồng bộ ra máy chủ tại phân vùng đệm phục vụ cho việc truy xuất dữ liệu từ bên ngoài. Khối thu thập dữ liệu SCADA (DAN – Data Acquisition Node): Vùng đệm lưu trữ dữ liệu SCADA từ các trạm biến áp, nhà máy điện gửi về.
- Khối GW(Gateway): Cổng giao tiếp với các Trung tâm Điều độ.

Các giải pháp định hướng đảm bảo an toàn, an ninh thông tin cho hệ thống mini SCADA được bố trí như sau:



TKTC-BV 2 Sơ đồ giải pháp thiết kế định hướng ATTT cho hệ thống mini SCADA của TCT ĐL TP Hà Nội và TP Hồ Chí Minh kèm theo Quyết định số 168/QĐ-EVN

Tham khảo: Quyết định số 168/QĐ-EVN ngày 23/02/2023 của Tập đoàn Điện lực Việt Nam, mục III.4.2.d. Trung tâm điều khiển xa cụm nhà máy trực thuộc TCTĐL/CTĐL, trang 95, Hình 22. Thiết kế hệ thống TTĐKX thuộc TCTĐL/CTĐL

Trong đó các giải pháp chi tiết như sau:

Yêu cầu chung	Vùng mạng	Giải pháp kỹ thuật yêu cầu	Mức độ đáp ứng QĐ 168/QĐ-EVN trước khi triển khai dự án	Giải pháp tại EVNHANOI	Mức độ đáp ứng QĐ 168/QĐ-EVN sau khi triển khai dự án
OT.01	Kiểm soát an ninh vật lý cho toàn bộ hệ thống DCS	Triển khai các biện pháp an ninh vật lý quản lý việc truy cập hệ thống DCS	Đáp ứng	Tận dụng thiết bị kiểm soát an ninh vật lý đã có	Đáp ứng
OT.10	Lớp 3: Control Center	Tường lửa công nghiệp/Bảo mật hai chiều	Chưa đáp ứng	Triển khai bổ sung một cặp tường lửa bảo mật hai chiều OT FW đặt tại TTĐK. Cặp tường lửa hiện tại sẽ bàn giao lại cho X6 sử dụng.	Đáp ứng
OT.05		Giải pháp giám sát an ninh, phát hiện tấn công xâm nhập, hành vi bất thường trong hệ thống	Chưa đáp ứng	- Sử dụng OT FW dạng NGFW có sẵn tính năng IDS - phát hiện tấn công xâm nhập lớp mạng. - Triển khai mới giải pháp Antivirus có tính năng IDS ở mức server (host-based IDS)	Đáp ứng
OT.02		Phòng, chống mã độc/virus	Đáp ứng một phần	Triển khai mới giải pháp Antivirus phòng chống mã độc	Đáp ứng
OT.03		Giám sát thay đổi/đóng băng cấu hình	Chưa đáp ứng	- Giám sát việc thay đổi cấu hình các máy chủ, máy trạm, thiết bị mạng thông qua triển khai mới giải pháp	Đáp ứng

Yêu cầu chung	Vùng mạng	Giải pháp kỹ thuật yêu cầu	Mức độ đáp ứng QĐ 168/QĐ-EVN trước khi triển khai dự án	Giải pháp tại EVNHANOI	Mức độ đáp ứng QĐ 168/QĐ-EVN sau khi triển khai dự án
				SIEM và viết các tập luật phát hiện. Bất cứ hành động thay đổi cấu hình hệ thống đều được cảnh bảo cho người quản trị. - Triển khai mới giải pháp PAM giám sát phiên làm việc của tài khoản quản trị, cấu hình tự động ngắt phiên làm việc nếu người quản trị có sử dụng các câu lệnh bất thường như thay đổi cấu hình quan trọng của hệ thống. - Triển khai mới giải pháp Backup cho phép sao lưu cấu hình cho các máy chủ, máy trạm, đảm bảo khôi phục nguyên trạng khi có nhu cầu.	
OT.09		Xác thực mạnh	Chưa đáp ứng	Triển khai mới giải pháp xác thực đa yếu tố MFA	Đáp ứng
OT.04		Quản lý định danh	Đáp ứng	Tận dụng giải pháp Active Directory đã triển khai	Đáp ứng
OT.10	Lớp 4.1: SCADA/GW	Tường lửa công nghiệp/Bảo mật hai chiều	Chưa đáp ứng	Triển khai bổ sung một cặp tường lửa bảo mật hai chiều OT FW đặt	Đáp ứng

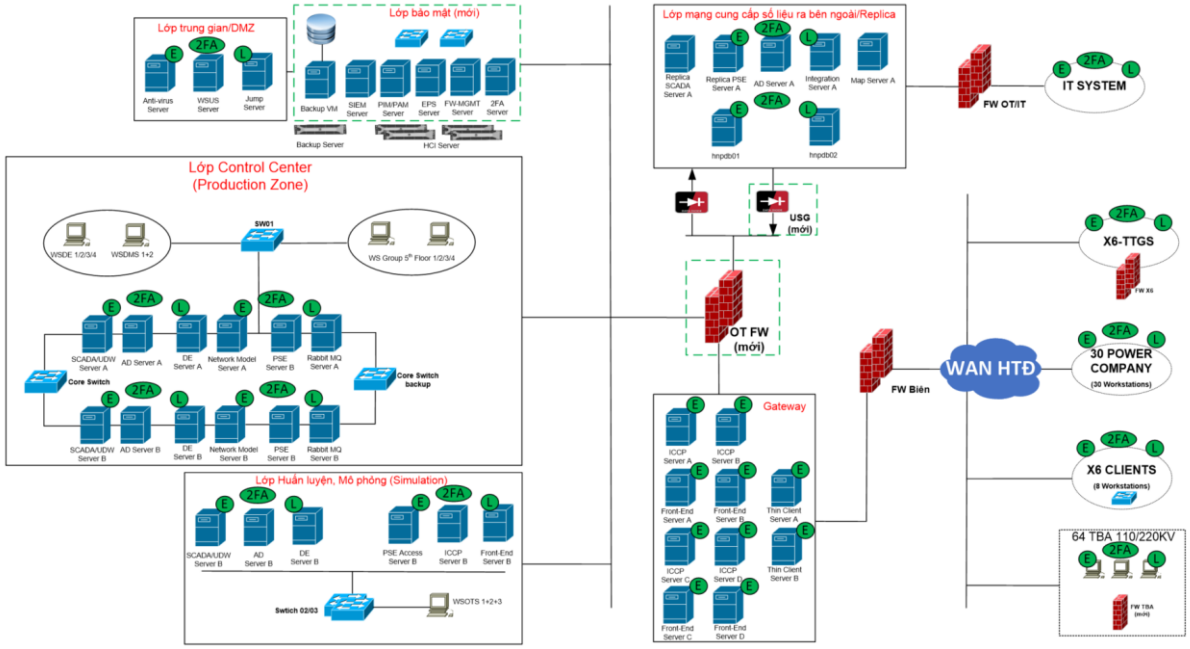
Yêu cầu chung	Vùng mạng	Giải pháp kỹ thuật yêu cầu	Mức độ đáp ứng QĐ 168/QĐ-EVN trước khi triển khai dự án	Giải pháp tại EVNHANOI	Mức độ đáp ứng QĐ 168/QĐ-EVN sau khi triển khai dự án
				giữa lớp SCADA/GW và lớp biên kết nối đến các đơn vị thành viên. Cặp tường lửa hiện tại sẽ bàn giao lại cho đơn vị QLVH sử dụng.	
OT.05		Giải pháp giám sát an ninh, phát hiện tấn công xâm nhập, hành vi bất thường trong hệ thống	Chưa đáp ứng	- Sử dụng OT FW dạng NGFW có sẵn tính năng IDS - phát hiện tấn công xâm nhập lớp mạng. - Triển khai mới giải pháp Antivirus có tính năng IDS ở mức server (host-based IDS)	Đáp ứng
OT.02		Phòng, chống mã độc/virus	Đáp ứng một phần	Triển khai mới giải pháp Antivirus phòng chống mã độc	Đáp ứng
OT.10	Lớp 4.2: Mạng Trung gian	Tường lửa công nghiệp/Bảo mật hai chiều	Chưa đáp ứng	Triển khai bổ sung một cặp tường lửa bảo mật hai chiều đặt tại TTĐK (Sử dụng chung cặp thiết bị này với lớp Control Center)	Đáp ứng

Yêu cầu chung	Vùng mạng	Giải pháp kỹ thuật yêu cầu	Mức độ đáp ứng QĐ 168/QĐ-EVN trước khi triển khai dự án	Giải pháp tại EVNHANOI	Mức độ đáp ứng QĐ 168/QĐ-EVN sau khi triển khai dự án
OT.05		Giải pháp giám sát an ninh, phát hiện tấn công xâm nhập, hành vi bất thường trong hệ thống	Chưa đáp ứng	- Triển khai mới OT FW dạng NGFW có sẵn tính năng IDS - phát hiện tấn công xâm nhập lớp mạng. - Triển khai mới giải pháp Antivirus có tính năng IDS ở mức server (host-based IDS)	Đáp ứng
OT.02		Phòng, chống mã độc/virus	Chưa đáp ứng	Triển khai mới giải pháp Antivirus phòng chống mã độc.	Đáp ứng
OT.13		Cổng quét an ninh	Chưa đáp ứng	Triển khai giải pháp Antivirus quét mã độc trên file trước khi copy vào hệ thống. Cấu hình phần mềm Antivirus ngăn chặn kết nối thiết bị ngoại vi như USB trái phép.	Đáp ứng
OT.12		Giải pháp giám sát người dùng đặc quyền	Chưa đáp ứng	Triển khai mới giải pháp PAM	Đáp ứng
OT.11		Quản lý tài sản hệ thống OT	Chưa đáp ứng	Triển khai quy trình quản lý thiết bị, tài sản trong hệ thống	Đáp ứng trong quá trình triển khai và áp dụng

Yêu cầu chung	Vùng mạng	Giải pháp kỹ thuật yêu cầu	Mức độ đáp ứng QĐ 168/QĐ-EVN trước khi triển khai dự án	Giải pháp tại EVNHANOI	Mức độ đáp ứng QĐ 168/QĐ-EVN sau khi triển khai dự án
					quy trình quản lý tài sản.
OT.08		Thu thập và sự kiện an ninh quản lý nhật ký	Chưa đáp ứng	Triển khai giải pháp thu thập và quản lý sự kiện an ninh SIEM	Đáp ứng
OT.10	Lớp 4.3: Replica (mạng cấp số liệu ra bên ngoài)	Tường lửa công nghiệp/Bảo mật hai chiều	Chưa đáp ứng	Triển khai bổ sung một cặp tường lửa bảo mật hai chiều OT FW đặt giữa lớp Replica và lớp biên kết nối đến mạng IT	Đáp ứng
OT.14		Cổng an ninh một chiều (1)	Chưa đáp ứng	Triển khai cổng an ninh một chiều USG/ Datadiode (1)	Đáp ứng
		Cổng an ninh một chiều (2)	Đáp ứng một phần	Tận dụng thiết bị cổng an ninh một chiều USG/Datadiode có sẵn (2)	Đáp ứng
OT.02		Phòng, chống mã độc/virus	Đáp ứng	Triển khai giải pháp Antivirus phòng chống mã độc.	Đáp ứng
OT.10	Lớp 4.4: Vùng Huấn luyện, Mô phỏng (Simulation)	Tường lửa công nghiệp/ Bảo mật hai chiều	Đáp ứng	Triển khai bổ sung một cặp tường lửa bảo mật hai chiều đặt tại TTĐK (Sử dụng chung cặp thiết bị này với lớp Control Center và lớp mạng trung gian)	Đáp ứng

Yêu cầu chung	Vùng mạng	Giải pháp kỹ thuật yêu cầu	Mức độ đáp ứng QĐ 168/QĐ-EVN trước khi triển khai dự án	Giải pháp tại EVNHANOI	Mức độ đáp ứng QĐ 168/QĐ-EVN sau khi triển khai dự án
OT.02		Phòng, chống mã độc/virus	Đáp ứng một phần	Triển khai giải pháp Antivirus phòng chống mã độc.	Đáp ứng
Tư vấn đề xuất thêm (1) – dựa trên quy mô hiện trạng của EVNHANOI về việc quản trị Firewall và các chính sách bảo mật trên Firewall				Để tối ưu trong việc quản trị chính sách, luật trên Firewall đồng thời tăng tính an toàn, tránh việc chỉnh sửa cấu hình Firewall trái phép thì chúng tôi đề xuất giải pháp quản lý tường lửa tập trung	
Tư vấn đề xuất thêm (2) – dựa trên quy mô hiện trạng của EVNHANOI về việc sao lưu, khôi phục cấu hình, dữ liệu các hệ thống				Trang bị giải pháp sao lưu dữ liệu cho toàn bộ dữ liệu quan trọng trong đó bao gồm thông tin cấu hình của các máy chủ, máy trạm. Đảm bảo khả năng khôi phục cấu hình khi có sự cố	
Tư vấn đề xuất thêm (3) - dựa trên nhu cầu phần cứng triển khai các giải pháp bảo mật				Trang bị hạ tầng phần cứng và lưu trữ đảm bảo tài nguyên cho các giải pháp bảo mật ở trên.	

Mô hình thiết kế tổng quan cho hệ thống OT tại EVNHANOI như sau:



TKTC-BV 3 Mô hình thiết kế tổng quan cho hệ thống OT tại EVNHANOI

Tại TTĐK:

- 02 thiết bị tường lửa (OT Firewall) trung tâm mới sẽ đóng vai trò là trung tâm kiểm soát kết nối và thiết lập chính sách giữa các phân vùng nội bộ trại TTĐK. 02 thiết bị tường lửa này sẽ được chạy với chế độ High Availability Active/Passive để đảm bảo khả năng dự phòng. Cặp thiết bị tường lửa mới này sẽ đảm nhận nhiệm vụ kiểm soát và ứng dụng các tính năng bảo mật nâng cao để bảo vệ truy cập thông qua WAN giữa TTĐK và các TBA 110/220KV, 12 Công ty Điện lực, hệ thống số hóa, người dùng tại các đơn vị.

- 01 thiết bị cổng một chiều (USG/ Datadiode) sẽ được triển khai thay thế thiết bị cũ để nhằm kiểm soát truy cập giữa mạng IT (hệ thống OMS, hệ thống GIS...) và mạng OT/SCADA.

- Hạ tầng máy chủ mới bao gồm 04 máy chủ HCI và 02 thiết bị chuyển mạch mới sẽ được triển khai để phục vụ cài đặt và đấu nối cho các máy chủ ảo hóa của các giải pháp SIEM, PIM/PAM, Firewall Management, 2FA, EPS…

- Ngoài ra, các phần mềm và bản quyền như Backup sẽ được triển khai giúp đảm bảo an toàn giúp có thể khôi phục khi có sự cố mất mát hoặc mã hóa dữ liệu.

- Giải pháp quản lý thông tin và sự kiện an ninh mạng (SIEM) cho phép thu thập, lưu trữ, xử lý nhật ký hoạt động (log) phát sinh trên các máy chủ, máy trạm, cơ sở dữ liệu, thiết bị mạng…, tại Trung tâm Điều khiển cũng như các trạm biến áp không người trực, công ty điện lực; từ đó phát hiện các sự kiện, hành vi bất thường dựa trên những luật tương quan, đối sánh (correnlation rule), đưa ra cảnh báo để giúp đơn vị phát hiện, khắc phục sớm sự cố, giảm thiểu rủi ro, và/hoặc điều tra sự cố đã xảy ra.

- Giải pháp xác thực 02 nhân tố 2FA sẽ giúp đảm bảo an toàn cho người dùng, người quản trị vận hành có thể được xác thực mạnh trước khi đăng nhập vào hệ thống.

- Giải pháp bảo vệ cho thiết bị đầu cuối EPS có các tính năng phân tích hành vi đưa ra các biện pháp ngăn chặn các cuộc tấn công lây nhiễm mã độc.

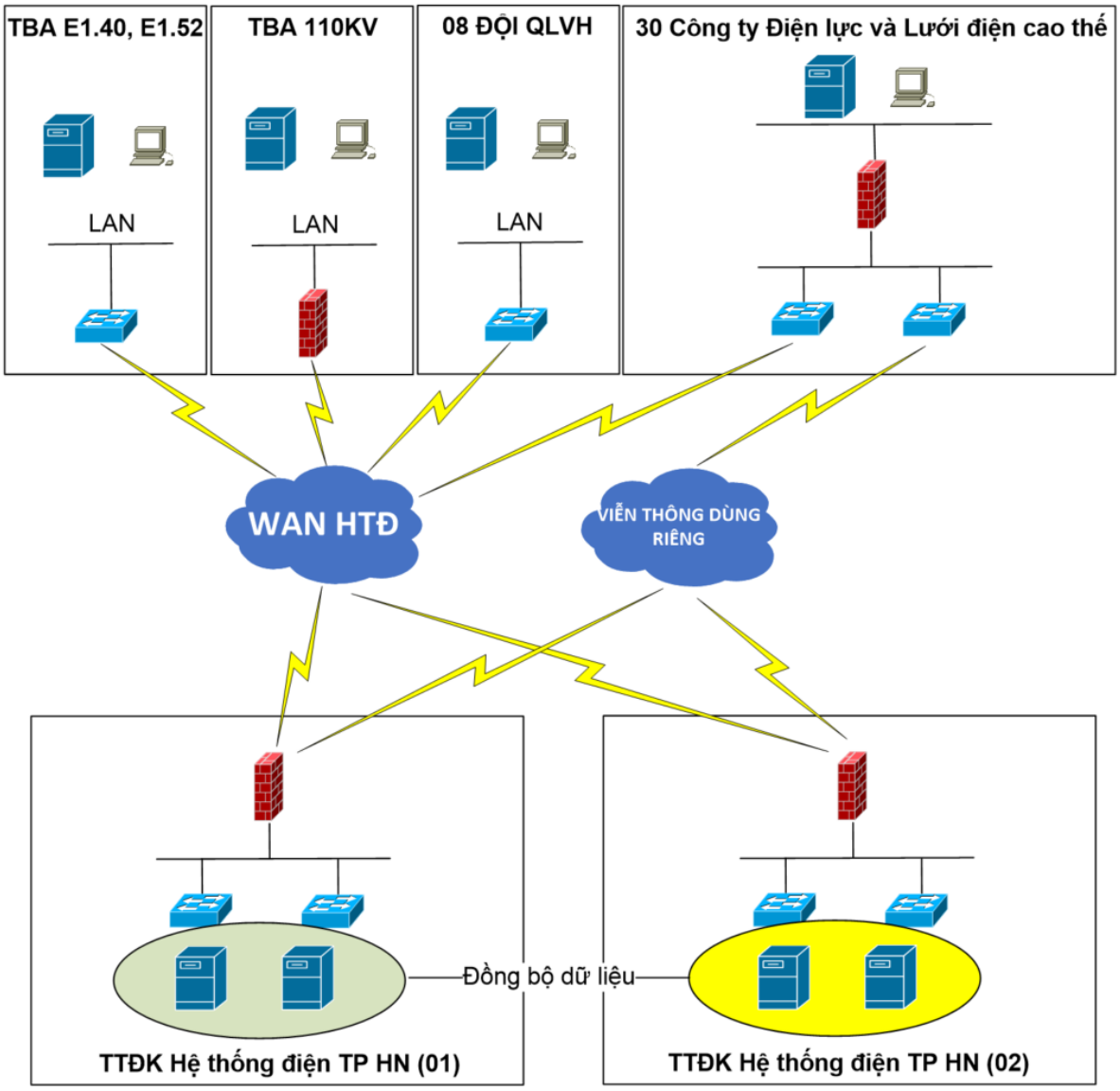
- Giải pháp Quản lý tài khoản đặc quyền PIM/PAM giúp quản lý, giám sát đồng nhất và lưu giữ một cách an toàn cho các tài khoản quản trị có quyền cao nhất trong hệ thống. Phân tách và quản lý theo vai trò của các cán bộ quản trị hệ thống.

- Tại các Trạm biến áp 110/220KV sẽ triển khai tại mỗi trạm một thiết bị tường lửa để bảo vệ luồng dữ liệu vào ra. Các thiết bị này sẽ được quản trị tập trung tại máy chủ quản trị được đặt tại TTĐK thông qua kết nối WAN-HTĐ.

Để hỗ trợ vận hành hiệu quả các giải pháp nêu trên, tại trung tâm cần triển khai một số giải pháp sau:

- Giải pháp quản lý tường lửa (Firewall management) cho phép quản lý tập trung cấu hình/firmware/hoạt động của toàn bộ tường lửa tại trung tâm cũng như các trạm biến áp, và/hoặc cho phép quản lý, tối ưu, triển khai tập luật (rule), chính sách (policy) của các tường lửa đó một cách nhất quán, nhanh chóng, hiệu quả.

Ngoài ra, trong tương lai nếu xây dựng thêm một Trung tâm Điều khiển mới để hoạt động liên tục và dự phòng cho Trung tâm Điều khiển hiện tại, mô hình sẽ được thiết kế như sau:



TKTC-BV 4 Thiết kế Trung tâm Điều khiển mới

- Các máy chủ ảo hóa của các giải pháp đảm bảo ATTT sẽ được triển khai cài đặt thêm tại TTĐK mới, hoạt động theo cơ chế đảm bảo tính sẵn sàng Active/Standby với máy chủ đang hoạt động tại TTĐK hiện có.

- Để đảm bảo tính dự phòng và tính liên tục thì việc đồng bộ dữ liệu giữa các máy chủ của các giải pháp là vô cùng quan trọng. Vậy cần một kênh truyền kết nối trực tiếp giữa 02 TTĐK để đồng bộ dữ liệu và tín hiệu trạng thái trong thời gian thực. Khi TTĐK chính đang hoạt động gặp một sự cố chưa thể khắc phục được ngay thì TTĐK dự phòng sẽ chuyển trạng thái Active thay thế đảm bảo hệ thống hoạt động và được bảo vệ liên tục.

- TTĐK dự phòng cũng sẽ có đầy đủ các kết nối xuống các TBA, Công ty điện lực, Công ty lưới điện cao thế tương tự như TTĐK chính để đảm bảo tính liên tục trong kết nối và áp dụng các chính sách, thu thập thông tin về ATTT.

Trạm biến áp không người trực và 08 tổ TTLĐ:

- 01 tường lửa (OT Firewall) có chức năng IPS/IDS để kiểm soát luồng thông tin vào/ra trạm, giảm thiểu truy cập không được phép, mã độc lan truyền từ mạng WAN vào bên trong trạm.

- Giải pháp bảo vệ điểm cuối để bảo vệ các máy tính trước mối đe dọa về mã độc lây lan vào máy.

- Giải pháp xác thực đa yếu tố MFA tăng cường quản lý và bảo vệ tài khoản đăng nhập vào máy tính để làm việc.

- Giải pháp PIM/PAM bổ sung lớp bảo vệ cho các tài khoản đặc quyền.

- Giải pháp quản lý thông tin và sự kiện an ninh mạng (SIEM) cho phép thu thập, lưu trữ, xử lý nhật ký hoạt động (log) phát sinh trên các máy chủ, máy trạm, cơ sở dữ liệu, thiết bị mạng tại các trạm biến áp. Ngoài ra để giám sát việc thay đổi cấu hình trên các máy chủ, máy trạm thì trên các thiết bị này sẽ được cài đặt agent để thu thập log và đẩy về giải pháp thu thập và quản lý nhật ký sự kiện an ninh tập trung

- Tại 08 đội quản lý vận hành sẽ được triển khai thêm tại mỗi đội 01 thiết bị chuyển mạch để phục vụ đấu nối.

Công ty lưới điện cao thế và Khối Công ty điện lực:

- Giải pháp bảo vệ điểm cuối để bảo vệ các máy tính trước mối đe dọa về mã độc lây lan vào máy.

- Giải pháp xác thực đa yếu tố MFA tăng cường quản lý và bảo vệ tài khoản đăng nhập vào máy tính để làm việc.

Tổng hợp khối lượng thiết bị và phần mềm:

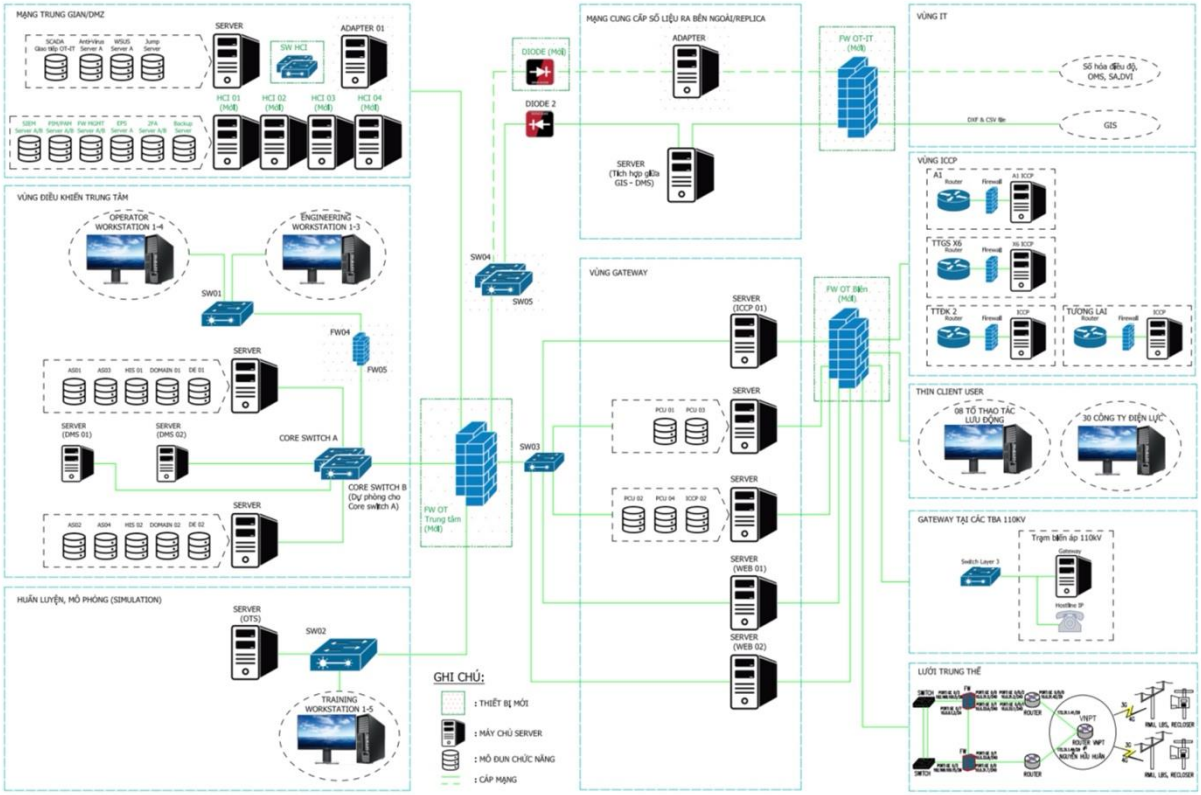
STT	TÊN HẠNG MỤC	Đơn vị tính	SỐ LƯỢNG	LƯU Ý
I	**Firewall tại TTĐK**			
	Firewall tại TTĐK (Firewall OT Core tại TTĐK)	Thiết bị	02	- Giữ nguyên số lượng, cấu hình so Thiết kế cơ sở
II	**Firewall tại các TBA**			
	Firewall OT loại 2	Thiết bị	66	- Giữ nguyên số lượng, cấu hình so Thiết kế cơ sở
III	**Giải pháp quản lý tường lửa tập trung**	Gói	01	- Giữ nguyên số lượng, cấu hình so Thiết kế cơ sở
IV	**Giải pháp cổng một chiều (USG/ Datadiode)**	Thiết bị	01	- Giữ nguyên số lượng, cấu hình so Thiết kế cơ sở
V	**Bản quyền giải pháp EPS**	Bản quyền	270	Thay đổi theo số lượng thực tế thiết bị
VI	**Bản quyền giải pháp PIM/PAM**	Gói	01	- Giữ nguyên số lượng, cấu hình so Thiết kế cơ sở
VII	**Bản quyền giải pháp 2FA**	Gói	01	- Giữ nguyên số lượng, cấu hình so Thiết kế cơ sở

STT	TÊN HẠNG MỤC	Đơn vị tính	SỐ LƯỢNG	LƯU Ý
VIII	**Bản quyền giải pháp SIEM**	Gói	01	- Giữ nguyên số lượng, cấu hình so Thiết kế cơ sở
IX	**Bản quyền giải pháp backup**	Gói	01	- Giữ nguyên số lượng, cấu hình so Thiết kế cơ sở
X	**Máy chủ HCI**			- Giữ nguyên số lượng, cấu hình so Thiết kế cơ sở
A	Thiết bị Hyper Converge	Thiết bị	04	- Giữ nguyên số lượng, cấu hình so Thiết kế cơ sở
B	Bản quyền phần mềm đối với mỗi thiết bị Hyper Converge	Bản quyền	04	- Giữ nguyên số lượng, tuy nhiên yêu cầu phần mềm so với Thiết kế cở sở để phù hợp với các giải pháp HCI trên thị trường tại thời điểm làm Thiết kế cơ sở
C	Thiết bị Switch back-end	Thiết bị	02	- Giữ nguyên số lượng, cấu hình so Thiết kế cơ sở
XI	**Máy trạm**		04	- Giữ nguyên số lượng, cấu hình so Thiết kế cơ sở

1.4 Thiết kế kỹ thuật chi tiết

1.4.1 Mô hình thiết kế luận lý tại TTĐK

Dưới đây là mô hình thiết kế luận lý cho toàn bộ hệ thống:



TKTC-BV 5 Mô hình thiết kế luận lý cho toàn bộ hệ thống

Mô tả và diễn giải mô hình thiết kế:

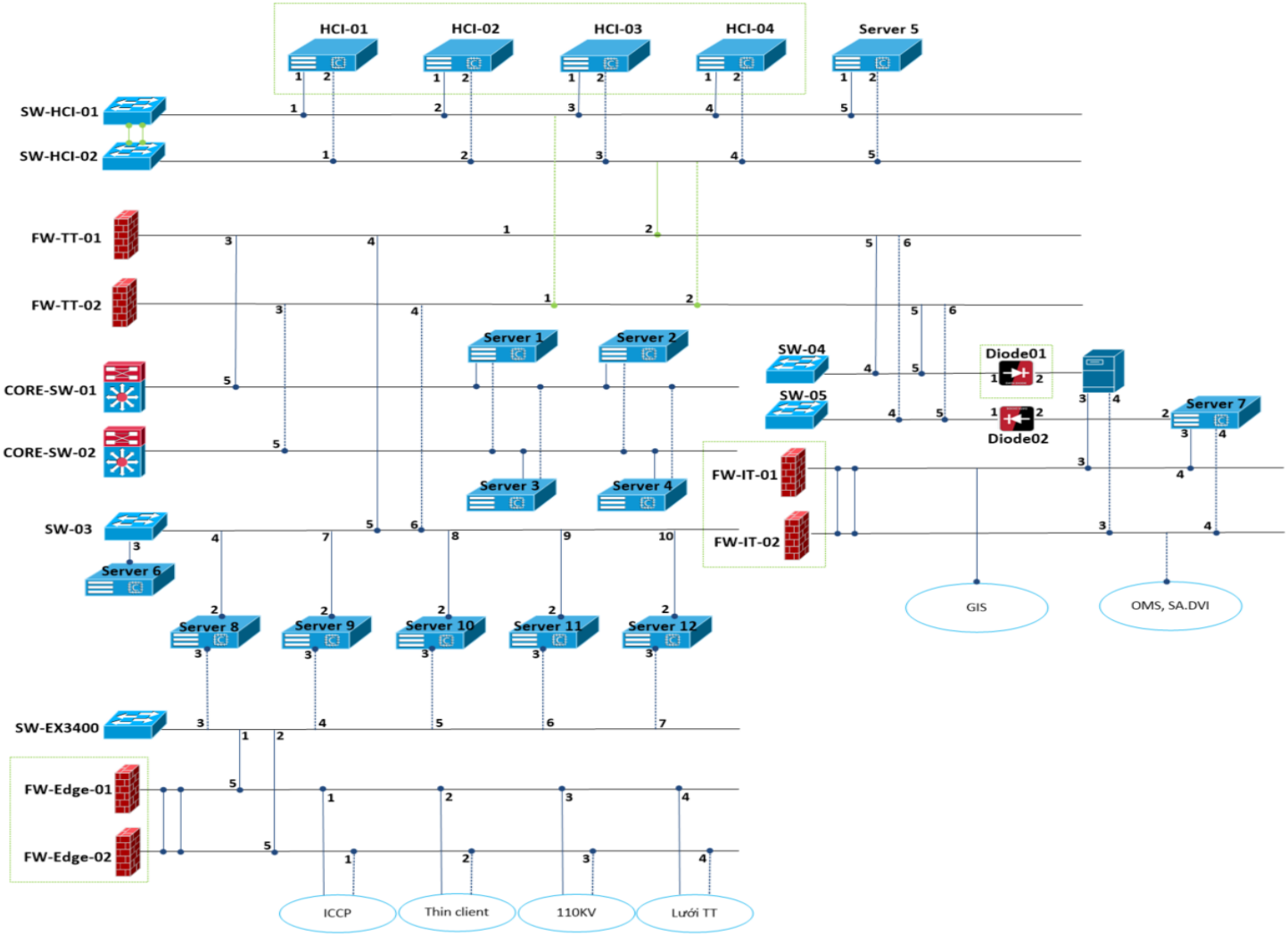
Căn cứ vào các giải pháp và thiết bị được đề xuất, áp dụng vào hiện trạng hệ thống Giám sát và điều khiển tự động hóa của EVNHN cụ thể như sau:

- 02 thiết bị Firewall OT mới sẽ được bổ sung đóng vai trò là trung tâm kiểm soát kết nối và thiết lập chính sách giữa các phân vùng nội bộ trại TTĐK. 02 thiết bị tường lửa này sẽ được chạy với chế độ High Availability Active/Passive để đảm bảo khả năng dự phòng. Cặp thiết bị tường lửa mới này sẽ đảm nhận nhiệm vụ kiểm soát và ứng dụng các tính năng bảo mật nâng cao để bảo vệ truy cập thông qua WAN giữa TTĐK và các TBA 110/220KV, 12 Công ty Điện lực, hệ thống số hóa, người dùng tại các đơn vị…
- 01 thiết bị cổng an ninh một chiều (USG/Datadiode) sẽ được triển khai mới để thay thế cho thiết bị USG/Datadiode cũ nhằm kiểm soát truy cập giữa mạng IT (hệ thống OMS, hệ thống GIS...) và mạng OT/SCADA.
- Hạ tầng máy chủ mới bao gồm 04 máy chủ HCI và 02 thiết bị chuyển mạch mới sẽ được triển khai để phục vụ cài đặt và đấu nối cho các máy chủ ảo hóa của các giải pháp SIEM, PIM/PAM, Firewall Management, 2FA, EPS…
- Ngoài ra, các phần mềm và bản quyền như Backup sẽ được triển khai giúp đảm bảo an toàn giúp có thể khôi phục khi có sự cố mất mát hoặc mã hóa dữ liệu.
- Giải pháp quản lý và thu thập các sự kiện, nhật ký tập trung như SIEM sẽ giúp tương quan đưa ra các cảnh báo sớm về các nguy cơ mất an toàn thông tin trong hệ thống.

- Giải pháp xác thực 02 nhân tố 2FA sẽ giúp đảm bảo an toàn cho người dùng, người quản trị vận hành có thể được xác thực mạnh trước khi đăng nhập vào hệ thống.
- Giải pháp bảo vệ cho thiết bị đầu cuối EPS có các tính năng phân tích hành vi đưa ra các biện pháp ngăn chặn các cuộc tấn công lây nhiễm mã độc.
- Giải pháp Quản lý tài khoản đặc quyền PIM/PAM giúp quản lý, giám sát đồng nhất và lưu giữ một cách an toàn cho các tài khoản quản trị có quyền cao nhất trong hệ thống. Phân tách và quản lý theo vai trò của các cán bộ quản trị hệ thống.
- Tại các Trạm biến áp 110/220KV sẽ triển khai tại mỗi trạm một thiết bị Firewall để bảo vệ luồng dữ liệu vào ra. Các thiết bị này sẽ được quản trị tập trung tại máy chủ quản trị Firewall được đặt tại TTĐK thông qua kết nối WAN-HTĐ.

1.4.2 Mô hình thiết kế vật lý tại TTĐK

Dưới đây là mô hình thiết kế vật lý:



TKTC-BV 6 Mô hình thiết kế vật lý tại TTĐK

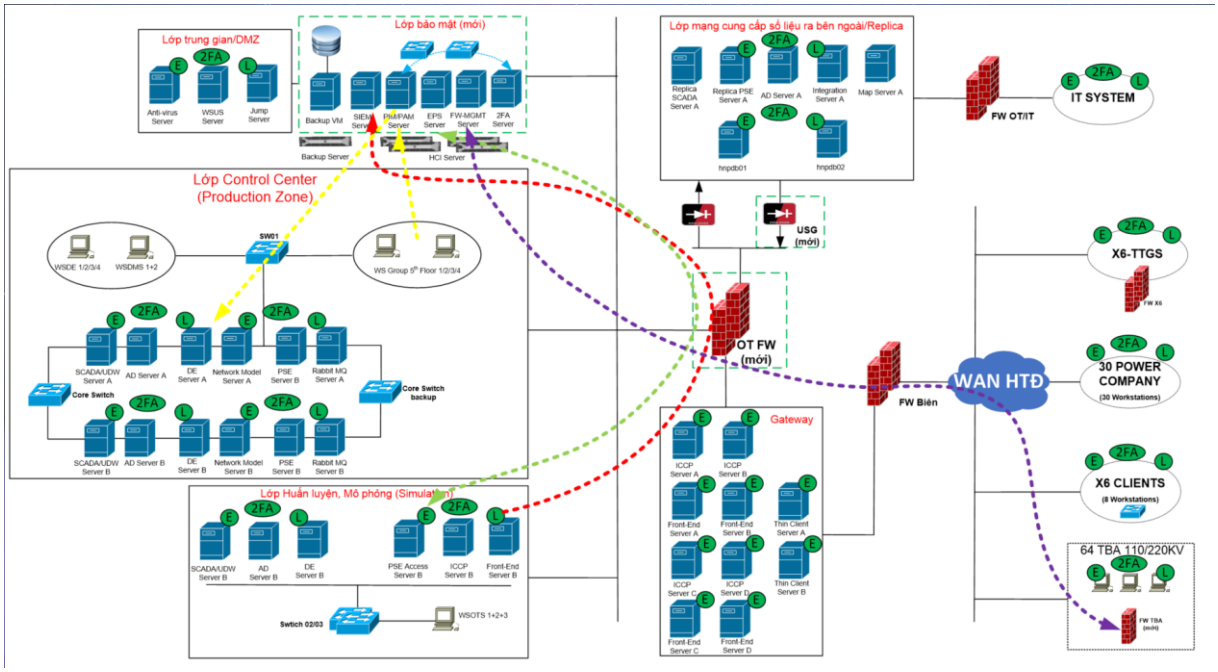
Bảng thông tin đấu nối:

STT	Điểm đầu					Điểm cuối			
	R-U	Thiết bị	Cổng	Cáp	Tốc độ	R-U	Thiết bị	Cổng	Mode
1	R8U32	FW CORE 01	HA1	Đồng	1Gbps	R8U33	FW CORE 02	HA1	Auto
2	R8U32	FW CORE 01	HA2	Đồng	1Gbps	R8U33	FW CORE 02	HA2	Auto
3	R8U32	FW CORE 01	Eth1	Đồng	1Gbps	R7U30	SW02	Eth10	Auto
4	R8U33	FW CORE 01	Eth2	Đồng	1Gbps	R7U27	SW03	Eth10	Auto
5	R8U33	FW CORE 01	Eth3	Đồng	1Gbps	R7U30	Core SW A	Eth3	Auto
6	R8U32	FW CORE 01	Eth4	Đồng	1Gbps	R7U30	Core SW B	Eth3	Auto
7	R8U33	FW CORE 02	Eth1	Đồng	1Gbps	R7U30	SW02	Eth11	Auto
8	R8U32	FW CORE 02	Eth2	Đồng	1Gbps	R7U27	SW03	Eth11	Auto
9	R8U32	FW CORE 02	Eth3	Đồng	1Gbps	R7U30	Core SW A	Eth4	Auto
10	R8U32	FW CORE 02	Eth4	Đồng	1Gbps	R7U30	Core SW B	Eth4	Auto
11	R7U19-20	HCI Server 01	Eth1	Đồng	1Gbps	R7U27	SW HCI 01	Eth1	Auto
12	R7U19-20	HCI Server 01	Eth2	Đồng	1Gbps	R7U27	SW HCI 01	Eth2	Auto
13	R7U19-20	HCI Server 01	Eth3	Đồng	1Gbps	R7U30	SW HCI 02	Eth1	Auto
14	R7U19-20	HCI Server 01	Eth4	Đồng	1Gbps	R7U30	SW HCI 02	Eth2	Auto
15	R7U31-32	HCI Server 02	Eth1	Đồng	1Gbps	R7U27	SW HCI 01	Eth3	Auto
16	R7U31-32	HCI Server 02	Eth2	Đồng	1Gbps	R7U27	SW HCI 01	Eth4	Auto
17	R7U31-32	HCI Server 02	Eth3	Đồng	1Gbps	R7U30	SW HCI 02	Eth3	Auto
18	R7U31-32	HCI Server 02	Eth4	Đồng	1Gbps	R7U30	SW HCI 02	Eth4	Auto
19	R7U33-34	HCI Server 03	Eth1	Đồng	1Gbps	R7U27	SW HCI 01	Eth5	Auto
20	R7U33-34	HCI Server 03	Eth2	Đồng	1Gbps	R7U27	SW HCI 01	Eth6	Auto
21	R7U33-34	HCI Server 03	Eth3	Đồng	1Gbps	R7U30	SW HCI 02	Eth5	Auto
22	R7U33-34	HCI Server 03	Eth4	Đồng	1Gbps	R7U30	SW HCI 02	Eth6	Auto

STT	Điểm đầu					Điểm cuối			
	R-U	Thiết bị	Cổng	Cáp	Tốc độ	R-U	Thiết bị	Cổng	Mode
23	R7U35-36	HCI Server 04	Eth1	Đồng	1Gbps	R7U27	SW HCI 01	Eth7	Auto
24	R7U35-36	HCI Server 04	Eth2	Đồng	1Gbps	R7U27	SW HCI 01	Eth8	Auto
25	R7U35-36	HCI Server 04	Eth3	Đồng	1Gbps	R7U30	SW HCI 02	Eth7	Auto
26	R7U35-36	HCI Server 04	Eth4	Đồng	1Gbps	R7U30	SW HCI 02	Eth8	Auto
27	R7U27	SW HCI 01	Eth23	Đồng	1Gbps	R7U27	SW HCI 01	Eth23	Auto
28	R7U30	SW HCI 02	Eth24	Đồng	1Gbps	R7U30	SW HCI 02	Eth24	Auto
29	R7U27	SW HCI 01	Eth22	Đồng	1Gbps		SW02	Eth22	Auto
30	R7U30	SW HCI 02	Eth22	Đồng	1Gbps		SW03	Eth22	Auto
31	R8U27	Backup Server	Eth1	Đồng	1Gbps	R7U27	SW HCI 01	Eth7	Auto
32	R8U27	Backup Server	Eth2	Đồng	1Gbps	R7U30	SW HCI 02	Eth7	Auto
33	R8U230-31	Backup Storage	Eth1	Đồng	1Gbps	R7U27	SW HCI 01	Eth5	Auto
34	R8U230-31	Backup Storage	Eth2	Đồng	1Gbps	R7U30	SW HCI 01	Eth6	Auto
35	R8U230-31	Backup Storage	Eth3	Đồng	1Gbps	R7U27	SW HCI 02	Eth5	Auto
36	R8U230-31	Backup Storage	Eth4	Đồng	1Gbps	R7U30	SW HCI 02	Eth6	Auto

1.4.3 Mô hình luồng dữ liệu tại TTĐK

Dưới đây là mô hình mô tả luồng kết nối giữa các thành phần của giải pháp đảm bảo ATTT cho Trung tâm điều khiển:



Mô tả:

Chúng tôi sử dụng các ký hiệu và đường nét đứt với các màu khác nhau để mô tả về luồng kết nối giữa các thành phần trong hệ thống ATTT cho TTĐK như sau:

- Ký hiệu chữ E trong hình tròn màu xanh thể hiện cho thành phần Endpoint Security Agent được cài đặt trên các máy trạm và máy chủ trong TTĐK và các TBA.
- Ký hiệu chữ 2FA nằm trong hình oval màu xanh thể hiện cho thành phần giải pháp Xác thực 02 yếu tố. Toàn bộ các quản trị viên đều phải xác thực với máy chủ 2FA thông qua giao thức RADIUS.
- Kỹ hiệu chữ L nằm trong hình tròn màu xanh thể hiện cho thành phần giải pháp Quản lý thông tin và sự kiện an ninh tập trung SIEM.
- Đường nét đứt màu đỏ thể hiện cho kết nối từ agent/syslog trên các máy chủ ứng dụng của hệ thống TTĐK về máy chủ SIEM để quản lý tập trung thông tin về nhật ký và sự kiện.
- Đường nét đứt màu xanh lá thể hiện kết nối giữa các Endpoint Security Agent được cài đặt trên các máy trạm và máy chủ. Các agent này sẽ được quản lý và cập nhật chính sách, các mẫu mã độc từ máy chủ Endpoint Security Server.
- Đường nét đứt màu vàng thể hiện kết nối từ các máy giám sát phải đi qua máy chủ PIM/PAM, áp dụng các chính sách, phân quyền và được ghi lại quá trình thao tác đối với các máy chủ tại TTĐK.
- Đường nét đứt màu xanh da trời thể hiện việc xác thực 02 yếu tố giữa quản trị viên sử dụng tài khoản để truy cập máy chủ thông qua máy chủ PIM/PAM.

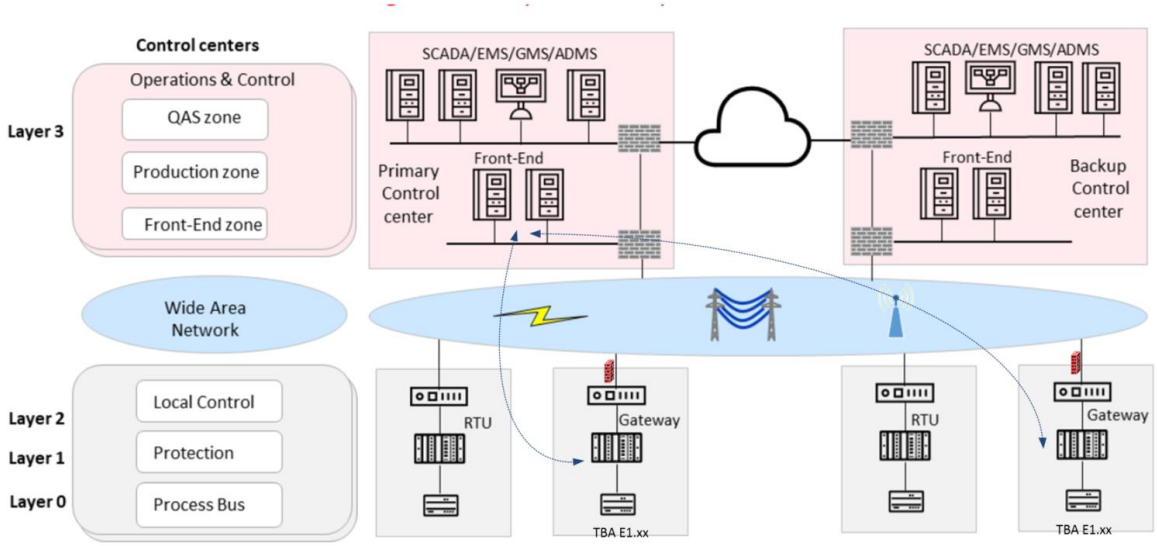
- Đường nét đứt màu tím thể hiện tổng hợp các kết nối cho quản trị tường lửa, cập nhật và quản lý endpoint agent, log từ các máy chủ/thiết bị tại TBA lên các máy chủ của hệ thống đảm bảo ATTT tại TTĐK.

Tại Trung tâm điều khiển, sẽ được phân chia thành các phân vùng chính theo QĐ 168 và với các VLAN tương ứng được mô tả như sau:

- Replica: Vùng mạng đặt các máy chủ, ứng dụng cung cấp số liệu ra bên ngoài hệ thống.
- DMZ: Vùng mạng trung gian đặt các máy chủ, ứng dụng, giải pháp đảm bảo ATTT cho dữ liệu vào/ra hệ thống TTĐK.
- Control Center: Vùng mạng lớp điều kiển trung tâm đặt các gồm các máy HMI, máy chủ điều khiển, HIS, máy vận hành, máy cấu hình (EWS).
- Simulation: Vùng mạng phục vụ các máy chủ, ứng dụng để huấn luyện và mô phỏng.
- Gateway: Vùng mặt đặt các máy chủ ứng dụng, dịch vụ giao tiếp với mạng OT WAN, nhận/gửi số liệu tới các TBA.

1.4.4 Mô hình luồng kết nối từ TBA về TTĐK

Dưới đây là mô hình mô tả luồng kết nối từ các TBA về TTĐK



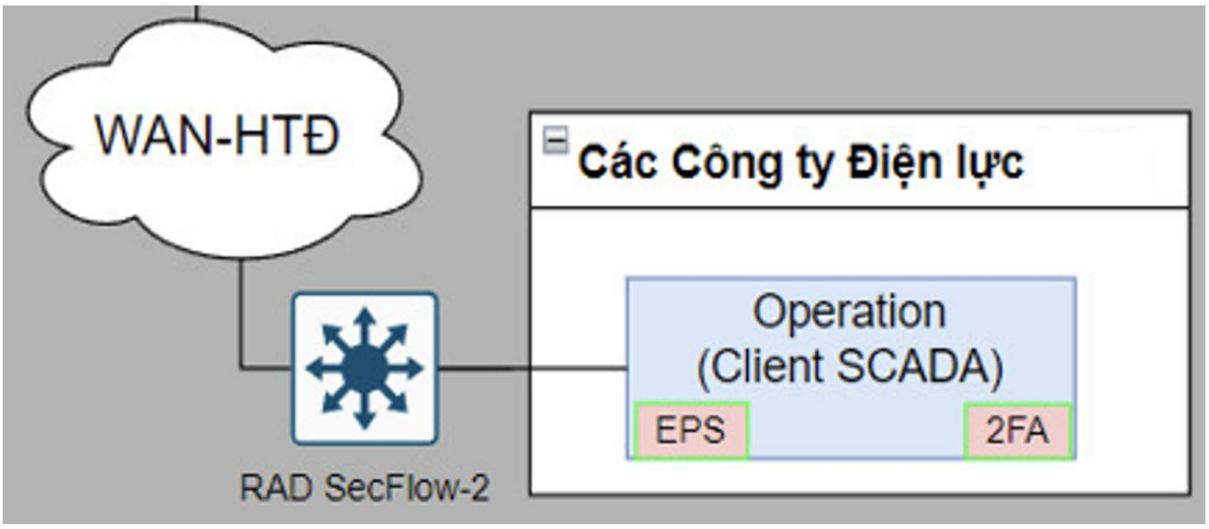
TKTC-BV 7 Mô hình mô tả luồng kết nối từ các TBA về TTĐK

Toàn bộ các kết nối trao đổi thông tin dựa trên các giao thức ICCP/TASE.2, DNP3.. giữa các máy tính gateway tại TBA, RTU và các máy chủ ICCP, Front-End tại TTĐK, sẽ được kiểm soát và áp dụng các tính năng bảo mật trên các thiết bị OT Firewall trang bị mới tại TBA và cặp OT Firewall được trang bị mới tại vùng biên của TTĐK.

1.4.5 Mô hình thiết kế tại các Công ty Điện lực

Tại thời điểm khảo sát là có 30 Công ty Điện lực, tuy nhiên theo công văn số 3687/EVN-TCNS ban hành ngày 10 tháng 06 năm 2025 về việc triển khai sắp xếp tinh gọn tổ chức, bộ máy quản lý, điều hành của EVNHANOI thì số lượng Công ty điện lực cập nhật là 12 công ty.

Dưới đây là mô hình thiết kế luận lý cho các Công ty Điện lực:



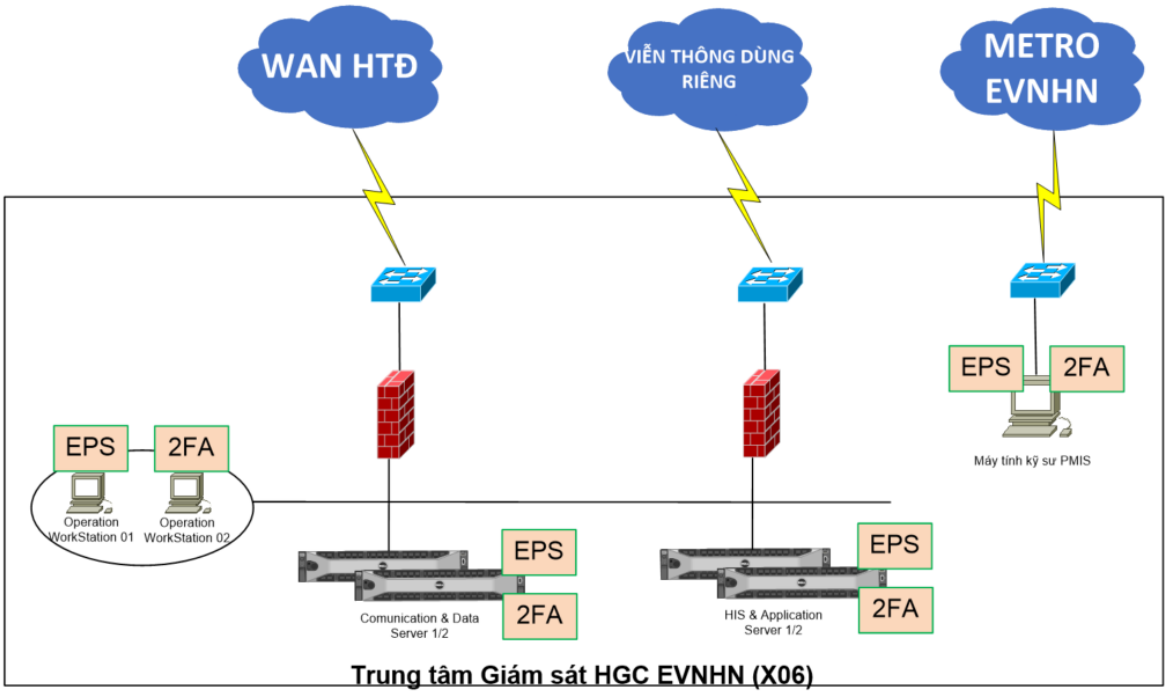
TKTC-BV 8 Mô hình thiết kế luận lý cho các Công ty Điện lực

Tại công ty điện lực các Quận, Huyện đều có máy tính HMI được cài đặt phần mềm Client SCADA Zenon - đóng vai trò client SCADA cho phép giám sát, điều khiển lưới điện trung thế thông qua Trung tâm điều độ. Hiện tại mỗi Công ty Điện lực trang bị một máy trạm client SCADA, chỉ kết nối trao đổi dữ liệu với TTĐK và không chia sẻ hay kết nối sang hệ thống nào khác. Dữ liệu trạng thái và các lệnh điều khiển của lưới trung thế sẽ được thu thập và xử lý tại Trung tâm điều độ, sau đó chia sẻ quyền giám sát, điều khiển xuống các máy trạm Client SCADA tại các Điện lực. Khi một Công ty Điện lực được cấp quyền điều khiển, lệnh điều khiển sẽ được gửi về Trung tâm và qua đó điều khiển các thiết bị trên lưới trung thế do Công ty Điện lực đó quản lý vận hành.

Các máy trạm HMI này kết nối trực tiếp vào thiết bị mạng để ra mạng WAN-HTĐ. Như vậy, với tất cả các rủi ro được tính đến, máy trạm này sẽ được cài đặt phần mềm endpoint protection được áp dụng chính sách bảo vệ từ máy chủ EPS đặt tại TTĐK. Ngoài ra, cán bộ quản trị và vận hành khi đăng nhập vào máy trạm này sẽ phải xác thực qua 02 yếu tố và máy chủ đóng vai trò xác thực định danh truy cập sẽ là máy chủ 2FA đặt tại TTĐK.

1.4.6 Mô hình thiết kế tại Công ty Lưới điện cao thế (TTGS X6)

Dưới đây là mô hình thiết kế cho Công ty Lưới điện cao thế:



TKTC-BV 9 Mô hình thiết kế cho Công ty Lưới điện cao thế

Công ty lưới điện là đơn vị trực tiếp quản lý, vận hành các trạm biến áp không người trực. Tại đây có một Trung tâm giám sát bao gồm các máy chủ, máy trạm, cơ sở dữ liệu phục vụ chức năng này.

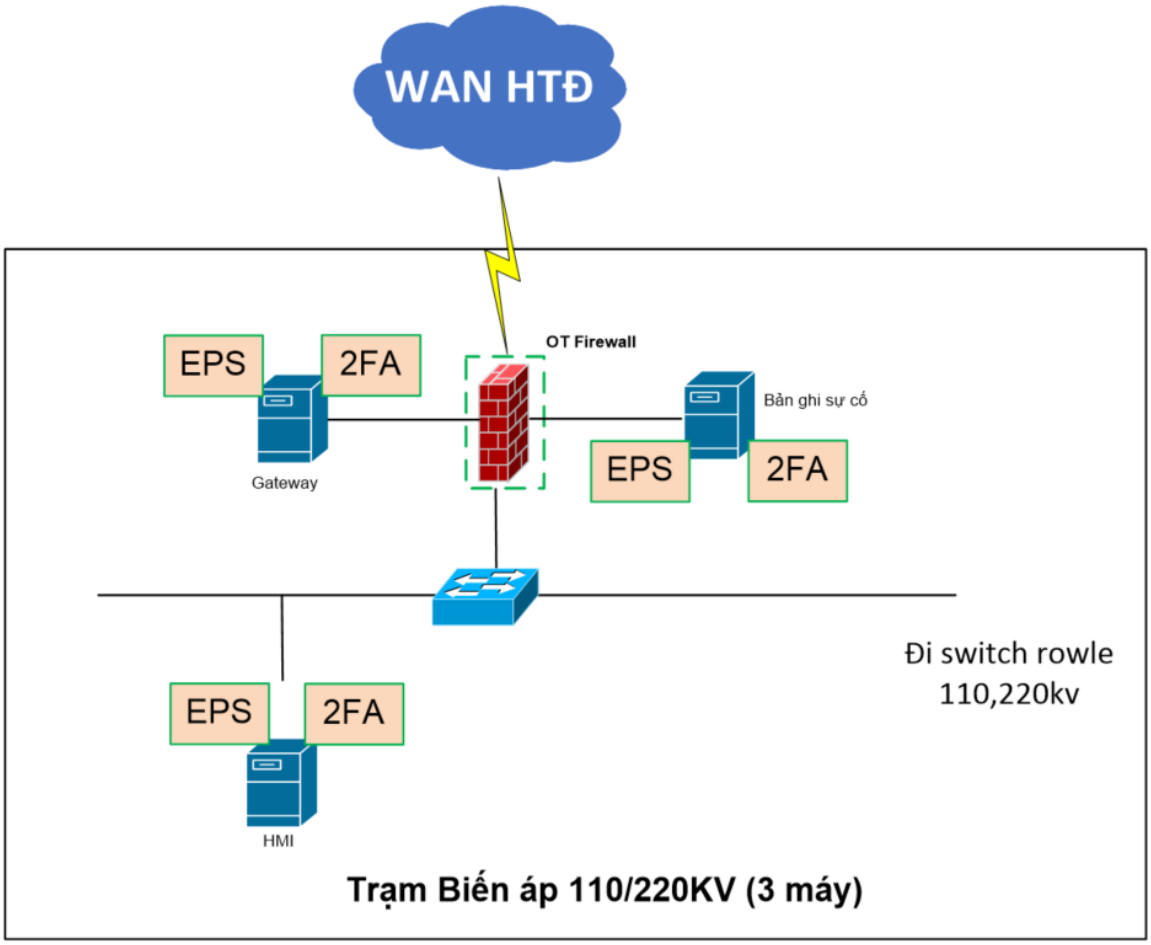
Hiện tại, TTGS tại Công ty Lưới điện cao thế đã có sẵn các thiết bị Tường lửa mới được đầu tư, đóng vai trò kiểm soát và bảo vệ các kết nối trao đổi thông tin giữa X6, TTĐK và các TBA không người trực.

Vậy để đảm bảo an toàn một các toàn diện hơn nữa, các máy chủ, máy trạm, sẽ được cài đặt phần mềm endpoint protection với các chính sách bảo mật được áp dụng và quản lý bởi máy chủ EPS đặt tại TTĐK.

Ngoài ra, các cán bộ quản trị và vận hành hệ thống sẽ cần phải xác thực 2 yếu tố khi đăng nhập vào toàn bộ các máy chủ và máy trạm. Việc xác thực này sẽ được đảm nhiệm bởi máy chủ 2FA đặt tại TTĐK.

1.4.7 Mô hình thiết kế cho các Trạm biến áp không người trực 110/220KV (64 trạm)

Dưới đây là mô hình thiết kế cho các TBA 110/220KV có 03 máy:



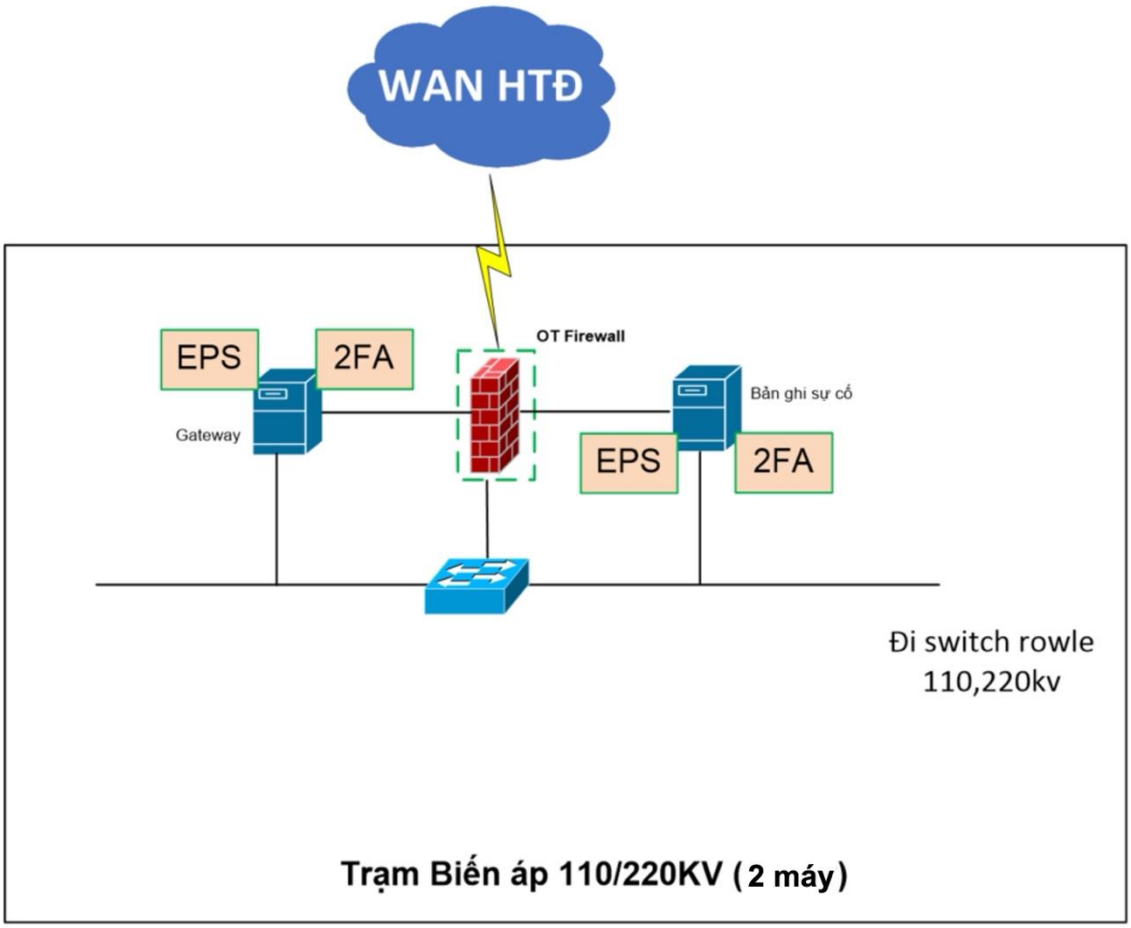
TKTC-BV 10 Mô hình thiết kế cho các TBA 110/220KV (Trạm có 03 máy)

Các trạm biến áp không người trực 110KV và 220KV bao gồm máy trạm điều khiển, máy trạm HMI, máy bản ghi sự cố và thiết bị mạng.

Với mô hình phòng thủ theo chiều sâu nêu trên, mỗi trạm biến áp không người trực được bảo vệ bởi:

- 01 tường lửa có chức năng IPS để kiểm soát luồng thông tin vào/ra trạm, giảm thiểu truy cập không được phép, mã độc lan truyền từ mạng WAN vào bên trong trạm. Ngoài ra, tường lửa này còn chịu trách nhiệm phân chia ra các phân vùng mạng theo chức năng phù hợp với QĐ/168.
- Giải pháp bảo vệ điểm cuối để bảo vệ các máy tính trước mối đe dọa về mã độc lây lan vào máy.
- Giải pháp xác thực hai yếu tố 2FA tăng cường quản lý và bảo vệ tài khoản đăng nhập vào máy tính để làm việc.

Dưới đây là mô hình thiết kế cho các TBA 110/220KV có 02 máy:



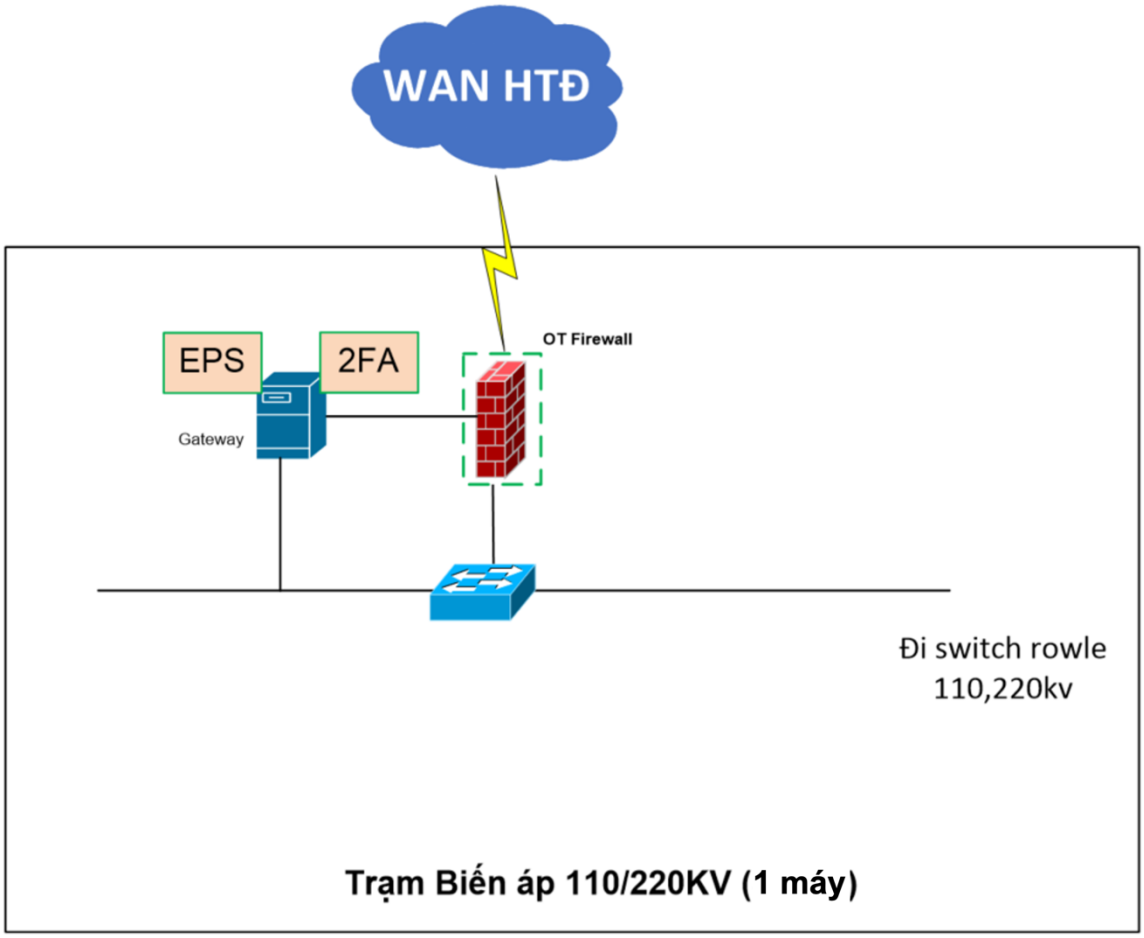
TKTC-BV 11 Mô hình thiết kế cho các TBA 110/220KV (Trạm có 02 máy)

Các trạm biến áp không người trực 110KV và 220KV bao gồm máy trạm điều khiển, máy bản ghi sự cố và thiết bị mạng.

Với mô hình phòng thủ theo chiều sâu nêu trên, mỗi trạm biến áp không người trực được bảo vệ bởi:

- 01 tường lửa có chức năng IPS để kiểm soát luồng thông tin vào/ra trạm, giảm thiểu truy cập không được phép, mã độc lan truyền từ mạng WAN vào bên trong trạm. Ngoài ra, tường lửa này còn chịu trách nhiệm phân chia ra các phân vùng mạng theo chức năng phù hợp với QĐ/168.
- Giải pháp bảo vệ điểm cuối để bảo vệ các máy tính trước mối đe dọa về mã độc lây lan vào máy.
- Giải pháp xác thực hai yếu tố 2FA tăng cường quản lý và bảo vệ tài khoản đăng nhập vào máy tính để làm việc.

Dưới đây là mô hình thiết kế cho các TBA 110/220KV có 01 máy:



TKTC-BV 12 Mô hình thiết kế cho các TBA 110/220KV (Trạm có 01 máy)

Các trạm biến áp không người trực 110KV và 220KV bao gồm máy trạm điều khiển, và thiết bị mạng.

Với mô hình phòng thủ theo chiều sâu nêu trên, mỗi trạm biến áp không người trực được bảo vệ bởi:

- 01 tường lửa có chức năng IPS để kiểm soát luồng thông tin vào/ra trạm, giảm thiểu truy cập không được phép, mã độc lan truyền từ mạng WAN vào bên trong trạm. Ngoài ra, tường lửa này còn chịu trách nhiệm phân chia ra các phân vùng mạng theo chức năng phù hợp với QĐ/168.
- Giải pháp bảo vệ điểm cuối để bảo vệ các máy tính trước mối đe dọa về mã độc lây lan vào máy.
- Giải pháp xác thực hai yếu tố 2FA tăng cường quản lý và bảo vệ tài khoản đăng nhập vào máy tính để làm việc.

1.4.8 Quy hoạch IP, Subnets, VLANs

Quy hoạch IP, VLAN, Subnet

VLAN	Subnet hiện hữu	Subnet bổ sung	Mô tả
TTĐK			
Vlan A	xx.xx.240.0/24		Control Center/Production

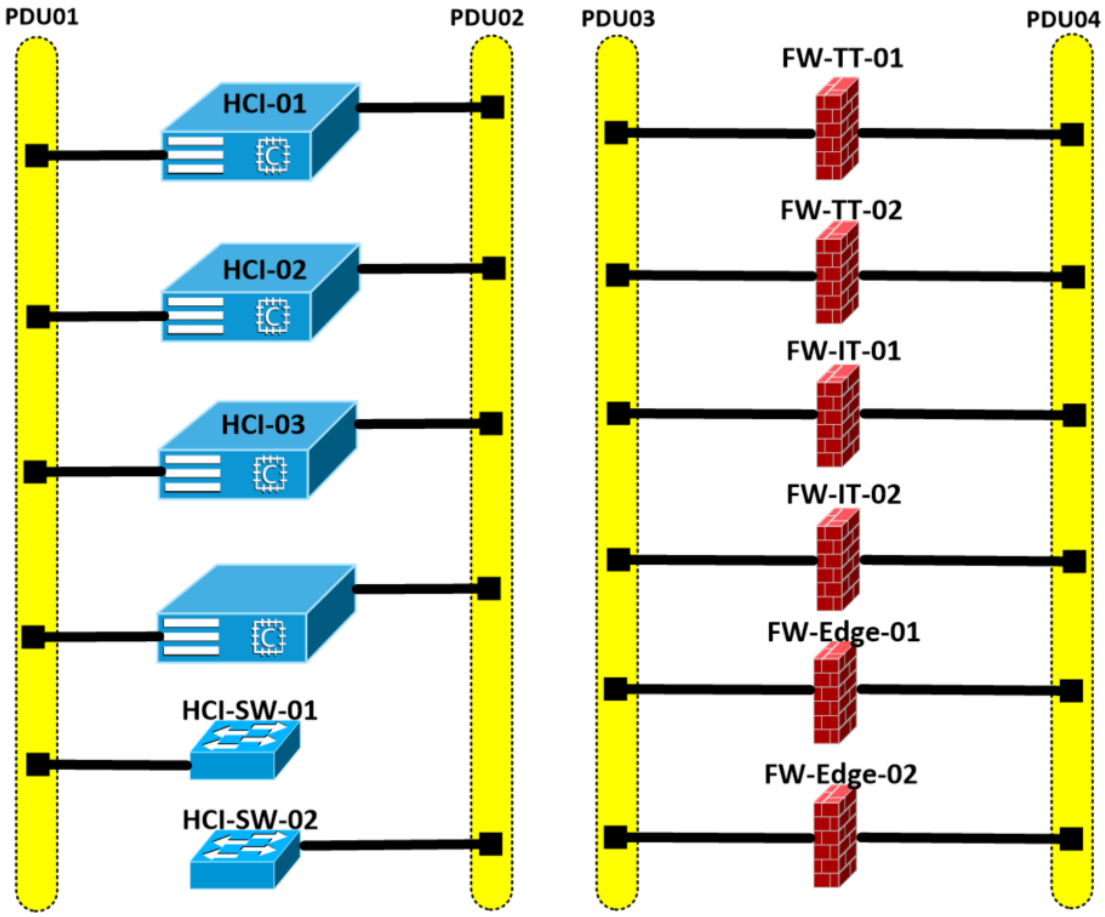
VLAN	Subnet hiện hữu	Subnet bổ sung	Mô tả
			Zone
Vlan B	xx.xx.240.0/24		DMZ Zone
Vlan C	xx.xx.240.0/24		Gateway Zone
Vlan D	xx.xx.240.0/24		OTS Zone
Vlan E	xx.xx.240.0/24		Replica Zone
Vlan F	xx.xx.240.0/24		Device Management Zone
Vlan G	xx.xx.240.0/24		Management & Support Zone
Vlan H	xx.xx.40.0/24		Communication Zone
TBA			
	yy.yy.1.0/24	zz.zz.1.0/24	E1.1 Đông Anh
	yy.yy.2.0/24	zz.zz.2.0/24	E1.2 Gia Lâm
	yy.yy.5.0/24	zz.zz.5.0/24	E1.5 Thượng Đình
	yy.yy.7.0/24	zz.zz.7.0/24	E1.7 Sơn Tây
	yy.yy.8.0/24	zz.zz.8.0/24	E1.8 Yên Phụ
	yy.yy.9.0/24	zz.zz.9.0/24	E1.9 Nghĩa Đô
	yy.yy.10.0/24	zz.zz.10.0/24	E1.10 Văn Điển
	yy.yy.12.0/24	zz.zz.12.0/24	E1.12 Trần Hưng Đạo
	yy.yy.13.0/24	zz.zz.13.0/24	E1.13 Phương Liệt
	yy.yy.14.0/24	zz.zz.14.0/24	E1.14 Giám
	yy.yy.15.0/24	zz.zz.15.0/24	E1.15 Sài Đồng
	yy.yy.16.0/24	zz.zz.16.0/24	E1.16 Nội Bài
	yy.yy.17.0/24	zz.zz.17.0/24	E1.17 Bắc Thăng Long
	yy.yy.18.0/24	zz.zz.18.0/24	E1.18 Bờ Hồ
	yy.yy.20.0/24	zz.zz.20.0/24	E1.20 Thanh Xuân
	yy.yy.21.0/24	zz.zz.21.0/24	E1.21 Nhật Tân
	yy.yy.22.0/24	zz.zz.22.0/24	E1.22 Thanh Nhàn
	yy.yy.24.0/24	zz.zz.24.0/24	E1.24 Hải Bối
	yy.yy.25.0/24	zz.zz.25.0/24	E1.25 Mỹ Đình
	yy.yy.26.0/24	zz.zz.26.0/24	E1.26 Linh Đàm
	yy.yy.27.0/24	zz.zz.27.0/24	E1.27 KĐT Nam Thăng Long
	yy.yy.28.0/24	zz.zz.28.0/24	E1.28 Phùng Xá
	yy.yy.30.0/24	zz.zz.30.0/24	E1.30 Văn Quán
	yy.yy.31.0/24	zz.zz.31.0/24	E1.31 Trôi
	yy.yy.32.0/24	zz.zz.32.0/24	E1.32 Thường Tín
	yy.yy.33.0/24	zz.zz.33.0/24	E1.33 Cầu Diễn
	yy.yy.34.0/24	zz.zz.34.0/24	E1.34 Quất Động
	yy.yy.36.0/24	zz.zz.36.0/24	E1.36 Quang Minh
	yy.yy.37.0/24	zz.zz.37.0/24	E1.37 Bắc An Khánh
	yy.yy.38.0/24	zz.zz.38.0/24	E1.38 Gia Lâm 2

VLAN	Subnet hiện hữu	Subnet bổ sung	Mô tả
	yy.yy.39.0/24	zz.zz.39.0/24	E1.39 Thanh Oai
	yy.yy.41.0/24	zz.zz.41.0/24	E1.41 Mai Lâm
	yy.yy.42.0/24	zz.zz.42.0/24	E1.42 Sân Bay Nội Bài
	yy.yy.43.0/24	zz.zz.43.0/24	E1.43 Mỗ Lao
	yy.yy.44.0/24	zz.zz.44.0/24	E1.44 Sơn Tây 2
	yy.yy.46.0/24	zz.zz.46.0/24	E1.46 Từ Liêm
	yy.yy.47.0/24	zz.zz.47.0/24	E1.47 Long Biên
	yy.yy.48.0/24	zz.zz.48.0/24	E1.48 Quốc Oai
	yy.yy.49.0/24	zz.zz.49.0/24	E1.49 Đông Anh 2
	yy.yy.51.0/24	zz.zz.51.0/24	E1.51 Phú Nghĩa
	yy.yy.52.0/24	zz.zz.52.0/24	E1.52 CV Thống Nhất
	yy.yy.53.0/24	zz.zz.53.0/24	E1.53 Ba Vì
	yy.yy.54.0/24	zz.zz.54.0/24	E1.54 Hòa Lạc
	yy.yy.56.0/24	zz.zz.56.0/24	E1.56 TT Phùng
	yy.yy.57.0/24	zz.zz.57.0/24	E1.57 Minh Khai
	yy.yy.58.0/24	zz.zz.58.0/24	E1.58 Phú Xuyên
	yy.yy.59.0/24	zz.zz.59.0/24	E1.59 Sài Đồng 2
	yy.yy.61.0/24	zz.zz.61.0/24	E1.61 Dương Nội
	yy.yy.62.0/24	zz.zz.62.0/24	E1.62 Ngọc Hồi
	yy.yy.63.0/24	zz.zz.63.0/24	E1.63 Bắc Thành Công
	yy.yy.64.0/24	zz.zz.64.0/24	E1.64 Hồ Yên Sở
	yy.yy.66.0/24	zz.zz.66.0/24	E1.66 Mỹ Đức
	yy.yy.67.0/24	zz.zz.67.0/24	E1.67 Công Viên Thủ Lệ
	yy.yy.68.0/24	zz.zz.68.0/24	E1.68 Chương Mỹ
	yy.yy.69.0/24	zz.zz.69.0/24	E1.69 Trâu Quỳ
	yy.yy.71.0/24	zz.zz.71.0/24	E1.71 Hồng Dương
	yy.yy.72.0/24	zz.zz.72.0/24	E1.72 Kim Chung
	yy.yy.73.0/24	zz.zz.73.0/24	E1.73 CNC2
	yy.yy.74.0/24	zz.zz.74.0/24	E1.74 Thạch Thất 2
Công ty Điện lực			
	yy.yy.230.0/28		C01 Hoàn Kiếm
	yy.yy.230.16/28		C02 Hai Bà Trưng
	yy.yy.230.32/28		C03 Ba Đình
	yy.yy.230.48/28		C04 Đống Đa
	yy.yy.230.64/28		C05 Nam Từ Liêm
	yy.yy.230.80/28		C06 Thanh Trì
	yy.yy.230.96/28		C07 Gia Lâm
	yy.yy.230.112/28		C08 Đông Anh
	yy.yy.230.128/28		C09 Sóc Sơn
	yy.yy.230.144/28		C10 Tây Hồ

VLAN	Subnet hiện hữu	Subnet bổ sung	Mô tả
	yy.yy.230.160/28		C11 Thanh Xuân
	yy.yy.230.176/28		C12 Cầu Giấy
	yy.yy.230.192/28		C13 Hoàng Mai
	yy.yy.230.208/28		C14 Long Biên
	yy.yy.230.224/28		C15 Mê Linh
	yy.yy.230.240/28		C16 Hà Đông
	yy.yy.231.0/28		C17 Sơn Tây
	yy.yy.231.16/28		C18 Chương Mỹ
	yy.yy.231.32/28		C19 Thạch Thất
	yy.yy.231.48/28		C20 Thường Tín
	yy.yy.231.64/28		C21 Ba Vì
	yy.yy.231.80/28		C22 Đan Phượng
	yy.yy.231.96/28		C23 Hoài Đức
	yy.yy.231.112/28		C24 Mỹ Đức
	yy.yy.231.128/28		C25 Phú Xuyên
	yy.yy.231.144/28		C26 Phúc Thọ
	yy.yy.231.160/28		C27 Quốc Oai
	yy.yy.231.176/28		C28 Thanh Oai
	yy.yy.231.192/28		C29 Ứng Hòa
	yy.yy.231.208/28		C30 Bắc Từ Liêm
Công ty lưới điện cao thế và tổ TTLĐ			
	yy.yy.220.0/28		Công ty lưới điện cao thế X6
	yy.yy.220.16/28		Tổ TTLĐ số 1
	yy.yy.220.32/28		Tổ TTLĐ số 2
	yy.yy.220.48/28		Tổ TTLĐ số 3
	yy.yy.220.64/28		Tổ TTLĐ số 4
	yy.yy.220.80/28		Tổ TTLĐ số 5
	yy.yy.220.96/28		Tổ TTLĐ số 6
	yy.yy.220.112/28		Tổ TTLĐ số 7
	yy.yy.220.128/28		Tổ TTLĐ số 8

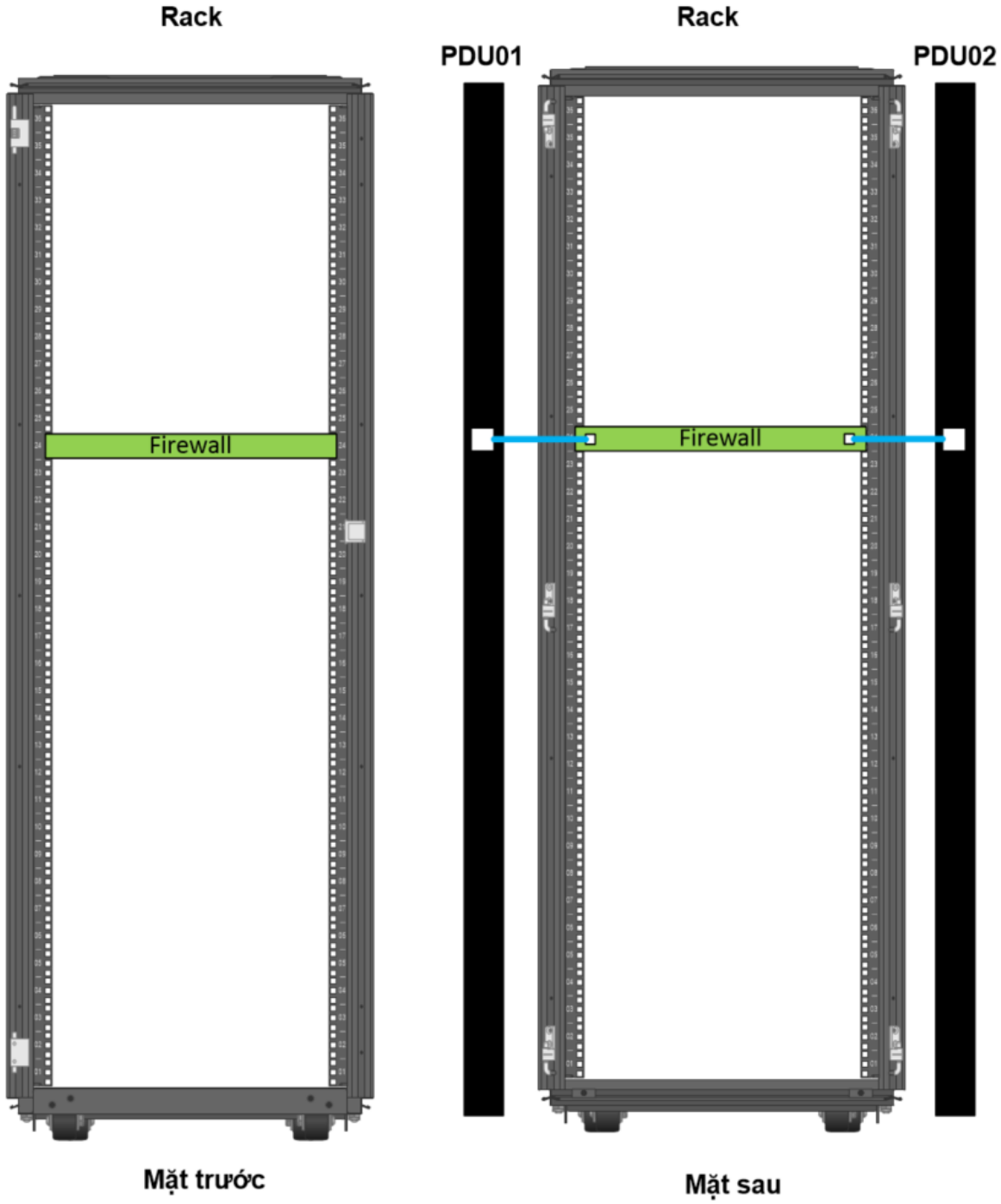
1.4.9 Mô hình đấu nối nguồn cho các thiết bị

Dưới đây là mô hình mô tả thiết kế đấu nối nguồn điện cho các thiết bị tại TTĐK:



TKTC-BV 13 Mô hình bản vẽ cấp nguồn cho các thiết bị tại TTĐK

Dưới đây là mô hình lắp đặt thiết bị tường lửa và đấu nối nguồn tại các TBA không người trực:



1.5 Thiết kế kỹ thuật chi tiết cho các giải pháp

1.5.1 Hệ thống tường lửa

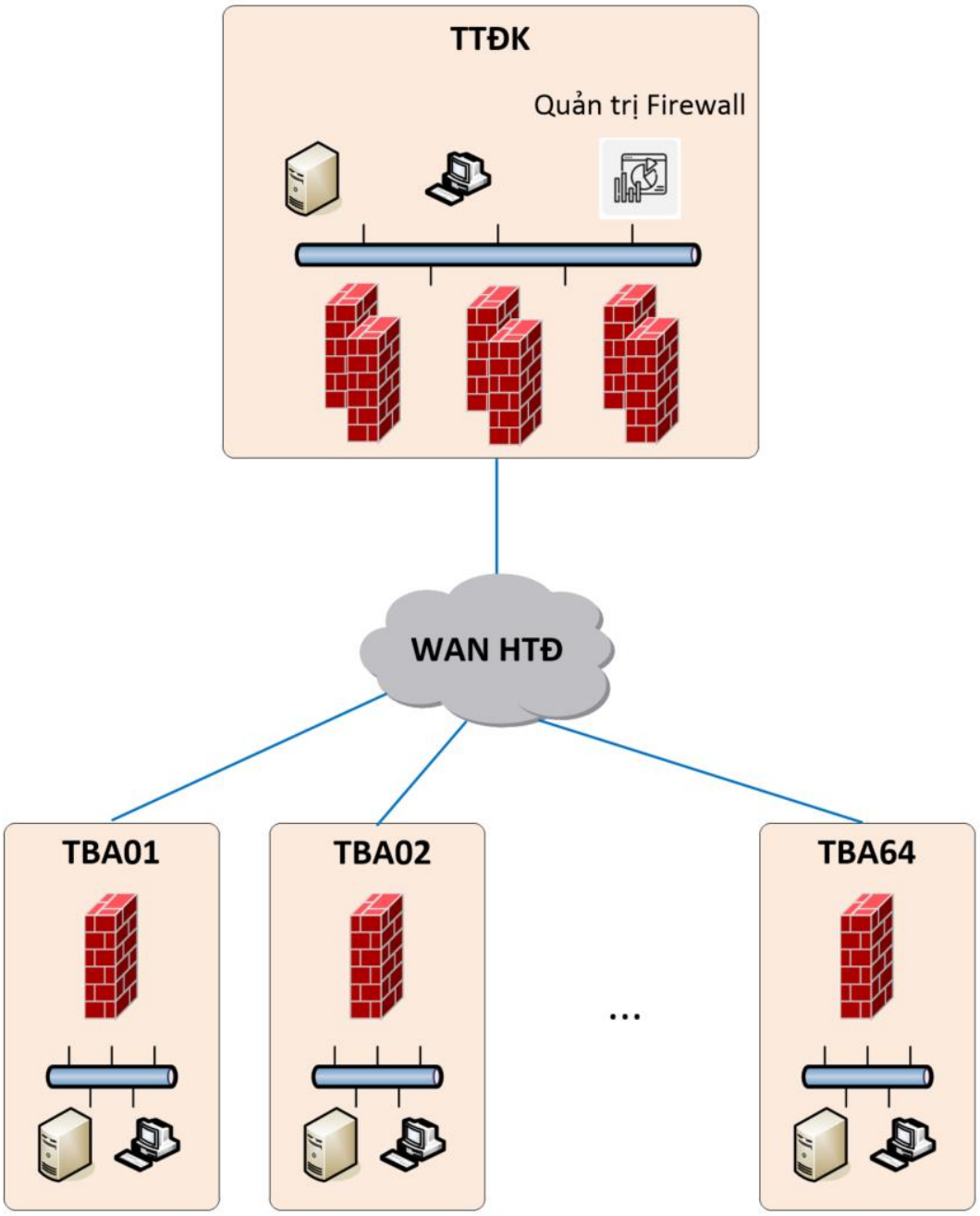
1.5.1.1 Danh mục thiết bị lắp đặt, cài đặt

STT	TÊN HẠNG MỤC	Đơn vị	SỐ LƯỢNG	GHI CHÚ
I	Firewall tại TTĐK	Thiết bị	02	
II	Firewall tại các TBA	Thiết bị	66	Trang bị cho 60 Trạm và 6 Trạm dự phòng

STT	TÊN HẠNG MỤC	Đơn vị	SỐ LƯỢNG	GHI CHÚ
III	Giải pháp quản lý tường lửa tập trung	Gói	01	Quản lý tập trung 68 thiết bị tường lửa hiện tại trong dự án và số lượng thiết bị tường lửa tăng từ 3-5 thiết bị/năm theo nhu cầu tăng trưởng của TBA

1.5.1.2 Mô hình thiết kế luận lý

Mô hình tường lửa tổng thể

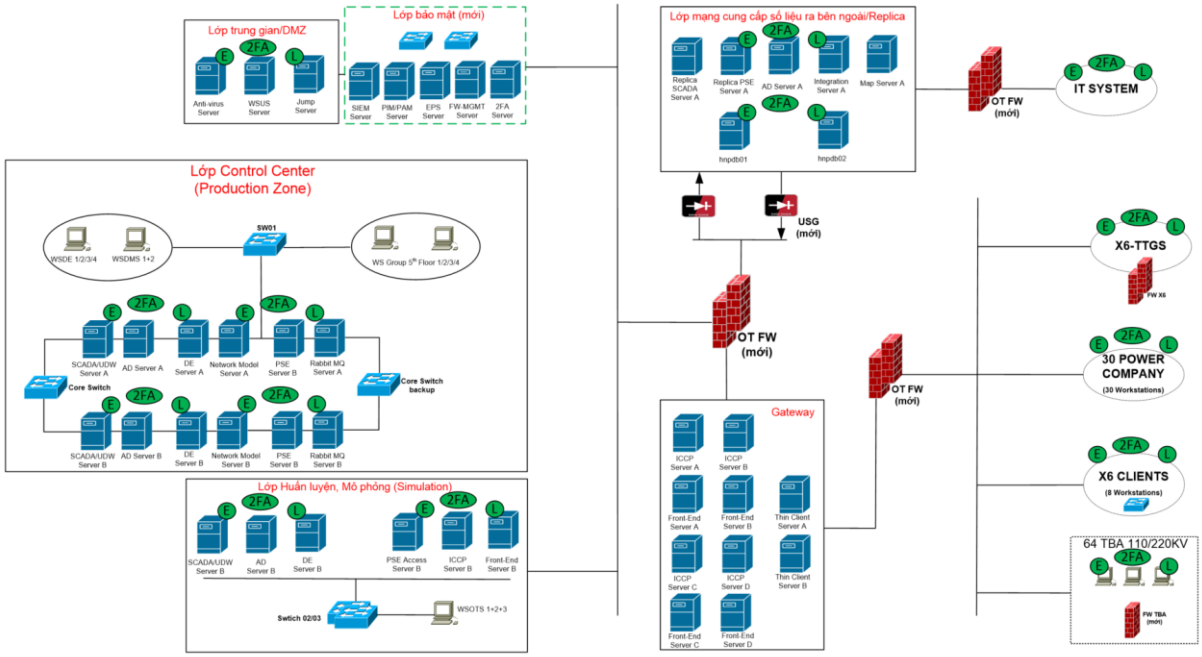


TKTC-BV 14 Mô hình tường lửa tổng thể

Các thiết bị tường lửa sẽ được trang bị tại TTĐK và các TBA nhằm nâng cao khả

năng ngăn chặn xâm nhập và bổ sung các tính năng bảo vệ cho các luồng dữ liệu bên trong và giữa các vùng mạng này.

Mô hình tường lửa tại TTĐK



TKTC-BV 15 Mô hình tường lửa tại TTĐK

01 cặp Firewall OT sẽ được đặt tại TTĐK, từ cặp switch Layer 3 thực hiện định tuyến lên Firewall, Firewall sẽ kiểm soát luồng thông tin trao đổi giữa các khối trong hệ thống mini SCADA và thực hiện định tuyến lại về cặp switch Layer 3 để tiếp tục đi đến các thành phần đích của hệ thống

Giải pháp tường lửa nhằm ngăn chặn xâm nhập có chức năng bảo vệ cho các khối dưới đây trong TTĐK:

- Khối mô phỏng (Simulator): Các máy tính phục vụ mô phỏng đào tạo điều độ viên thực hành điều khiển (OTS – Operator Trainning Simulator).
- Khối máy kỹ sư (EWS – Engineering Workstations): Các máy tính của kỹ sư cấu hình, bảo trì hệ thống SCADA/DMS.
- Khối vận hành (Operation): Các máy tính của kỹ sư Điều độ.
- Khối máy chủ (HMI/Application/HIS Servers): Các máy chủ giao diện người dùng (HMI Servers), máy chủ ứng dụng (Application Servers), máy chủ lưu trữ dữ liệu quá khứ (Historian Servers)

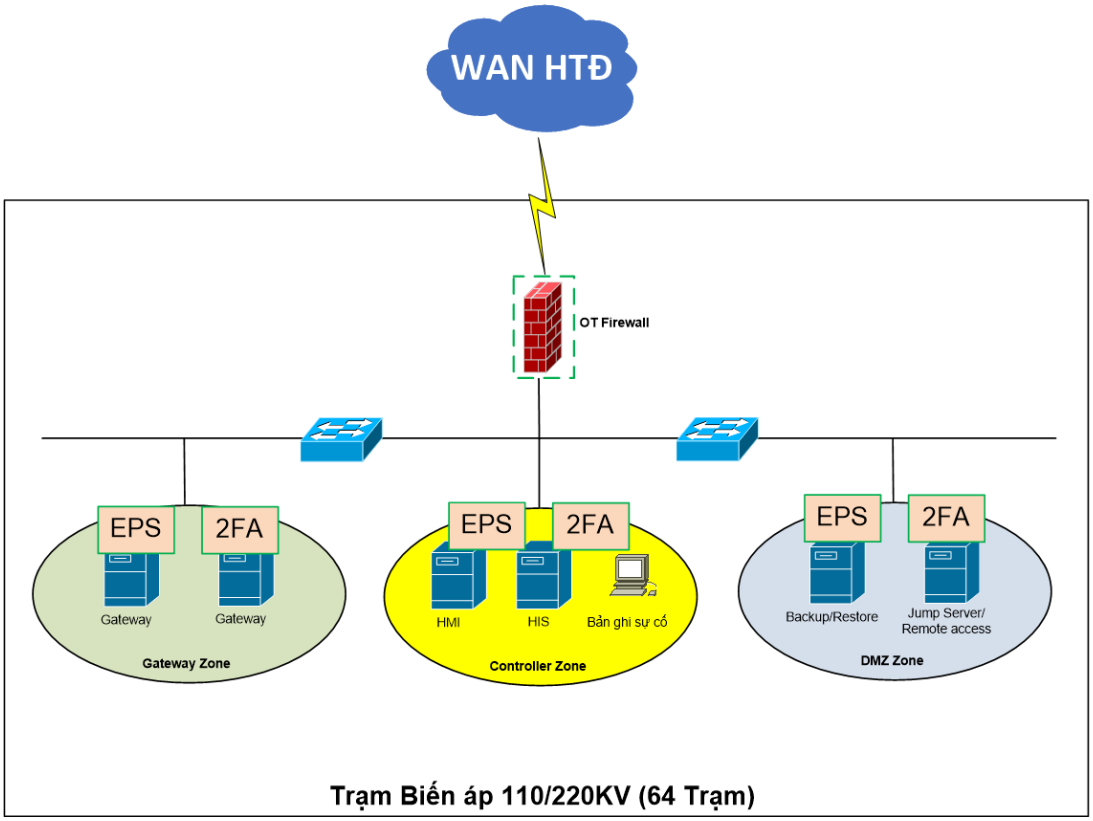
Cài đặt, cấu hình hệ thống quản lý giám sát tập trung thiết bị cho tất cả các thiết bị firewall trong hệ thống.

Mô hình triển khai cho thiết bị Firewall trung tâm. Firewall sẽ được đặt tại TTĐK, từ cặp switch Layer 3 thực hiện định tuyến lên Firewall, Firewall sẽ kiểm soát luồng thông tin trao đổi giữa các khối trong hệ thống mini SCADA và thực hiện định tuyến lại về cặp switch Layer 3 để tiếp tục đi đến các thành phần đích của hệ thống.

Firewall trung tâm cần có khả năng phân tích gói tin sâu, đảm bảo triển khai các chính sách an ninh ở lớp ứng dụng của các giao thức công nghiệp như: IEC 60870-5-

104, ICCP, Modbus TCP, DNP3, OPC, v.v. Tính năng này cho phép bảo vệ khỏi các kịch bản tấn công giả mạo lệnh điều khiển. Cụ thể, firewall có thể cấu hình ngăn chặn toàn bộ các gói tin Modbus TCP từ máy tính HMI với lệnh Write, do các máy HMI chỉ làm nhiệm vụ đọc dữ liệu từ hệ thống, không cần ghi dữ liệu trở lại. Khi một máy tính HMI xuất hiện một lệnh Write có thể là một rủi ro an ninh, do vậy firewall sẽ chặn các gói tin này đi qua. Các khối trong hệ thống sẽ được phân tách về mặt logic, đảm bảo mọi luồng thông tin giữa các khối đều phải đi qua firewall trung tâm để kiểm tra việc tuân thủ chính sách an ninh, giảm thiểu tối đa rủi ro lây lan tác nhân độc hại ra các phân vùng khác nhau trong hệ thống trong trường hợp một phân vùng bị tấn công

Mô hình tại các TBA



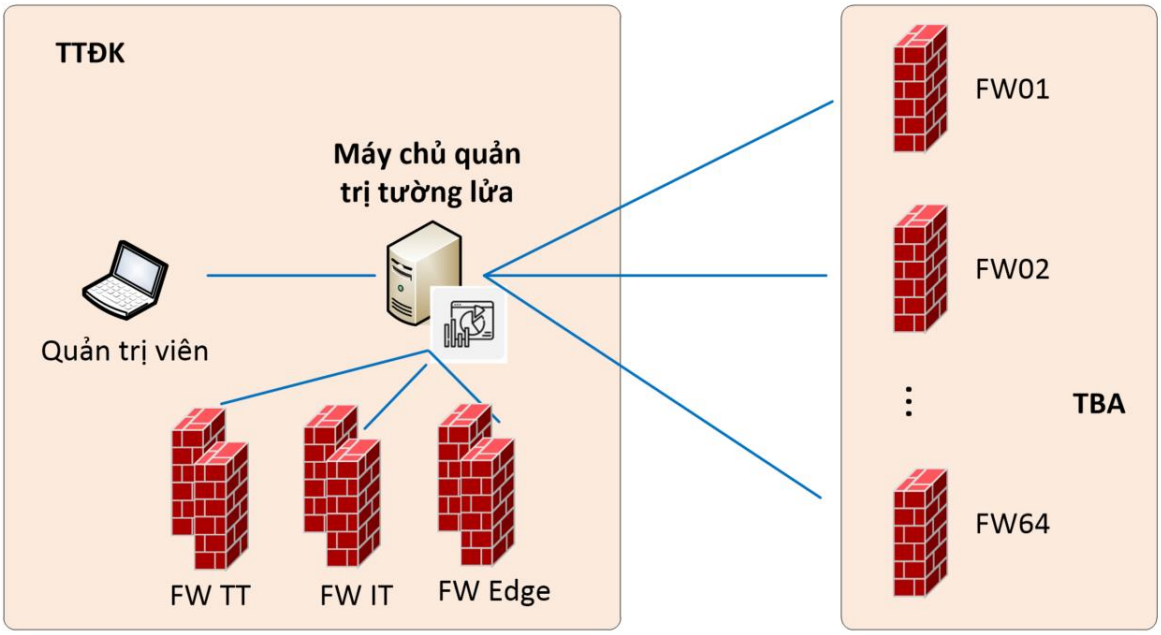
TKTC-BV 16 Mô hình tại các TBA

TBA sẽ được trang bị 01 thiết bị Firewall mới nhằm chia tách vùng mạng, kiểm soát luồng dữ liệu trước khi truyền về TTĐK qua mạng WAN HTĐ. Công nghệ cho các firewall cho các trạm biến áp không người trực được lựa chọn tương tự như firewall trung tâm, tuy nhiên thông số kỹ thuật sẽ được tính toán lại cho phù hợp (thấp hơn). Tại đây, theo QĐ-168 sẽ được thiết kế phân chia thành 03 phân vùng chính:

- Phân vùng Gateway: tại đây sẽ quy hoạch một dải mạng riêng dành cho các máy chủ Gateway trên firewall nhằm mục điểm kiểm soát toàn bộ các lưu lượng kết nối vào ra và áp dụng các tính năng bảo mật nâng cao.
- Phân vùng điều khiển (Controller) chứa các máy chủ HIS, HMI, máy bản ghi sự cố cũng được quy hoạch một dải mạng riêng trên firewall để kiểm soát truy cập và áp dụng các tính năng bảo mật nâng cao.

- Phân vùng trung gian (DMZ) được quy hoạch sẵn một dải mạng riêng trên firewall để phục vụ đặt các máy chủ backup, jump server.. trong tương lai nếu cần.

Thành phần quản trị tường lửa tập trung



TKTC-BV 17 Mô hình quản trị tường lửa tập trung

Toàn bộ các tường lửa tại TTĐK và TBA được quản trị bởi máy chủ quản trị tường lửa tập trung đặt tại trung tâm. Cấu phần này sẽ cung cấp giao diện đồ hoạ cho phép thiết lập thông số, chính sách, theo dõi, quản lý và giám sát tất cả các thiết bị tường lửa còn lại trong mạng. Giải pháp quản lý tập trung sẽ giúp đảm bảo khả năng vận hành, đồng bộ cấu hình, firmware, triển khai chính sách bảo mật, tập luật, báo cáo trên toàn bộ các tường lửa một cách thống nhất, nhanh chóng, hiệu quả.

Do đặc thù hoạt động trong môi trường cách ly khỏi internet, hệ thống quản lý tập trung phải được triển khai dạng vật lý hoặc phần mềm tại Trung tâm Điều khiển, kết nối đến tường lửa tại các chi nhánh thông qua hệ thống mạng WAN.

Các tính năng cần thiết phải có của thành phần quản lý tập trung như sau:

- Phải có khả năng giám sát hiệu năng hoạt động của các thiết bị tường lửa như CPU, thông lượng, số lượng phiên kết nối…
- Phải có khả năng quản lý các thiết bị theo nhóm được phân cấp (ví dụ như cấp Tổng công ty, cấp công ty, ...)
- Phải có khả năng thiết lập các chính sách bảo mật theo mô hình phân cấp (chính sách ở nhóm trên sẽ tự động áp xuống các nhóm ở cấp dưới).
- Phải có khả năng thiết lập cấu hình (cấu hình mạng, cấu hình các thông số của thiết bị) hàng loạt theo các mẫu cấu hình (template)
- Phải có khả năng thực hiện cập nhật hệ điều hành, cập nhật cơ sở dữ liệu phòng chống tấn công (antivirus, IPS) tập trung cho các thiết bị tường lửa thế hệ mới

Máy chủ quản trị được cài đặt dưới dạng máy ảo (VM) trên hạ tầng máy chủ được cung cấp kèm theo dự án.

Phân bổ địa chỉ IP và cổng cho các thiết bị

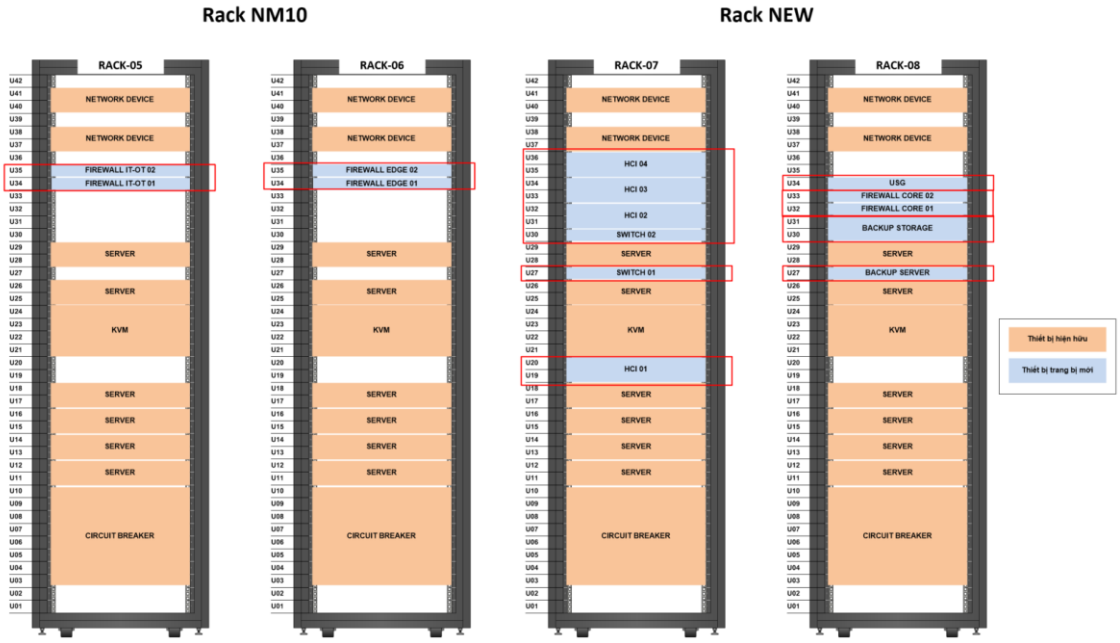
Thiết bị	Cổng	Zone	VLAN	Địa chỉ IP	Ghi chú
TTDK-FW-01	Management	Mgmt	24	10.24. x.x	
TTDK-FW-02	Management	Mgmt	24	10.24. x.x	
TTDK-FW-01 TTDK-FW-02	Ethernet1/1-2	Inside	240	10.240. x.x	Kết nối ra WAN
TTDK-FW-01 TTDK-FW-02	Ethernet1/3-4	Outside	240	10.240. x.x	Kết nối vào core switch

1.5.1.3 Mô hình thiết kế vật lý

Các thiết bị tường lửa sẽ được lắp đặt trên rack tại vị trí như sau:

Rack	U	Tên thiết bị
Rack 08	U32	FIREWALL CORE 01
Rack 08	U33	FIREWALL CORE 02
Rack 05	U34	FIREWALL IT-OT 01
Rack 05	U35	FIREWALL IT-OT 02
Rack 06	U34	FIREWALL EDGE 01
Rack 06	U35	FIREWALL EDGE 02

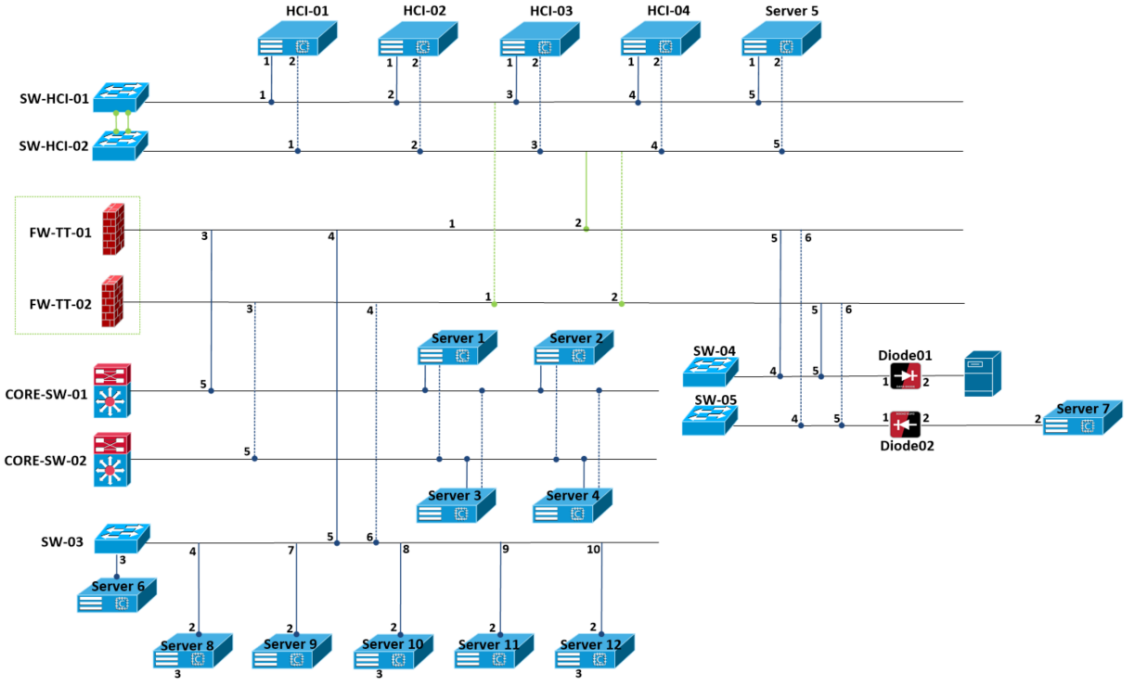
Sơ đồ lắp thiết bị lên tủ rack tại TTĐK như sau:



TKTC-BV 18 Sơ đồ lắp thiết bị lên tủ Rack tại TTĐK

Sơ đồ lắp đặt Firewall tại các TBA: Tham khảo phụ lục 05- Sơ đồ lắp đặt Firewall tại các TBA.

Sơ đồ đấu nối vật lý cho Firewal Trung tâm tại TTĐK:

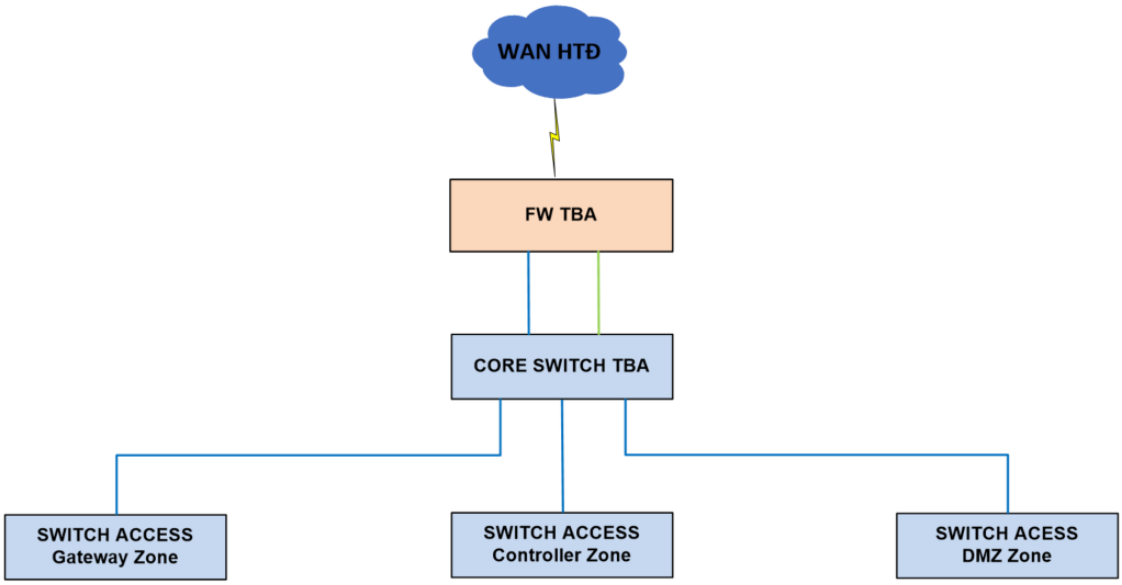


TKTC-BV 19 Sơ đồ đấu nối vật lý cho Firewall tại TTĐK

Mỗi thiết bị tường lửa sử dụng 02 kết nối quang 10Gbps tới hệ thống thiết bị chuyển mạch để phục vụ truyền dữ liệu mạng (data)

Đồng thời, mỗi thiết bị tường lửa sử dụng 01 kết nối đồng 1Gbps tới hệ thống thiết bị chuyển mạch để phục vụ quản trị thiết bị (management)

Sơ đồ đấu nối vật lý cho Firewall tại TBA:



TKTC-BV 20 Sơ đồ đấu nối vật lý cho Firewall tại TBA

Mỗi thiết bị Firewall tại từng Trạm Biến Áp sẽ có 02 kết nối 1Gbps tới hệ thống thiết bị chuyển mạch trung tâm sẵn có tại từng trạm.

Ngoài ra, sẽ sử dụng một đường kết nối đồng 1Gbps kết nối đến đường WAN HTĐ.

Bảng đấu nối vật lý tại TTĐK:

STT	Điểm đầu					Điểm cuối			
	R-U	Thiết bị	Cổng	Cáp	Tốc độ	R-U	Thiết bị	Cổng	Mode
1	R8U32	FW CORE 01	HA1	Quang	10Gbps	R8U33	FW CORE 02	HA1	Auto
2	R8U32	FW CORE 01	HA2	Quang	10Gbps	R8U33	FW CORE 02	HA2	Auto
3	R8U32	FW CORE 01	Eth1	Quang	10Gbps	R7U30	SW02	Eth10	Auto
4	R8U33	FW CORE 01	Eth2	Quang	10Gbps	R7U27	SW03	Eth10	Auto
5	R8U33	FW CORE 01	Eth3	Quang	10Gbps	R7U30	Core SW A	Eth3	Auto
6	R8U32	FW CORE 01	Eth4	Quang	10Gbps	R7U30	Core SW B	Eth3	Auto
7	R8U32	FW CORE 01	MGMT	Đồng	1Gbps	R7U30	SW02	Eth15	Auto
8	R8U33	FW CORE 02	MGMT	Đồng	1Gbps	R7U30	SW02	Eth16	Auto

Bảng đấu nối vật lý tại TBA:

STT	Điểm đầu					Điểm cuối			
	R-U	Thiết bị	Cổng	Cáp	Tốc độ	R-U	Thiết bị	Cổng	Mode
1		FW TBA	Eth1	Đồng	1Gbps		SW WAN HTĐ	Eth24	Auto
2		FW TBA	Eth2	Quang	10Gbps		SW CORE TBA	Eth23	Auto
3		FW TBA	Eth3	Quang	10Gbps		SW CORE TBA	Eth24	Auto

1.5.1.4 Phân bổ tài nguyên ảo hoá

Máy chủ quản trị tập trung của hệ thống yêu cầu tài nguyên như sau:

Thông số	**Giá trị**	**Ghi chú**
CPU	32 Core	
RAM	128GB RAM	
HDD	3 TB	

1.5.1.5 Thông số cài đặt và cấu hình

Thông tin cấu hình	**Giá trị**
Thông số chung	
Domain	evnhanoi.vn
Syslog	yy.yy.253.61
NTP	10.240. x.x 10.240. x.x 10.240. x.x
FW01	
Hostname	Ttđk-fw01.evnhanoi.vn
Ethernet Port	mgmt
IP Address / Subnet mask	10.24. x.x /24
Gateway	10.24.x.1
Service/port	443
Appliance Management/Port	443
FW02	
Hostname	Ttđk-fw02.evnhanoi.vn
Ethernet Port	mgmt
IP Address / Subnet mask	10.24. x.x /24
Gateway	10.24.x.1
Service/port	443
Appliance Management/Port	443

Thông số dự phòng:©

Thông tin cấu hình	**Giá trị**
Setup	Group ID: 1 Mode: Active/Passive Peer HA1 IP Address: 1.1.1.2 Backup Peer HA1 IP Address: yy.yy.253.11
Active/Passive Settings	Passive Link State: auto Monitor Fail Hold Down time: 1
Election Settings	Preemtive: Yes Heartbeat Backup: No
Control Link	HA1 + Port: dedicated-ha1 + Ipv4 Address: 1.1.1.1

Thông tin cấu hình	Giá trị
	+ Monitor Hold Time (ms): 3000 HA1 Backup + Port: management
Data Link	HA2 + Port: dedicated-ha2 + IP/Netmask: 10.10.10.1/30 + Transport: ethernet + Action: log-only + Threshold: 10000ms

Thông số định tuyến:

Virtual Router	Interface	Destination	Gateway	Ghi chú
Default	Ethernet1/1-2	10.18.240.0/24 10.19.240.0/24 10.20.240.0/24 10.21.240.0/24 10.22.240.0/24	10.240.40.x	To Firewall
Default	Ethernet1/3-4	0.0.0.0/0	10.240.40.x	To Router

1.5.1.6 Chính sách an ninh

STT	Name	Source Zone	Source Address	Source User	Dest Zone	Dest Address	Dest User	Service	Action	Option
1	SIEM	Inside	Any	Any	Inside	SIEM Server	Any	UDP/514 TCP/8413	Allow	Log
2	EPS	Inside Ouside	Any	Any	Inside	EPS Server	Any	TCP 80, 8014, 443, 2967	Allow	Log
3	PIM/PAM	Inside Ouside	Any	Any	Inside	PIM/PAM Server	Any	TCP/443	Allow	Log
4	2FA	Inside Outside	Any	Any	Inside	2FA Server	Any	UDP1812/1813	Allow	Log
	…									
-	Implicit deny	-	-	-	-	-	-	-	Deny	

1.5.1.7 Chỉ dẫn biện pháp triển khai

Chi tiết về cách thức thực hiện được thể hiện ở phụ lục 2 "Chỉ dẫn triển khai chi tiết"

1.5.1.8 Kết quả đạt được sau khi hệ thống đi vào hoạt động

Việc đầu tư và triển khai hệ thống Tường lửa thế hệ mới cho TTĐK và các TBA mang lại các kết quả tích cực cho EVNHN bao gồm:

- **Tăng cường bảo mật mạng**: NGFW cung cấp các lớp bảo vệ tiên tiến như phát hiện và ngăn chặn xâm nhập (IDS/IPS), lọc nội dung và kiểm soát ứng dụng. Điều này giúp ngăn chặn các mối đe dọa tinh vi và bảo vệ dữ liệu quan trọng.
- **Quản lý dễ dàng hơn**: NGFW tích hợp nhiều chức năng bảo mật trong một thiết bị duy nhất, giúp giảm bớt sự phức tạp trong quản lý và triển khai. Giao diện quản lý thân thiện và các công cụ báo cáo chi tiết giúp quản lý dễ dàng hơn.
- **Hiệu suất cao hơn**: Các hệ thống NGFW thường được thiết kế với phần cứng mạnh mẽ và tối ưu hóa phần mềm để xử lý lưu lượng mạng lớn mà không làm giảm hiệu suất.
- **Giảm thiểu rủi ro an ninh mạng**: Với khả năng phân tích và ngăn chặn các cuộc tấn công theo thời gian thực, NGFW giúp giảm thiểu nguy cơ bị tấn công mạng và bảo vệ hệ thống khỏi các cuộc tấn công tiềm ẩn.
- **Tuân thủ quy định**: NGFW giúp tổ chức tuân thủ các quy định và tiêu chuẩn an ninh mạng bằng cách cung cấp các công cụ kiểm soát và báo cáo chi tiết, đáp ứng yêu cầu của các quy định pháp lý và tiêu chuẩn ngành điện.

1.5.1.9 Tính toán thông số kỹ thuật

1.5.1.9.1 Tính toán thông số kỹ thuật cho Firewall tại TTĐK

Để đáp ứng các yêu cầu từ những mối đe dọa mới trên thực tế, các hãng bảo mật mạng đã đưa ra và khuyến cáo sử dụng thông số Threat Prevention Throughput (App, IPS, AV, Antispyware, Sandbox, DNS, File, Log) trong việc lựa chọn năng lực thiết bị tường lửa thế hệ mới thay vì dựa vào các thông số truyền thống như IPS, thông lượng lớp 4.

Để lựa đưa ra lựa chọn các thông số hợp lý, các yếu tố như hiệu năng và thông số giới hạn của các thiết bị đang hoạt động trong môi trường thực tế, kế hoạch tăng trưởng trong tương lai sẽ được sử dụng là dữ liệu đầu vào để phục vụ tính toán đưa ra yêu cầu về năng lực của thiết bị tương lai:

Một số thông tin về hiện trạng băng thông sử dụng như sau:

- Thông lượng được đo tại kết nối đầu vào từ phía 02 thiết bị router tại Trung tâm Điều khiển ~ 2 Mega bytes/giây = 16 Mbps (thông lượng cho từng kênh cụ thể được thể hiện trong *Bảng 3*).
- Dự kiến tăng trưởng số lượng thiết bị trong thời gian tới tại TTĐK.
- Số lượng máy chủ tăng lên 22.
- Số lượng máy trạm tăng lên 50.

Bảng 1: Thông lượng sử dụng thực tế tại TTĐK.

TÊN DỊCH VỤ	THÔNG LƯỢNG THEO KÊNH (BPS)	THÔNG LƯỢNG TỔNG (BPS)
Đi các đơn vị	32.157	1.959.256
Fault Recoder	1.848.438	
Hotline	2.315	
SCADA1	76.269	
SCADA2	77	

Dựa theo các yếu tố trên, năng lực của thiết bị của thiết bị tường lửa thế hệ mới cần đạt yêu cầu như sau:

- Mặc dù thông lượng hiện tại truyền tải về TTĐK tương đối thấp (chỉ 16 Mbps) tại thời điểm đo. Tuy nhiên hạ tầng các đường truyền, cổng kết nối tại TTĐK đều đạt tối thiểu 1Gbps. Do đó để đảm bảo khả năng mở rộng trong tương lai, các dịch vụ mới được phát triển thêm và không trở thành điểm tắc nghẽn của hệ thống, các thiết bị bảo mật như tường lửa thế hệ mới cũng nên có năng lực xử lý tối thiểu 10 Gbps khi bật đầy đủ mọi tính năng. (đảm bảo khi chạy full tải, thiết bị không bị treo hay ảnh hưởng đến hoạt động sản xuất kinh doanh)
- Do đó thông thông lượng Threat Prevention (Khi bật mọi tính năng bảo mật trên tường lửa như IPS, Antivirus, Application control…) đạt tối thiểu 10 Gbps
- Thông lượng IPSEC VPN cũng phải xấp xỉ thông lượng Threat Prevention: IPSEC VPN Throughput = 10 Gbps để đảm bảo khả năng xử lý khi thực hiện các kết nối mã hoá giữa các TBA hay trung tâm ĐH.
- Có khả năng nhận dạng và kiểm soát các luồng kết nối bằng các chính sách dựa trên ứng dụng, người dùng và nội dung.
- Tường lửa phải có khả năng nhận dạng và kiểm soát các ứng dụng ICS/SCADA ngay cả khi các license hết hạn (không được mua bản quyền hỗ trợ từ nhà cung cấp)
- Có khả năng ngăn chặn các tấn công khai thác lỗ hổng của các thành phần như HMIs, SCADA Master, Historians
- Có khả năng ngăn chặn các tấn công khai thác lỗ hổng của các ứng dụng như Mobus, DNP3, ICCP.
- Thiết bị phải có khả năng triển khai ở nhiều chế độ khác nhau như L2, L3, tap, virtual wire (transparent mode) để đảm bảo mức độ linh hoạt và đáp ứng các nhu cầu phát sinh trong thực tế.

1.5.1.9.2 Tính toán thông số kỹ thuật cho Firewall tại các TBA

Khi tính toán dự phòng để trang bị năng lực sẵn sàng cao (HA – High Availability) cho hệ thống firewall, có 2 phương án điển hình để thực hiện điều này:

- Phương án 1: Mỗi đơn vị được trang bị 01 cặp firewall cấu hình chạy HA cho nhau. Đây là phương án lý tưởng để đảm bảo tính liên tục, tuy nhiên đòi hỏi chi phí quá cao.
- Phương án 2: Dự phòng theo tỷ lệ. Thông thường, thiết bị phần cứng như firewall có xác suất gặp sự cố nhất định và xác suất này ngày càng được duy trì thấp do sự phát

triển của khoa học kỹ thuật. Do đó phương án dự phòng tiết kiệm, hợp lý hơn là duy trì một tỷ lệ phần trăm thiết bị dự phòng để có thể thay thế ngay lập tức khi có thiết bị trong hệ thống đang sử dụng gặp sự cố. Trong trường hợp EVNHANOI với 60 trạm biến áp không người trực, chúng tôi đề xuất tỷ lệ này là 10%, tương ứng với 66 thiết bị firewall. Theo khảo sát hoạt động thực tế tại trạm biến áp 110kV Dương Nội trên các kênh dịch vụ: "hotline", "fault recoder", "to gateway A1 11 Cbac", "to gateway X2", "to backup A1 18TNH"; Tại trạm biến áp 220kV Tây Hồ trên các kênh dịch vụ: "hotline", "fault recoder", "Scada". Kết quả thông lượng truyền tải các tín hiệu điều khiển tại các TBA là khá nhỏ, chỉ < **1 Mbps.** Tuy nhiên hạ tầng mạng của các TBA đều sử dụng các cổng mạng có tốc độ kết nối thông thường là 100 Mbps.

Do đó để đảm bảo khả năng mở rộng trong tương lai, cũng như đảm bảo thiết bị tường lửa không trở thành điểm tắc nghẽn trong hệ thống mạng, thông lượng xử lý của các thiết bị NGFW tại TBA phải đạt tối thiểu 200 Mbps để đảm bảo ngay cả khi hệ thống đạt ngưỡng 100 Mbps, thiết bị tường lửa cũng không bị treo gây ảnh hưởng đến hoạt động sản xuất kinh doanh.

Bảng 2: Thông lượng thực tế các kênh dịch vụ tại trạm biến áp.

TÊN TRẠM	KÊNH DỊCH VỤ	THÔNG LƯỢNG THỰC TẾ SỬ DỤNG
Trạm 110 E1.61	Hotline	0 bits/sec
	Fault Recoder	0 bits/sec
	To Gateway A1 Cua Bac	10000 bits/sec
	To Gateway X2	11000 bits/sec
	To A1 backup 18 TNH	0 bits/sec

Dựa trên các yếu tố trên, năng lực của thiết bị tường lửa thế hệ mới NGFW cho các TBA được đề xuất như sau:

- Thông số thông lượng kiểm soát ứng dụng App-ID ≥ 400Mbps.
- Thông số thông lượng Threat Prevention (Khi bật mọi tính năng bảo mật trên tường lửa như IPS, Antivirus, Application control…) ≥ 400 Mbps.
- Thông lượng IPSEC VPN ≥ 400 Mbps.

1.5.1.9.3 Tính toán thông số kỹ thuật cho giải pháp quản trị Firewall tập trung

Giải pháp quản trị Firewall tập trung yêu cầu 01 máy chủ cài đặt phần mềm quản trị với cấu hình tối thiểu như sau:

STT	Máy chủ	Yêu cầu	Số lượng
1	Máy chủ quản lý tập trung	32 Core	1
		128GB RAM	
		3 TB	

Dự phòng cho thành phần quản lý tập trung:

- Sử dụng máy ảo để cài đặt thành phần quản lý tập trung.

- Khả năng dự phòng của máy ảo sẽ dùng trên giải pháp ảo hóa bao gồm tính năng High Availability (cho phép máy ảo tự động khởi động trên một máy chủ vật lý khác khi máy chủ vật lý gốc bị lỗi).
- Khả năng dự phòng về lưu trữ: theo khả năng dự phòng của giải pháp ảo hóa, có các cơ chế RAID cho phép lỗi 01 ổ cứng đồng thời hoặc 01 node đồng thời (mô hình HCI) mà không ảnh hưởng tới dữ liệu và dịch vụ đang chạy.

1.5.1.10Thông số cấu hình thiết bị yêu cầu

Thiết kế thông số thiết bị theo yêu cầu:

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
I	**Firewall tại TTĐK**		**02**
1	Thông lượng khi bật các tính năng phòng chống tấn công Threat Prevention (Application, IPS, Antivirus, Antispyware, File blocking, DNS security, logging)	≥ 10 Gbps	
2	Thông lượng Next Generation Firewall/ tường lửa ứng dụng	≥ 10 Gbps	
3	Thông lượng IPSEC	≥ 10 Gbps	
4	Số lượng VLAN hỗ trợ	≥ 3000	
5	Số security zone	≥ 200	
6	Cổng kết nối dữ liệu (Có sẵn trên thiết bị)	≥ 02 cổng 1G RJ45 + 01 cổng 10G SFP+ dành riêng cho cấu hình HA	
		≥ 04 cổng 1GbE RJ45	
		≥ 04 cổng quang 1GbE/10GE SFP	
7	Cổng quản trị thiết bị	≥ 1 RJ45 Mgmt	
8	Giao diện quản trị	Web, CLI, API/REST API	
9	Tính năng HA	Active/active, Active/passive	
10	Hỗ trợ các giao thức định tuyến	OSPF, BGP, RIP, PIM (SM , SSM), IGMP	
11	Đảm bảo khả năng kiểm soát và nhận dạng các ứng dụng ICS/SCADA như sau:	Modbus, IEC-60870-5-104, IEC 60870-6 (ICCP), OPC DA & UA, DNP3, IEC 61850; BACnet, ABB Network Manager, ABB-RP570, ICCP, IP EtherNet, IP MTConnect, Cygnet SCADA, R-GOOSE, CIP EtherNet IP, Profinet, Schneider OASyS, Schneider Wonderware Suitelink, Schweitzer Engineering SEL Fast Messaging, Siemens FactoryLink, Siemens Profinet IO, Siemens-P2, Siemens S7, Siemens	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
		S7-Comm-Plus, DLMS, GE-Historian, GE-Eterra-SCADA.	
12	Tính năng bảo mật	- Có sẵn các tính năng dưới đây hoặc tương đương Stateful firewall , , IPSec VPN, Application Control, IPS, Antivirus	
		- Trên một chính sách bảo mật có thể thiết lập theo các thành tố như ứng dụng, người dùng, device, zone và bật các tính năng antivirus, ips, antispyware, lọc file.	
		- Có nhiều cơ chế định danh người dùng như Server monitoring, Port mapping, syslog, XFF Header, Username Header Insertion, Authentication policy, XML API, Client probing	
13	Tính năng ngăn chặn tấn công	Phát hiện và ngăn chặn các kết nối C2C, sử dụng DNS sinkholing để xác định các máy bị lây nhiễm	
		Phát hiện và ngăn chặn các loại mã độc, các tấn công khai thác lỗ hổng bảo mật	
14	Bản quyền sử dụng các tính năng bảo mật có sẵn	≥ 24 tháng	
15	Nguồn điện	Đảm bảo 02 nguồn dự phòng, điện áp 220VAC	
16	Bảo hành và hỗ trợ kỹ thuật	≥ 24 tháng	
II	**Firewall tại các TBA**		**66**
1	Thông lượng Threat Prevention (Application, IPS, Antivirus, Antispyware, File blocking, DNS security, logging)	≥ 400 Mbps	
2	Thông lượng Next Generation Firewall/tường lửa ứng dụng	≥ 400 Mbps	
3	Thông lượng IPSEC VPN	≥ 400 Mbps	
4	Số lượng VLAN hỗ trợ	≥ 3000	
5	Số security zone	≥ 50	
6	Cổng kết nối dữ liệu (Có sẵn trên thiết bị)	≥ 08 cổng 1GE RJ-45	
7	Cổng quản trị thiết bị	≥ 1 RJ45 Mgmt	
8	Giao diện quản trị	Web, CLI	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
9	Tính năng HA	Active/active, Active/passive	
10	Hỗ trợ các phương thức định tuyến	OSPF, BGP, RIP, PIM (SM, SSM), IGMP	
11	Đảm bảo khả năng kiểm soát và nhận dạng các ứng dụng ICS/SCADA như sau:	Modbus, IEC-60870-5-104, IEC 60870-6 (ICCP), OPC DA & UA, DNP3, IEC 61850; BACnet, ABB Network Manager, ABB-RP570, ICCP, IP EtherNet, IP MTConnect, Cygnet SCADA, R-GOOSE, CIP EtherNet IP, Profinet, Schneider OASyS, Schneider Wonderware Suitelink, Schweitzer Engineering SEL Fast Messaging, Siemens FactoryLink, Siemens Profinet IO, Siemens-P2, Siemens S7, Siemens S7-Comm-Plus, DLMS, GE-Historian, GE-Eterra-SCADA.	
12	Tính năng bảo mật	- Có sẵn các tính năng dưới đây hoặc tương đương Stateful firewall , IPSec VPN, Application Control, IPS, Antivirus	
		- Trên một chính sách bảo mật có thể thiết lập theo các thành tố như ứng dụng, người dùng, device, zone và bật các tính năng antivirus, ips, antispyware, lọc file.	
		- Có nhiều cơ chế định danh người dùng như Server monitoring, Port mapping, syslog, XFF Header, Username Header Insertion, Authentication policy, XML API, Client probing	
13	Tính năng ngăn chặn tấn công	Phát hiện và ngăn chặn các kết nối C2C, sử dụng DNS sinkholing để xác định các máy bị lây nhiễm	
		Phát hiện và ngăn chặn các loại mã độc, các tấn công khai thác lỗ hổng bảo mật	
14	Bản quyền sử dụng các tính năng bảo mật có sẵn	≥ 24 tháng	
15	Nguồn điện	Đảm bảo 02 nguồn dự phòng, điện áp 220VAC	
16	Bảo hành và hỗ trợ kỹ thuật	≥ 24 tháng	
III	**Giải pháp quản lý tường lửa tập trung**		**01**
1	Bản quyền phần mềm	Theo số lượng tường lửa thực tế	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
2	Tương thích với thiết bị tường lửa	Phần mềm quản lý tường lửa tập trung phải cùng hãng sản xuất và hoàn toàn tương thích với thiết bị tường lửa cung cấp ở trên	
3	Khả năng mở rộng số lượng thiết bị quản lý	≥ 1000	
4	Giao diện quản trị	Giao diện Web/ CLI / API	
5	Môi trường triển khai	Một trong các môi trường ảo hoá sau: VMware ESXi, KVM, và Microsoft Hyper-V	
6	Quản lý tập trung	- Có khả năng quản trị tập trung cấu hình chính sách các tường lửa	
		- Có khả năng quản lý hệ điều hành của các thiết bị - centralized device software installation.	
		- Quản lý chính sách theo nhóm thiết bị, mô hình phân cấp	
		- Tích hợp đồng thời cả tính năng quản trị cấu hình và quản lý tập trung log	
7	Tính năng quản trị network	Tự động hóa (Automation): - Có cơ chế tự động triển khai nhanh hoặc cùng lúc nhiều thiết bị	
		Phân tích (analyze) - Có khả năng giám sát hiệu năng của các thiết bị, giám sát các vấn đề về hiệu năng	
		- Có khả năng giám sát tốc độ kết của các thiết bị tường lửa	
8	Tính năng quản trị thiết bị firewall	Tạo và quản lý tập trung các chính sách bảo mật thông qua một giao diện duy nhất. Quản trị tập trung với duy nhất một giao diện console cho tất cả các tính năng bảo mật như Firewall, VPN, IPS, Application Control.	
		Hiển thị số lần truy cập thông qua policy theo thời gian thực.	
		Có khả năng thiết lập tự động tag người dùng, địa chỉ IP theo các điều kiện lọc log ngay trên thiết bị, có thể tự động đưa người dùng, IP vào danh sách nhóm chặn khi phát sinh các rủi ro.	
		Có khả năng tự động phân tích các sự kiện trong hệ thống mạng để xác định các đối tượng bị thoả hiệp trong hệ thống mạng.	
		Hiển thị nơi các mối đe dọa bắt nguồn.	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
		Có tính năng chuyển đổi các signature của Snort và Suricata signature sang signature cho tường lửa	
		Thiết bị quản lý tập trung có khả năng phân phối lại các thông tin như IP User Mappings, IP Tags, User Tags, Quarantine List đến các tường lửa được quản lý	
		Giám sát sức khoẻ của firewall: - Sử dụng CPU - Sử dụng bộ nhớ	
		Sytem logs được chuyển tiếp đến thông tin bảo mật và quản lý sự kiện (SIEM).	
9	Báo cáo và cảnh báo	Các báo cáo được tạo ra và được gửi tự động qua e-mail	
		Có khả năng tuỳ biến các báo cáo	
10	Bảo hành và hỗ trợ với phần mềm	≥ 24 tháng	

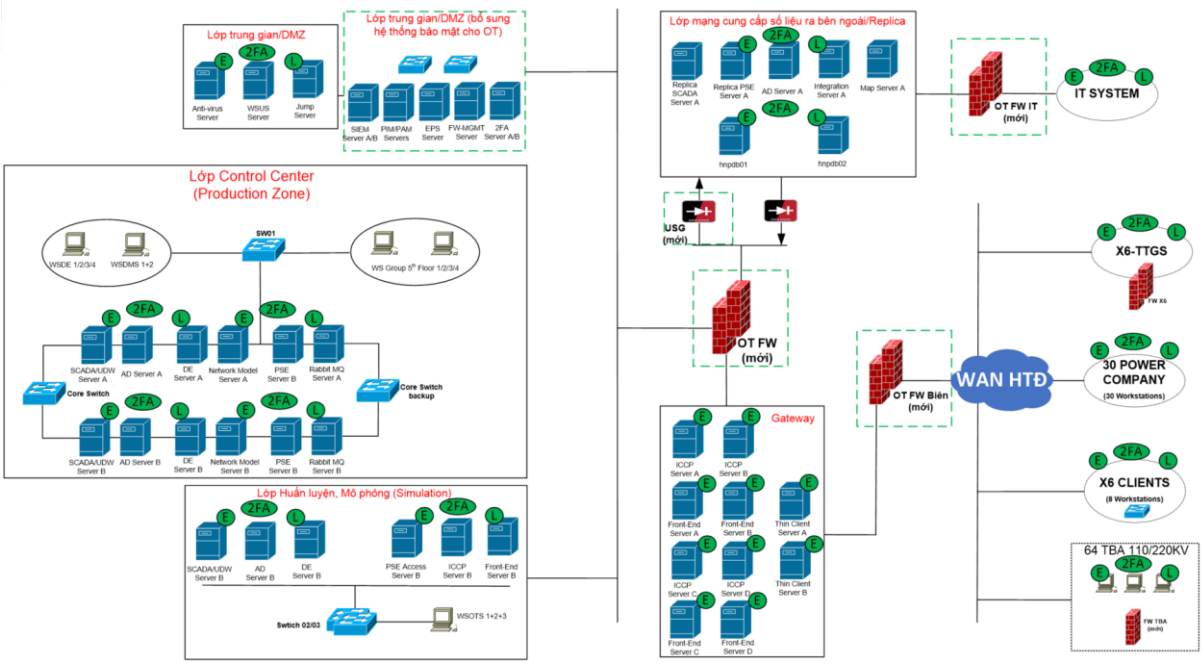
1.5.2 Hệ thống cổng một chiều

1.5.2.1 Danh mục thiết bị lắp đặt, cài đặt

STT	TÊN HẠNG MỤC	SỐ LƯỢNG
IV	Giải pháp cổng một chiều (USG/Datadiode)	01

1.5.2.2 Mô hình thiết kế luận lý

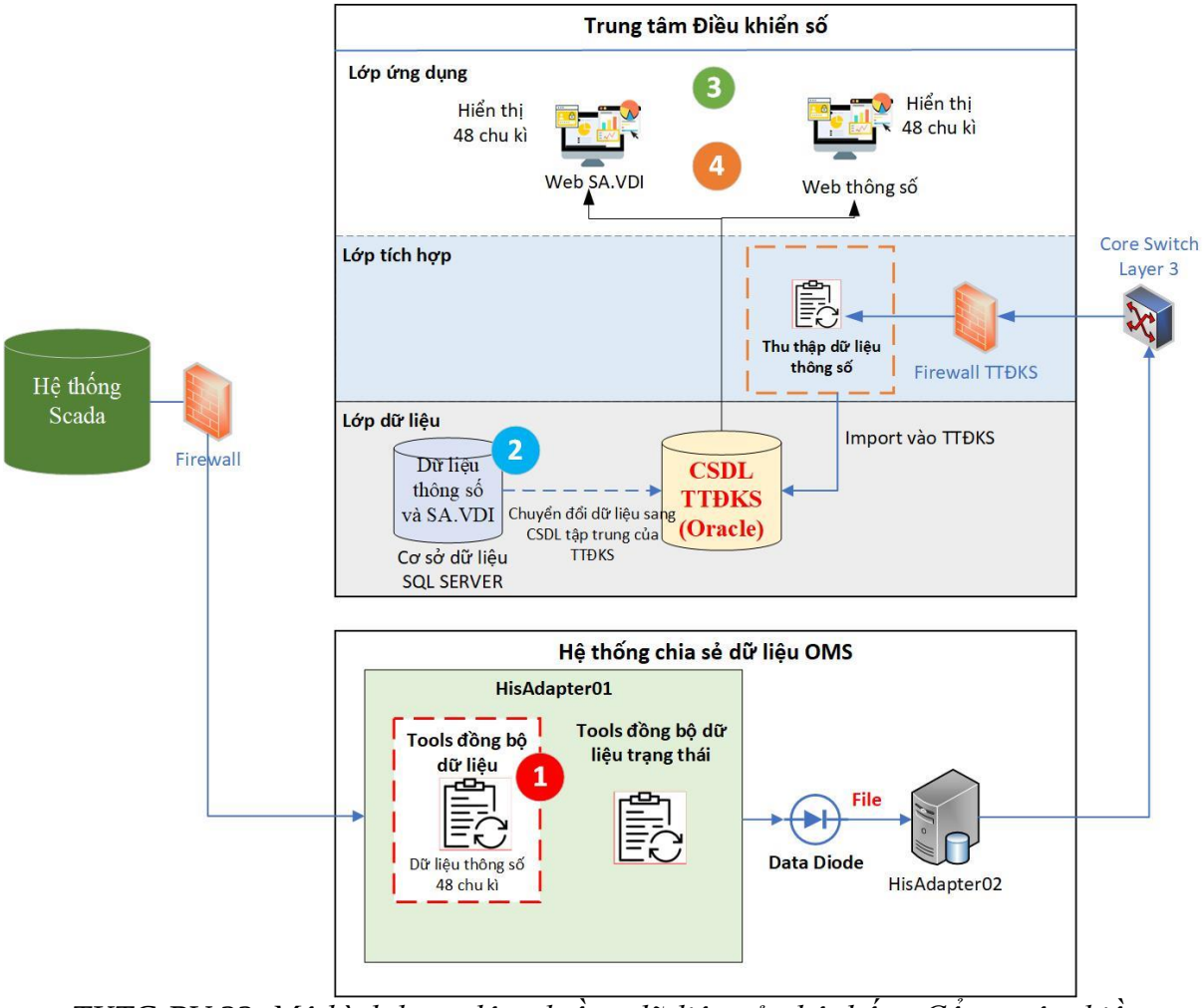
Dưới đây là mô hình thiết kế luận lý cho hệ thống Cổng bảo mật một chiều tại TTĐK:



TKTC-BV 21 Mô hình thiết kế luận lý cho hệ thống Cổng bảo mật một chiều tại TTĐK

Tích hợp hệ thống Điều khiển trung tâm: để thu thập thông tin dữ liệu thông số, cảnh báo, thao tác xa từ hệ thống Scada (thông qua HisAdapter2 của hệ thống chuyển đổi dữ liệu từ Hệ thống điều khiển trung tâm sang Hệ thống OMS). Dữ liệu thu thập sẽ phục vụ xây dựng hệ thống quản lý thông số, SA.VDI, cung cấp thông tin sự cố lưới điện thời gian thực cho ca trực điều độ.

Mô hình hoạt động luồng dữ liệu được mô tả như hình sau:



TKTC-BV 22 Mô hình hoạt động luồng dữ liệu của hệ thống Cổng một chiều

- Mục đích:
  - Thu thập dữ liệu từ hệ thống Điều khiển trung tâm. Các dữ liệu thu thập bao gồm
    - Các dữ liệu về sự cố
    - Các dữ liệu về thao tác điều khiển xa
    - Các dữ liệu về thống số vận hành (48 chu kì)
- Tần suất: định kì

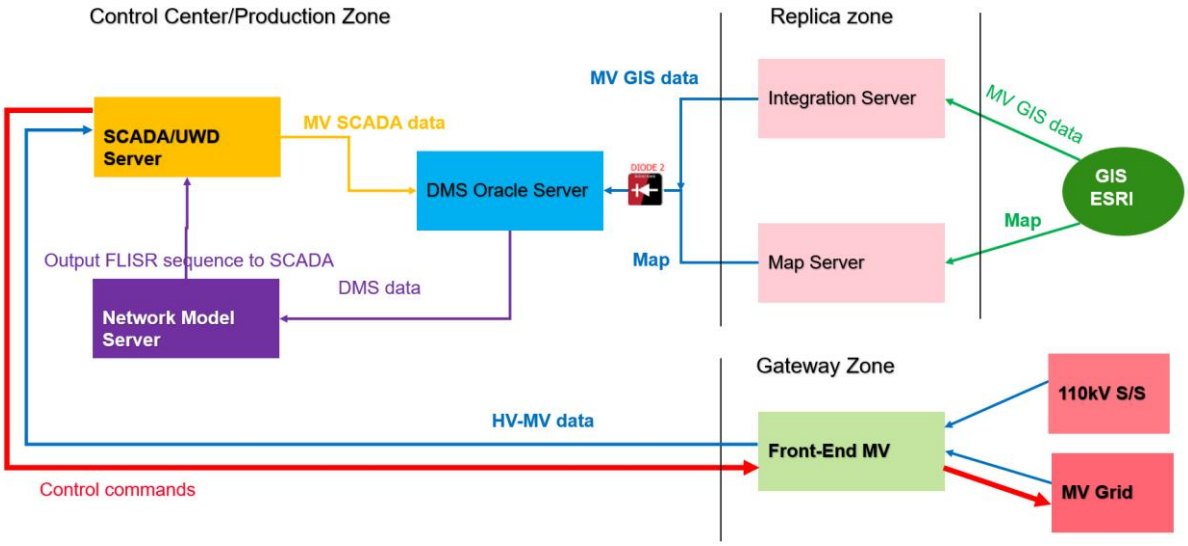
- Phương thức: chia sẻ file. Trong đó TTĐKS sẽ thực hiện thu thập các file từ HisAdapter2 về kho dữ liệu tập trung của TTĐKS.

Máy chủ Adapter 01 được cấu hình với chức năng chia sử file dữ liệu từ hệ thống OT sang TI, đồng thời thực hiện lưu trữ các bản vá phục vụ cập nhật Windows từ hệ thống IT.

Máy chủ Adapter 02 kết nối trực tiếp với hệ thống OMS trong mạng IT.

- Thiết bị cổng một chiều từ IT sang OT (DataDiode 02) phục vụ công tác cập nhật:
  - Cập nhật bản vá Windows.
  - Cập nhật phần mềm Antivirus Symantec.
  - Cập nhật firmware (nếu có).
  - File dữ liệu phục vụ vận hành đảm bảo ATTT.
  - File dữ liệu MV từ hệ thống GIS
  - File dữ liệu map từ hệ thống ESRI

Mô hình hoạt động luồng dữ liệu được mô tả như sau:



Cổng bảo mật một chiều (USG/Datadiode) giúp đảm bảo về mặt vật lý luôn luôn chỉ cho phép dữ liệu truyền một chiều từ mạng IT (Corporate Network) về mạng IT (Industrial network), mà không cho truyền dữ liệu hoặc điều khiển từ chiều ngược lại.

Giải pháp hỗ trợ các giao thức:

- CSDL như MSSQL, MySQL, Oracle: thông qua cơ chế truyền file hoặc data stream
- IEC 60870-5-104
- Các giao thức truyền file như FTP, FTPS, SFTP, TFTP, SMB

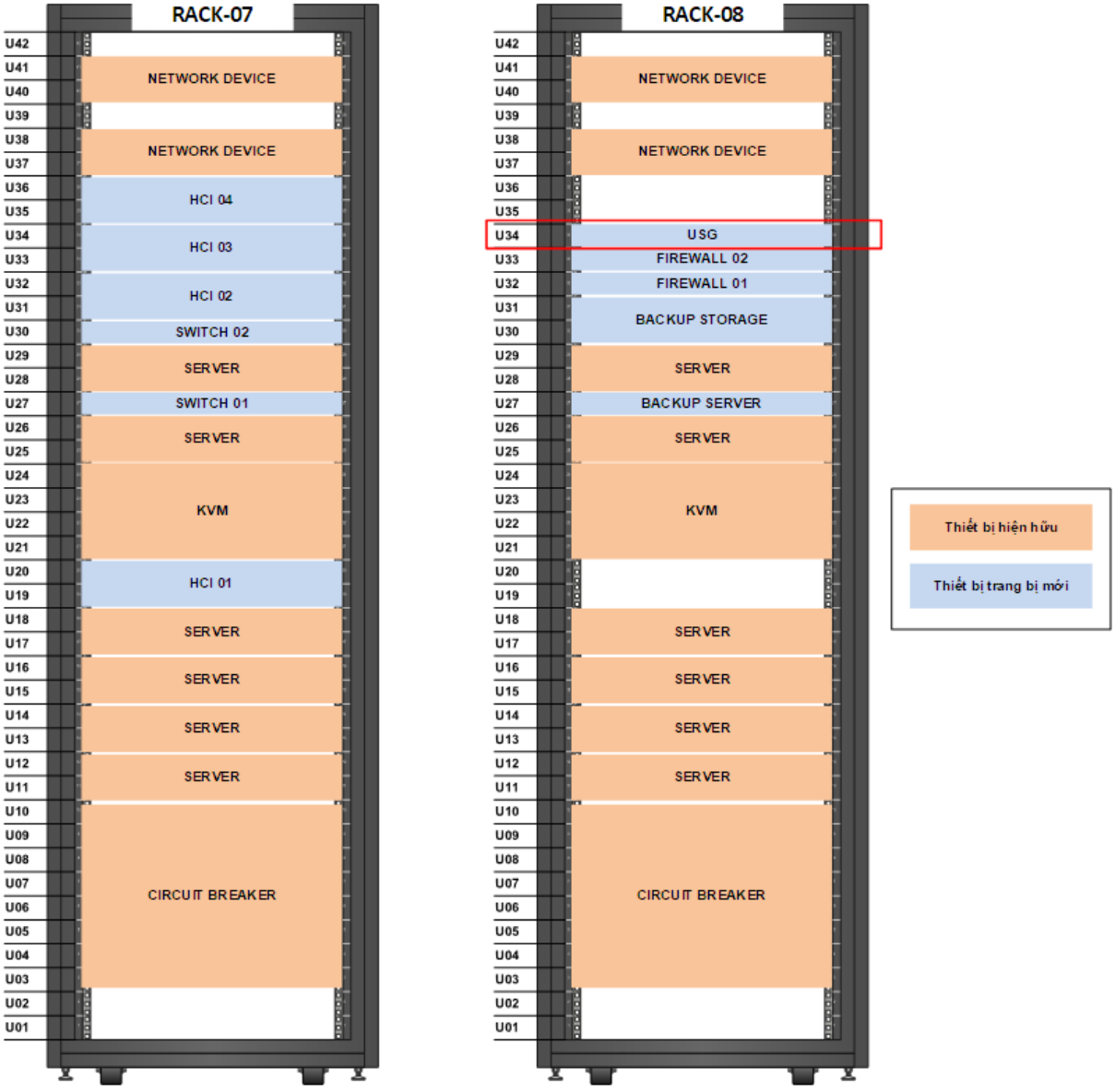
Trong dự án này, sẽ thực hiện đầu tư bổ sung 01 thiết bị cổng 1 chiều mới để thay thế cho thiết bị DataDiode 02 đang hiện hữu với hiệu năng thấp (thông lượng 200Mbps) để đảm bảo hiệu năng cho hệ thống hiện tại và tương lai với việc ngày càng cần chi sẻ nhiều dữ liệu sang Kho Dữ liệu tập trung công tác QLKT của EVNHN.

1.5.2.3 Mô hình thiết kế vật lý

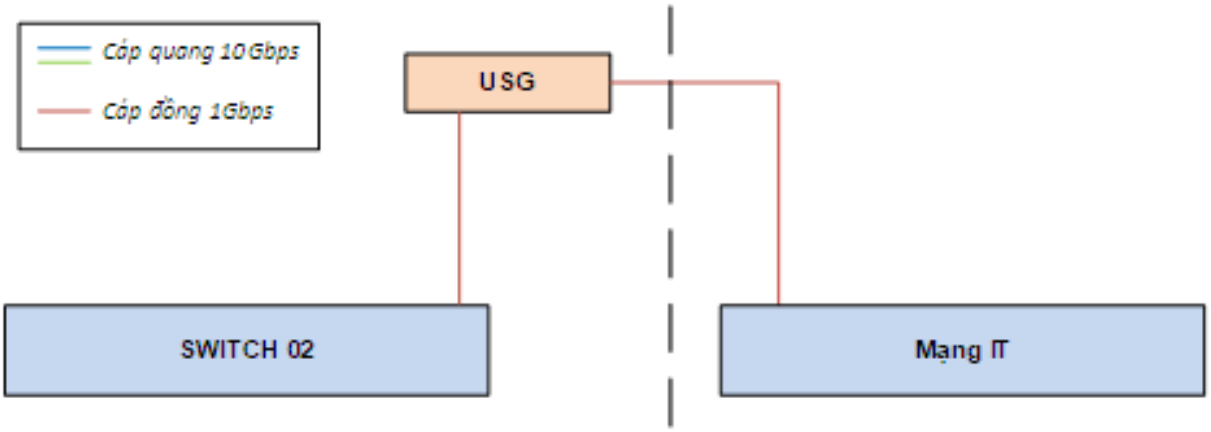
Thiết bị cổng một chiều sẽ được lắp đặt trên rack tại vị trí như sau:

Rack	U	Tên thiết bị
Rack 07	U34	USG

Sơ đồ lắp rack như sau:



Sơ đồ đấu nối vật lý



Thiết bị cổng một chiều sử dụng 01 kết nối đồng 1Gbps tới hệ thống thiết bị chuyển mạch của mạng OT và IT để phục vụ truyền dữ liệu mạng (data)

Bảng đấu nối vật lý:

STT	Điểm đầu					Điểm cuối				Ghi chú
	R-U	Thiết bị	Cổng	Cáp	Tốc độ	R-U	Thiết bị	Cổng	Mode	
1	R8U34	USG-RED	LAN1	Đồng	1G	Switch IT	Switch IT	Ethx	Auto	
2	R8U34	USG-BLUE	LAN1	Đồng	1G	R7U30	Switch 02	Eth19	Auto	
3	R8U34	USG-RED	SFPTX	Quang	1G	R8U34	USG-BLUE	SFPRX	Auto	
4	R8U34	USG-BLUE	SFPTX	Quang	1G	R8U34	USG-RED	SFPRX	Auto	

1.5.2.4 Thông số cài đặt và cấu hình

Thông số FTP

Thông số	Giá trị	Ghi chú
USG-RED (IT)		
User	ftpuser	
Password		
Server	(IP)	
Share	/	Thư mục chứa file nhận về
Enabled	Yes	
Delete Files on Share after transfer	No	
USG-BLUE (OT)		
User	ftpuser	
Password		
Server	(IP)	
Share	/	Thư mục chứa file gửi đi
Enabled	Yes	
Delete Files on Share after transfer	No	

Thông số SFTP

Thông số	Giá trị	Ghi chú
USG-RED (IT)		
User	sftpuser	
Auth	Password	
Password		
Server	(IP)	
Port	22	
Share Path	/	Thư mục chứa file nhận về
Enabled	Yes	
Delete Files on Share after transfer	No	
USG-BLUE (OT)		
User	sftpuser	
Auth	Password	
Password		
Server	(IP)	
Port	22	
Share Path	/	Thư mục chứa file gửi đi
Enabled	Yes	

Thông số	Giá trị	Ghi chú
Delete Files on Share after transfer	No	

Thông số Windows File Share

Thông số	Giá trị	Ghi chú
USG-RED (IT)		
User	windowsuser	
Password		
Server	(IP)	
Share	(folder name)	Thư mục chứa file nhận về
Enabled	Yes	
USG-BLUE (OT)		
User	windowsuser	
Password		
Server	(IP)	
Port	22	
Share	(folder name)	Thư mục chứa file gửi đi
Enabled	Yes	

Thông số TCP/UDP stream

Thông số	Giá trị	Ghi chú
USG-RED (IT)		
Channel	1	Cần khớp với BLUE
Type	Unilateral	
Name	TCP01	
Protocol	TCP	
Destination port	(port)	
Destination address	(IP)	
Enabled	Yes	
Terminate on Failure	No	
Max Buffer Items	10	
USG-BLUE (OT)		
Channel	1	Cần khớp với RED
Type	Unilateral	
Name	TCP01	
Protocol	TCP	
Source port	(port)	
Source address	(IP)	
Enabled	Yes	
Max Session	100	
Bitrate	100 Mb/s	

Thông số IEC 104

Thông số	Giá trị	Ghi chú
USG-RED (IT)		
Channel	1	Cần khớp với BLUE
Allowed Controlling Station IP	(IP)	
Controlled Station Port	(port)	
Originator/Common Address	(1-65534)	
Max Open Connection	1	Số controlling station tối đa được kết nối đồng thời
Connection Timeout	30s	Thời gian timeout cho việc thiết lập kết nối
Send/Request Timeout	15s	Thời gian timeout cho việc gửi hoặc test APDU
Acknowledge Timeout	10S	Thời gian timeout cho việc xác nhận khi không có dữ liệu truyền
Test Frame Timeout	20S	Thời gian timeout cho việc gửi test frame khi ở trong trạng thái nghỉ kéo dài
Max Outstanding APDUs	12 APDU	Giới hạn số APDU tối đa IEC 104 client có thể gửi mà không được xác nhận
Max Latest Acknowledge APDUs	8 APDU	Giới hạn tần suất IEC 104 client xác nhận APDU
USG-BLUE (OT)		
Channel	1	Cần khớp với RED
Controlling Station IP	(IP)	IP của thiết bị IEC 104 controlling station cần thu thập dữ liệu
Controlling Station Port	(port)	
Originator address	(1-255)	Địa chỉ IEC 104 của originator
Common Address	(1-65536)	Địa chỉ ứng dụng của client (logical station) Cần khớp với cấu hình trên client
Connection Timeout	30s	Thời gian timeout cho việc thiết lập kết nối
Send/Request Timeout	15s	Thời gian timeout cho việc gửi hoặc test APDU
Acknowledge Timeout	10S	Thời gian timeout cho việc xác nhận khi không có dữ liệu truyền
Test Frame Timeout	20S	Thời gian timeout cho việc gửi test frame khi ở trong trạng thái nghỉ kéo dài

Thông số	Giá trị	Ghi chú
Max Outstanding APDUs	12 APDU	Giới hạn số APDU tối đa IEC 104 client có thể gửi mà không được xác nhận
Max Latest Acknowledge APDUs	8 APDU	Giới hạn tần suất IEC 104 client xác nhận APDU

Thông số cấu hình NTP Server

Thông số	Giá trị	Ghi chú
NTP Server 01	10.240. x.x	Máy chủ GPS and Time Frequency
NTP Server 02	10.240. x.x	Máy chủ GPS and Time Frequency
NTP Server 03	10.240. x.x	Máy chủ GPS and Time Frequency

1.5.2.5 Chính sách an ninh

Chính sách phát hiện dò quét cổng

Thông số	Giá trị	Ghi chú
Port Scan Threshold	16	Ngưỡng cho từng port
Single IP Scan Threshol	6	Ngưỡng cho từng IP
Overall Port Scan Threshold	8	Ngưỡng cộng dồng nhiều port
Last Seen Delta	28800	Block các máy có hành vi trong khoảng thời gian gần nhất
Lockout Time	32400	Khoảng thời gian unblock sau khi đã bị block
Ports to Ignore	22,80,443,514	Các port ngoại lệ
Hot Ports		Block ngay lập tức các port này

Chính sách Allow list IP

IP	Ghi chú
(IP)	Các IP ngoại lệ, không được kiểm soát

Chính sách Blocklist IP

IP	Ghi chú
(IP)	Các IP tự động bị block

1.5.2.6 Chỉ dẫn biện pháp triển khai

Chi tiết về cách thức thực hiện được thể hiện ở phụ lục 2 “Chỉ dẫn triển khai chi tiết”

1.5.2.7 Kết quả đạt được sau khi hệ thống đi vào hoạt động

Giải pháp cổng an ninh một chiều cho phép truyền số liệu từ mạng OT sang mạng IT, nhưng vẫn đảm bảo tính an toàn tuyệt đối như khi cô lập vật lý (Air Gap). Cổng an toàn một chiều cho phép truyền dữ liệu ra bên ngoài mà không sợ hacker, mã độc xâm nhập, lây lan ngược vào mạng OT, ngay cả trong trường hợp mạng IT bên ngoài đã bị xâm nhập.

1.5.2.8 Tính toán thông số kỹ thuật

Dựa trên hướng dẫn của QĐ-758 định hướng trang bị cấu hình cho công nghệ Cổng an ninh một chiều với thông số băng thông từ 100Mbps đến 500Mbps. Tuy nhiên để đáp ứng khả năng mở rộng trong tương lai và các thiết bị cổng một chiều hiện nay đều hỗ trợ tối thiểu throughput là 1Gbps, chúng tôi đề xuất trang bị cấu hình băng thông từ 1Gbps. Ngoài ra cần đảm bảo hỗ trợ 2 nguồn cấp điện, kích thước 1U. Tiêu chuẩn an ninh EAL 4+ hoặc tương đương trở lên.

1.5.2.9 Thống số kỹ thuật thiết bị yêu cầu

Thiết kế thông số thiết bị theo yêu cầu:

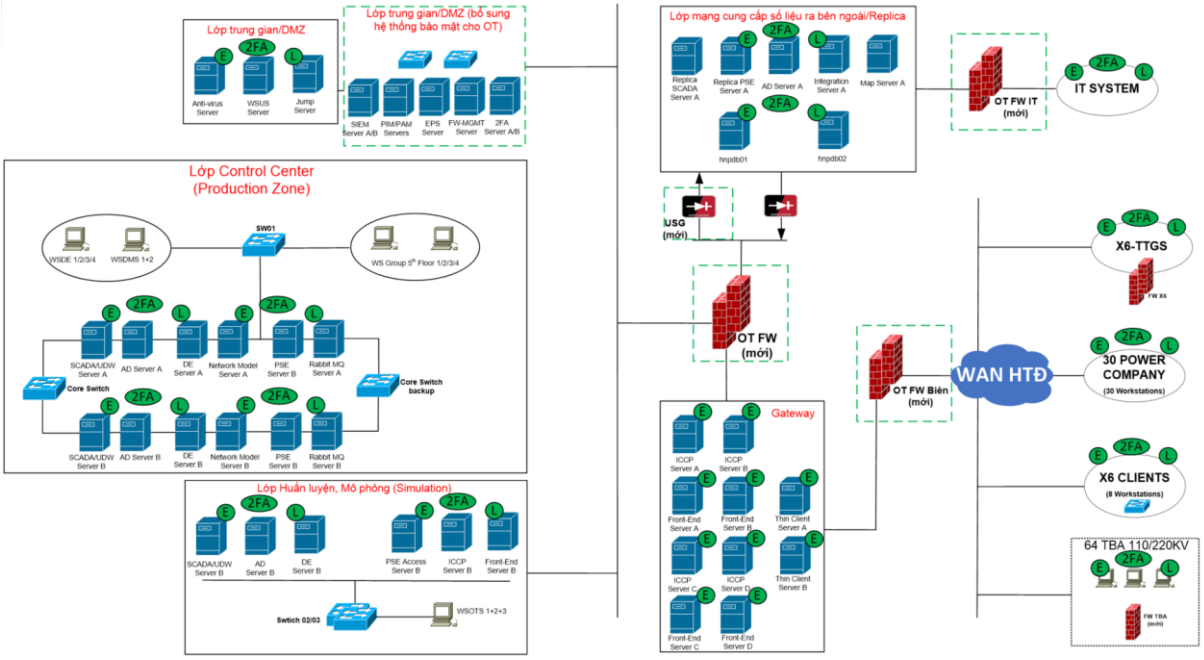
STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
IV	**Giải pháp cổng một chiều**		**1**
1	Throughput	≥ 1Gbps	
2	Giải pháp phải vận hành	Theo phương thức cho phép thông tin theo luồng một chiều từ thiết bị truyền dành riêng (dedicated transmit -TX module) tới thiết bị thu dành riêng (dedicated receiver - RX module) được đảm bảo qua đặc tính điện hoặc vật lý mà vai trò kênh truyền không bị đảo lại hoặc bị chuyển mạch bởi cấu hình phần mềm	
3	Giao thức hỗ trợ	S-FTP, TFTP,FTP-S, CIFS	
4	Yêu cầu hỗ trợ việc replicate Database	Oracle, MySQL, MSSQL.	
5	Tính sẵn sàng	Giải pháp hỗ trợ tuỳ chọn mở rộng sẵn sàng cao (High-Availability).	
6	Thiết kế module	Thiết bị gateway một chiều (cabinet) có thể chứa các host module và các module phát TX, module thu RX trong cùng phần cứng kích thước 1U	
7	Bảo hành và hỗ trợ kỹ thuật	≥ 24 tháng	

1.5.3 Hệ thống bảo vệ điểm cuối

1.5.3.1 Danh mục thiết bị lắp đặt, cài đặt

STT	TÊN HẠNG MỤC	SỐ LƯỢNG
V	Bản quyền giải pháp EPS	270

1.5.3.2 Mô hình thiết kế luận lý



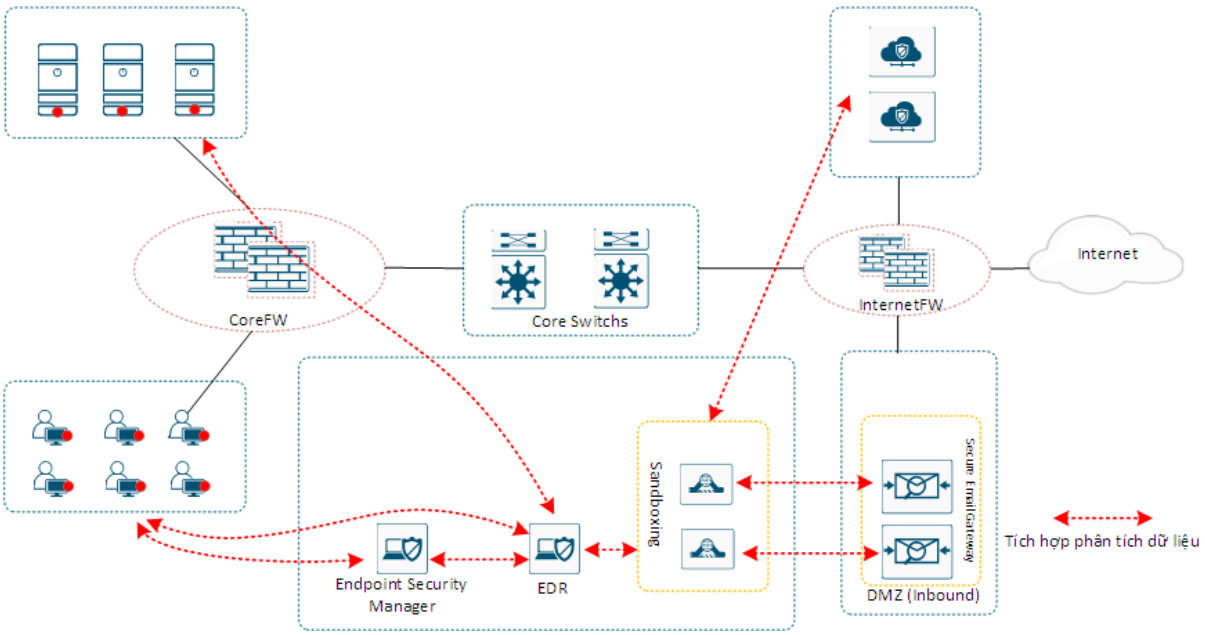
Giải pháp phòng chống mã độc điểm cuối (EPS) trang bị cho các hệ thống máy chủ, máy trạm tại hệ thống OT tại EVNHN.

Hệ thống bao gồm một server quản lý tập trung: Để cập nhật cơ sở dữ liệu virus và các phiên bản mới của hãng và quản lý các hệ thống máy chủ, máy trạm.

Các agent sẽ được cài đặt trên các máy chủ, máy trạm ở tất cả các site: TTĐK, TBA, Công ty điện lực.

Thành phần Agent có thể được triển khai/cài đặt xuống máy chủ, máy trạm theo một số cách sau:

- Triển khai tập trung từ xa qua server quản lý tập trung: Tích hợp server với Active Directory.
- Triển khai thủ công: Tạo gói cài đặt và cài đặt thủ công trên các máy chủ, máy trạm.



TKTC-BV 23 Mô hình luồng hoạt động của giải pháp Endpoint Security

Ngay sau khi thành phần Agent được cài đặt lên các máy chủ, máy trạm, người quản trị có thể tiến hành triển khai các thành phần, tính năng bảo mật của giải pháp EPS xuống các máy trạm thông qua thành phần quản trị tập trung.

Thông qua thành phần quản trị tập trung, người quản trị tiến hành cấu hình chính sách bảo mật tập trung, cũng như tạo báo cáo bảo mật tập trung cho toàn bộ hệ thống.

Thành phần Agent được cài đặt trên các máy trạm cần bảo vệ và kiểm soát. Agent sẽ thực thi các chính sách bảo mật được thiết lập từ máy chủ quản lý tập trung, đồng thời thu thập và gửi các thông tin, sự kiện bảo mật liên quan về thành phần quản trị tập trung, phục vụ quá trình giám sát và báo cáo bảo mật tập trung.

Danh sách các máy chủ, máy trạm work Station tại TTĐK nằm trong dự án NM10.4:

STT	Tên máy	Phiên bản HĐH	Ghi chú
Control Center Zone (Production Zone)			
1	SCADA/UDW Server A	RHEL 8	
2	AD Server A	Windows Server 2022	
3	DE Server A	Windows Server 2022	
4	PSE Access Server A	Windows Server 2022	
5	Rabbit MQ Server A	RHEL 8	
6	Network Model Server A	RHEL 8	
7	SCADA/UDW Server B	RHEL 8	
8	AD Server B	Windows Server 2022	
9	DE Server B	Windows Server 2022	
10	PSE Access Server B	Windows Server 2022	
11	Rabbit MQ Server B	RHEL 8	
12	Network Model Server B	RHEL 8	
13	Oracle Database Server 1	RHEL 8	
14	Oracle Database Server 2	RHEL 8	
DMZ Zone			
15	Replica SCADA/UDW server A	RHEL 8	
16	AD Server A	Windows Server 2022	
17	Replica PSE Access Server A	Windows Server 2022	
18	Anti-Virus Server A	Windows Server 2022	
19	WSUS Server A	Windows Server 2022	
20	Jump Server A	Windows Server 2022	
21	Replica SCADA/UDW server B	RHEL 8	
22	AD Server B	Windows Server 2022	
23	Replica PSE Access Server B	Windows Server 2022	
24	Anti-Virus Server B	Windows Server 2022	
25	WSUS Server B	Windows Server 2022	
26	Jump Server B	Windows Server 2022	
Gateway Zone			

STT	Tên máy	Phiên bản HĐH	Ghi chú
27	ICCP Server A	Windows Server 2022	
28	ICCP Server B	Windows Server 2022	
29	Front-End A	Windows Server 2022	
30	Front-End C	Windows Server 2022	
31	ICCP Server C	Windows Server 2022	
32	ICCP Server D	Windows Server 2022	
33	Front-End B	Windows Server 2022	
34	Front-End D	Windows Server 2022	
35	Thin Client Server 1	Windows Server 2022	
36	Thin Client Server 2	Windows Server 2022	
OTS Zone (Simulation Zone)			
37	SCADA/UDW Server A	RHEL 8	
38	SCADA/UDW Server B	RHEL 8	
39	AD Server A	Windows Server 2022	
40	DE Server A	Windows Server 2022	
41	PSE Access Server A	Windows Server 2022	
42	Front-End A	Windows Server 2022	
43	Front-End B	Windows Server 2022	
44	ICCP Server A	Windows Server 2022	
45	ICCP Server B	Windows Server 2022	
46	AD Server B	Windows Server 2022	
47	DE Server B	Windows Server 2022	
48	PSE Access Server B	Windows Server 2022	
Replica Zone			
49	Integration Server A	Windows Server 2022	
50	Map Server A	Windows Server 2022	
51	Integration Server B	Windows Server 2022	
52	Map Server B	Windows Server 2022	
Work Station			
53	Work Station 1	Windows 10	
54	Work Station 2	Windows 10	
55	Work Station 3	Windows 10	
56	Work Station 4	Windows 10	
57	Work Station 5	Windows 10	
58	Work Station 6	Windows 10	
59	Work Station 7	Windows 10	
60	Work Station 8	Windows 10	
61	Work Station 9	Windows 10	
62	Work Station 10	Windows 10	
63	Tranning Work Station 1	Windows 10	

Danh sách máy đầu cuối được cài agent bổ sung tại Công ty Điện lực:

Định danh (Hostname)	Hệ điều hành	Ghi chú
Nam Từ Liêm	Windows 10 Pro x64	Dell Precision 3630 Tower
Thanh Trì	Windows 10 Pro x64	Dell Precision 3630 Tower
Gia Lâm	Windows 10 Pro x64	Dell Precision 3630 Tower
Đông Anh	Windows 10 Pro x64	Dell Precision 3630 Tower
Sóc Sơn	Windows 10 Pro x64	Dell Precision 3630 Tower
Hoàng Mai	Windows 10 Pro x64	Dell Precision 3630 Tower
Long Biên	Windows 10 Pro x64	Dell Precision 3630 Tower
Mê Linh	Windows 10 Pro x64	Dell Precision 3630 Tower
Hà Đông	Windows 10 Pro x64	Dell Precision 3630 Tower
Sơn Tây	Windows 10 Pro x64	Dell Precision 3630 Tower
Chương Mỹ	Windows 10 Pro x64	Dell Precision 3630 Tower
Thạch Thất	Windows 10 Pro x64	Dell Precision 3630 Tower
Thường Tín	Windows 10 Pro x64	Dell Precision 3630 Tower
Ba Vì	Windows 10 Pro x64	Dell Precision 3630 Tower
Đan Phượng	Windows 10 Pro x64	Dell Precision 3630 Tower
Hoài Đức	Windows 10 Pro x64	Dell Precision 3630 Tower
Mỹ Đức	Windows 10 Pro x64	Dell Precision 3630 Tower
Phú Xuyên	Windows 10 Pro x64	Dell Precision 3630 Tower
Phúc Thọ	Windows 10 Pro x64	Dell Precision 3630 Tower
Quốc Oai	Windows 10 Pro x64	Dell Precision 3630 Tower
Thanh Oai	Windows 10 Pro x64	Dell Precision 3630 Tower
Ứng Hòa	Windows 10 Pro x64	Dell Precision 3630 Tower
Bắc Từ Liêm	Windows 10 Pro x64	Dell Precision 3630 Tower
Ba Đình	Windows 10 Pro x64	Dell Precision 3630 Tower
Hoàn Kiếm	Windows 10 Pro x64	Dell Precision 3630 Tower
Hai Bà Trưng	Windows 10 Pro x64	Dell Precision 3630 Tower
Đống Đa	Windows 10 Pro x64	Dell Precision 3630 Tower
Tây Hồ	Windows 10 Pro x64	Dell Precision 3630 Tower
Cầu Giấy	Windows 10 Pro x64	Dell Precision 3630 Tower
Thanh Xuân	Windows 10 Pro x64	Dell Precision 3630 Tower

Danh sách máy đầu cuối được cài agent bổ sung tại Công ty Lưới điện cao thế:

STT	Tên máy	Phiên bản HĐH	Ghi chú
1	Communication & Data Server 1	Windows	
2	Communication & Data Server 2	Windows	
3	HIS & Application Server 1	Windows	
4	HIS & Application Server 2	Windows	
5	Operation Workstation 1	Windows	

STT	Tên máy	Phiên bản HĐH	Ghi chú
6	Operation Workstation 2	Windows	
7	Máy tính kỹ sư 1	Windows	
8	Máy tính kỹ sư 2	Windows	

Danh sách các máy đầu cuối được cài agent bổ sung tại các TBA:

STT	Trạm	Gateway	HMI	Engineer	HIS	Bản ghi sự cố
1	Đông Anh	1 - win 10/ chưa active	0	0	0	1
2	Gia Lâm	1 - win 10/2022	1 - win 10/2020	0	0	1
3	Thượng Đình	1 - win 7 1 - win 7 hỏng	0	0	0	1
4	Sơn Tây	1 - win 7	0	0	0	1
5	Yên Phụ	1 - win 7	1 - win 7	1	0	1
6	Nghĩa Đô	1 - win 10	1 - win 10	0	0	1
7	Văn Điển	1 - win 10	1 - win 10	0	0	1
8	Trần Hưng Đạo	1 - win 10		0	0	1
9	Phương Liệt	1 - win SV 12	1 - win SV 12	0	0	1
10	Giám	1 - win 10	1 - win 10 (sv2)	0	0	1
11	Sài Đồng	1 - win 10	1 - win 10	0	0	1
12	Nội Bài	1 - win 10 active	1 - win 10 active	0	0	1
13	Bắc Thăng Long	1 - win 10 active	0	0	0	1
14	Bờ Hồ	1 -win 10/ Thiếu key	1 -win 10	0	0	1
15	Thanh Xuân	1 -win 10	1 -win 10	0	0	1
16	Nhật Tân	1 - win 10	1 - win 10	0	0	1
17	Thanh Nhàn	1 - win 7	1 - win 7	0	0	1
18	Hải Bối	1 - win 10 active	1 - win 10	0	0	1
19	Mỹ Đình	1 - win 10	1 - win 10	0	0	1

STT	Trạm	Gateway	HMI	Engineer	HIS	Bản ghi sự cố
20	Linh Đàm	1 - win 7	1 - win 7	1/ VH 2017	0	1
21	Phùng Xá	1 - win 10	0	0	0	1
22	Văn Quán	1 - win 10	1 - win 10	0	0	1
23	Trôi	1 - win 7	0	0	0	1
24	Thường Tín	1 - win 10 chưa active	1 - win 10 chưa active	0	0	1
25	Cầu Diễn	1 - win 7	1 - win 7	1/ win 7	0	1
26	Quang Minh	1 - win 10 chưa active	0	0	0	1
27	Bắc An Khánh	1 - win 7	0	0	0	1
28	Gia Lâm 2	1 - win 7	1 - win 7	1/ win 7	0	1
29	Thanh Oai	1 -win 7	0	0	0	1
30	Tây Hồ	1 - win 10	2 - win 10	1	0	1
31	Mai Lâm	1 - win 10 active	1 - win 10 chưa active	0	0	1
32	SB Nội Bài	1 - win 7	1 - win 7	0	0	1
33	Mỗ Lao	1 - win 7	1 - win 7	0	0	1
34	Sơn Tây 2	1 - win 10	1 - win 10	0	0	1
35	Từ Liêm	1 - win 10	1 - win 10 / hỏng	0	0	1
36	NC Long Biên	1 - win SV 12	1 - win SV 12	0	0	1
37	NC Quốc Oai	2 - win 7	1 - win 7	0	0	1
38	NC Đông Anh	2 - win 7	1 - win 7	0	0	1
39	Phú Nghĩa	2 - win 7	1 - win 7	0	0	1
40	CV Thống Nhất	1 - win 7 1 - win 7 hỏng, mất key	1 - win 7	0	0	1
41	Ba Vì	1 - win 7	1 - win 7	0	0	1
42	CNC Hòa Lạc	2 - win 10	2 - win 10	1	1	1
43	Phùng	1 - win SV 12 / win 10 k chạy đc Sys600	1 - win 10 / k chạy được HMI	0	0	1
44	Minh Khai	1 - win 10	1 - win 10	0	0	0

STT	Trạm	Gateway	HMI	Engineer	HIS	Bản ghi sự cố
45	Phú Xuyên	1 - win 10	1 - win 10	0	0	0
46	Sài Đồng 2	1 - win 10	1 - win 10	0	0	0
47	Dương Nội	1 - win 10	1 - win 10	0	0	0
48	Ngọc Hồi	1 - win 10	1 - win 10	0	0	0
49	Bắc Thành Công	1 - win 10	1 - win 10	0	0	0
50	CV Hồ Yên Sở	1 - win 10	1 - win 10	0	0	0
51	Mỹ Đức	1 - win 10	1 - win 10	0	0	0
52	CV Thủ Lệ	2 - win 10	1 - win 10	0	0	0
53	Trâu Quỳ	1 - win 10	1 - win 10	0	0	0
54	Hồng Dương	1 - win 10	1 - win 10	0	0	0
55	CNC Hòa Lạc 2	1 - win 10	1 - win 10	0	0	0
56	Thạch Thất 2	1 - win 10	1 - win 10	0	0	1
57	Vân Đình	1 - win 10	0	0	0	1
58	Tía	1 - win 7/10	1	0	0	1
59	Phúc Thọ	1 - win 10	1 - win 10	0	0	1
60	Xuân Mai	1 - win 7	1 - win 10	0	0	1
Tổng		60 máy	55 máy	5 máy	1 máy	48 máy

Với số lượng thống kê các máy chủ, máy trạm tại các đơn vị nằm trong dự án đầu tư có tổng 270 máy bao gồm cả các máy nằm trong hệ thống dự án NM10.4. Trong trường hợp các máy trong dự án NM10.4 đã có bản quyền hệ thống EPS riêng, thì tổng số lượng máy thống kê được là 207 máy.

1.5.3.3 Hệ thống yêu cầu các kết nối mạng như sau:

STT	Nguồn	Đích	Dịch vụ	Ghi chú
1	Máy đầu cuối	Endpoint Security Manager	TCP 80, 8014, 443, 2967	Quản trị agent

1.5.3.4 Phân bổ tài nguyên ảo hoá

Máy chủ quản trị tập trung của hệ thống yêu cầu tài nguyên như sau:

Thông số	Giá trị	Ghi chú
CPU	8 Core	
RAM	16GB RAM	
HDD	1 TB	

1.5.3.5 Thông số cài đặt và cấu hình

Thông số	Giá trị	Ghi chú
IP Address	10.24. x.x	

Thông số	Giá trị	Ghi chú
Subnet Mask	255.255.255.0	
Default Gateway	10.24.x.1	
NTP Server	10.240. x.x 10.240. x.x 10.240. x.x	

1.5.3.6 Chính sách an ninh

Firewall policy

No	Name	Action	App	Host	Service	Log	Severity
1	Allow ICMP	Allow	Any	Any	ICMP	No	Minor
2	Block Local File Sharing	Block	Any	Any	SMB	Yes	Minor
3	Block Access to Critical Servers	Block	Any	[Critical Servers]	Any	Yes	Minor
4	Block Blacklisted ports	Block	Any	Any	[Blacklisted ports]	Yes	Minor
5	Block Blacklisted apps	Block	[Blacklisted apps]	Any	Any	Yes	Minor
6	Allow All	Allow	Any	Any	Any	No	Minor

IPS policy

Thông số	Giá trị	Ghi chú
Enable IPS	Yes	
Excluded Hosts	[Host list]	
Enable Browser IPS	Yes	

Application and device control policy

Enabled	Rule set	Environment
Yes	Block access to Autorun.inf	
Yes	Block file extend	
Yes	Block Hash	
Yes	Block Game	
Yes	Block Malware	

1.5.3.7 Chỉ dẫn biện pháp triển khai

Chi tiết về cách thức thực hiện được thể hiện ở phụ lục 2 “Chỉ dẫn triển khai chi tiết”

1.5.3.8 Kết quả đạt được sau khi hệ thống đi vào hoạt động

Giải pháp EPS bảo vệ các máy chủ, máy trạm trước các mối nguy hại từ các mã độc như Virus, Spyware, Malware, … và các phần mềm độc hại. Cung cấp nhiều mức bảo vệ cho người dùng, phát hiện sớm và phòng ngừa mã độc. Ngoài ra, giải pháp còn có khả năng phát hiện mã độc dựa trên việc đưa ra phân tích đối với các hành vi bất thường. Áp dụng các công nghệ tiên tiến như AI, Machine Learning để giúp hiệu quả hơn trong việc bảo vệ các máy chủ, máy trạm trong hệ thống.

1.5.3.9 Tính toán thông số kỹ thuật

Tổng số lượng bản quyền được yêu cầu theo số lượng máy trạm thực tế theo khảo sát là 270 máy, số lượng bản quyền yêu cầu tối thiểu cho 270 máy

1.5.3.10 Thông số kỹ thuật yêu cầu

Thông số kỹ thuật yêu cầu cho giải pháp bảo vệ điểm cuối:

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
I	**Bản quyền giải pháp EPS**		**270**
1	Quản lý tập trung	Giải pháp cung cấp quản lý tập trung tất cả các máy trạm, thiết bị; phần mềm bảo mật đầu cuối; chính sách bảo mật; theo dõi giám sát.	
2	Tích hợp và nền tảng mở	Mở rộng giải pháp Symantec hiện có hoặc một giải pháp mới tương đương.	
3	Loại hiết bị được bảo vệ	Thiết bị bao gồm máy chủ, máy trạm.	
4	Quản trị	Có hệ thống quản trị tại chỗ (on-premised)	
		Hỗ trợ khả năng báo cáo, tìm kiếm thông tin theo thời gian thực, trong quá khứ và dữ liệu theo yêu cầu	
		Tích hợp với các hệ thống SIEM như IBM Qrada, Splunk	
5	Tính năng bảo mật	Phát hiện và ngăn chặn các loại mã độc: malware, ransomware, malicious scripts, unknown và new threats	
		Phát hiện và ngăn chặn mã độc chưa biết với công nghệ Signature-less bao gồm	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
		machine learning, behavioral analysis,...	
		Tích hợp tường lửa - Firewall	
		Tích hợp tính năng phát hiện và phòng chống xâm nhập – Host Intrusion Prevention System	
		Tích hợp bảo vệ và lọc web - Web Filter	
		Tích hợp quản lý ứng dụng và thiết bị - Application and Device Control	
		Tự động phục hồi sự thay đổi gây ra bởi mã độc và đảm bảo hệ thống hoạt động ở trạng thái khoẻ mạnh gần nhất	
6	Hệ điều hành được hỗ trợ	Windows, MAC, Linux	
7	Phương thức quét	Hỗ trợ nhiều phương thức quét: Full Scan, Quick scan, Auto Protect, v.v…	
		Hỗ trợ thực hiện Quick scan 1 ngày / lần, Full scan 1 tuần/lần	
		Hỗ trợ tự động quét mã độc trên các file mới xuất hiện trên hệ thống (Từ các vật mang tin từ bên ngoài, dữ liệu được tải xuống từ internet, v.v…)	
8	Bảo hành và hỗ trợ kỹ thuật	≥ 24 tháng	

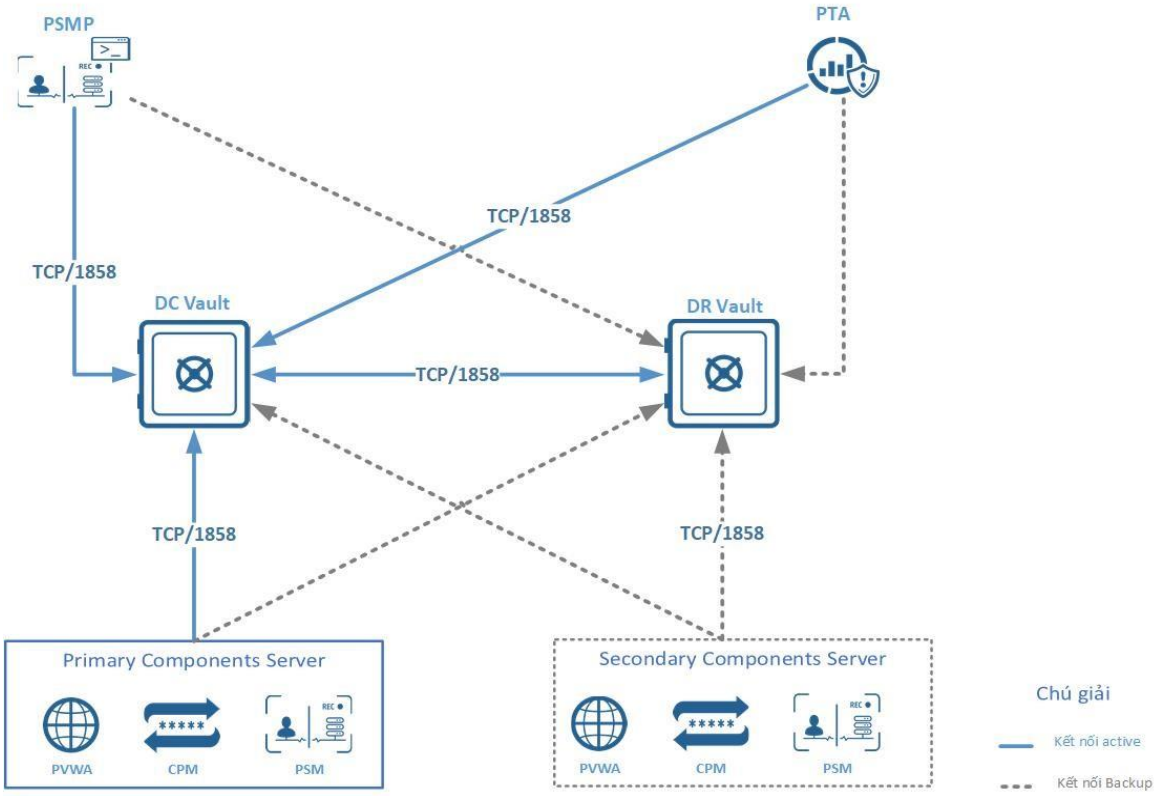
1.5.4 Hệ thống quản lý tài khoản đặc quyền

1.5.4.1 Danh mục thiết bị lắp đặt, cài đặt

STT	TÊN HẠNG MỤC	SỐ LƯỢNG
VI	Bản quyền giải pháp PIM/PAM	01

1.5.4.2 Mô hình thiết kế luận lý

Sơ đồ logic mô tả luồng kết nối giữa các thành phần trong hệ thống:



TKTC-BV 24 Mô hình thiết kế luận lý giải pháp PAM

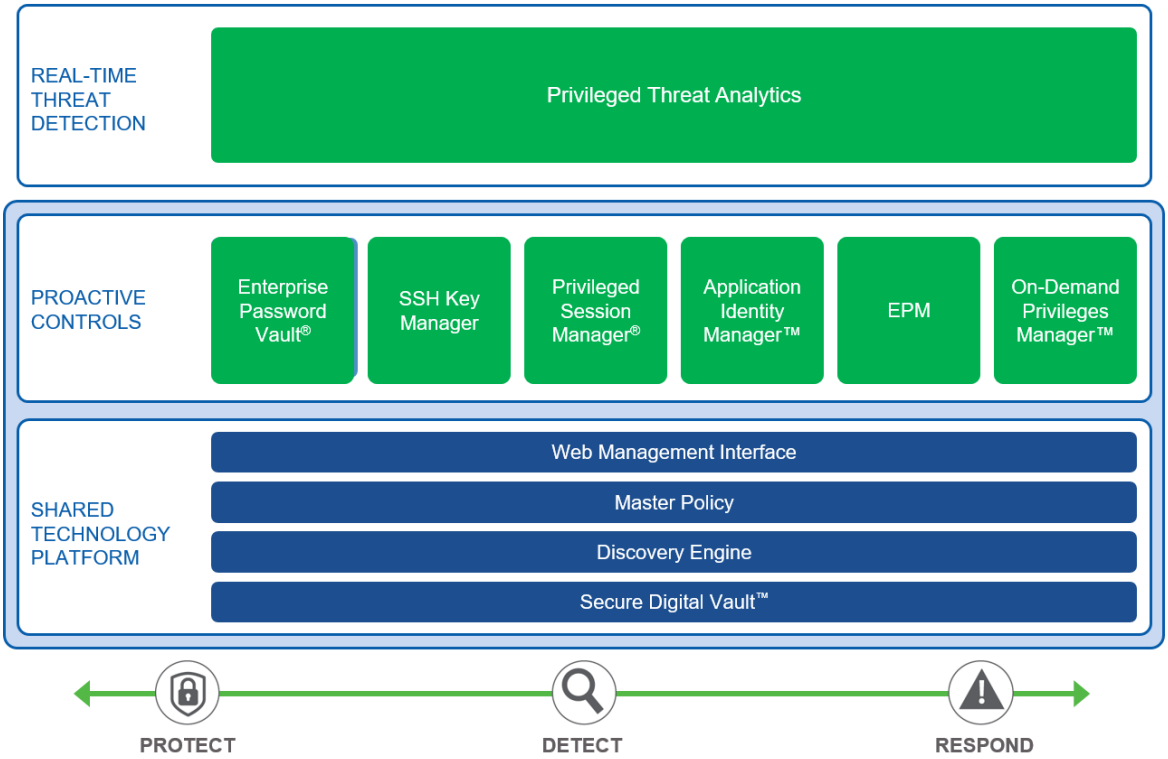
Mô hình triển khai bao gồm các thành phần:

- 01 DC Vault: Đây là Vault lưu trữ chính của toàn bộ hệ thống. Trong điều kiện bình thường, mọi thông tin lưu trữ sẽ được tập trung tại đây.
- 01 DR Vault: Là Vault Backup, sao chép toàn bộ thông tin của Vault chính (DC Vault). Khi Vault chính gặp sự cố và không thể hoạt động được DR Vault sẽ trở thành Vault chạy chính.
- 02 Components Server: Là 02 thành phần cài đặt các ứng dụng PVWA, CPM, PSM theo cơ chế Active - Backup. Trong điều kiện bình thường, đây là thiết bị chịu tải chính. Khi Components Server 01 lỗi và không thể hoạt động được, Components Server 02 sẽ chuyển thành thiết bị chịu tải chính của người dùng.
- 01 PSMP: Là thành phần hỗ trợ người dùng truy cập vào các thiết bị đích thông qua SSH-Proxy.
- 01 PTA: Là thành phần thu thập thông tin và giám sát truy nhập đặc quyền của toàn bộ hệ thống.

Tính năng các thành phần như sau:

Giải pháp quản trị truy nhập đặc quyền (PAM) của cung cấp một "giải pháp bảo mật" bên trong doanh nghiệp nơi mà tất cả những mật khẩu đặc quyền được bảo mật, tự động quản lý, và chia sẻ giữa những người dùng được phép như nhân viên IT, nhân viên quản trị dữ liệu, nhân viên quản trị vùng hoặc từ xa hay những dịch vụ thiếu sự quan

tâm cần thiết như những ứng dụng trong kinh doanh, hệ thống quản trị thông tin…Cấu trúc của hệ thống quản lý mật khẩu đặc quyền - PAM bao gồm những thành phần sau:



Vault Server (Secure Digital Vault)

- Là thành phần lưu trữ toàn bộ thông tin quan trọng nhất của hệ thống, thành phần này dựa trên công nghệ Digital Vault của PAM, đáp ứng với chuẩn bảo mật FIPS 140-2 và đã được chứng minh là đáp ứng các chuẩn bảo mật như: PCI, NERC, FERC, SOX, HIPAA, GLB…. Vault server được thiết kế với khả năng bảo mật đa lớp (bao gồm: tường lửa, VPN, xác thực, điều khiển truy cập, mã hóa…) kết hợp chặt chẽ với nhau và trung tâm là hệ thống quản lý mật khẩu đặc quyền – PIM Suite là giải pháp tối ưu trong vấn đề lưu trữ, chia sẻ định danh trong môi trường doanh nghiệp.

Central Policy Manager (CPM)

- CPM cho phép tổ chức định nghĩa các chính sách dựa trên quy trình công việc cụ thể tại tổ chức cũng như nhu cầu kiểm soát đối với các tài khoản đặc quyền.
- Cho phép tổ chức xác thực các mật khẩu trên các thiết bị và có khả năng đồng bộ lại mật khẩu trong trường hợp cần thiết như mất kết nối hệ thống quản lý mật khẩu tới các thiết bị cần quản lý …
- CPM cho phép tạo các mật khẩu mới một cách ngẫu nhiên và thay thế các mật khẩu hiện tại của các thiết bị do PIM quản lý. Các mật khẩu được tạo mới sẽ được lưu trữ trên Vault Server.
- Các chính sách được lưu trữ trong những tài khoản đặc quyền khác nhau, vì vậy chỉ có người dùng đáp ứng được các chính sách an ninh mới có thể truy cập.

Password Vault Web Access (PVWA)

- Password Vault Web Access (PVWA) mang đầy đủ một tính năng của một Cổng thông tin Web. Cung cấp giao diện cho phép điều khiển cho các yêu cầu, truy cập

và mật khẩu quản lý đặc quyền cũng như kết nối trong suốt để quản lý thiết bị. PVWA hỗ trợ cả người dùng, quản trị viên hệ thống.

- PVWA cung cấp giao diện đơn giản, thuận tiện cho người sử dụng. Ngoài ra người dùng có thể tìm kiếm các thông tin một cách dễ dàng và nhanh chóng thông qua công cụ tìm kiếm được thiết kế một cách hợp lý nhất.
- PVWA còn cung cấp giao diện ngọn nhẹ và đơn giản cho phép bạn truy cập PVWA thông qua các thiết bị di động (BlackBerry, Android, iPhone) để thao tác với tài khoản đặc quyền.

Privileged Session Management (PSM)

- PSM (Privileged Session Management): là giải pháp cho phép tổ chức kiểm soát, cô lập và theo dõi tất cả các phiên làm việc của các tài khoản đặc quyền trên các máy chủ, cơ sở dữ liệu hoặc các hệ thống máy ảo.

Privileged Threat Analytics (PTA)

- Privileged Threat Analytics (PTA) cho phép hệ thống thu thập thông tin bảo mật tài khoản đặc quyền, cung cấp các phân tích chi tiết, kịp thời về các mối đe dọa có thể hành động bằng cách xác định chính xác hoạt động độc hại của người dùng có đặc quyền ẩn trước đó.

Các tính năng chính:

- Các mật khẩu đặc quyền phải được lưu trữ dưới dạng mã hóa AES-256 và SHA1 theo chuẩn mã hóa FIPS 140-2.
- Quản lý mật khẩu đặc quyền tập trung qua giao diện Web.
- Chức năng kiểm soát kép (Dual Control) trong việc xin và phê duyệt mật khẩu đặc quyền.
- Quản trị viên đã có thể theo dõi real-time các hành động của người dùng khi truy cập vào server, thiết bị, cơ sở dữ liệu.
- Có khả năng tự động thay đổi mật khẩu đặc quyền theo chính sách đặt ra của các hệ thống sau: Hệ điều hành, Hệ quản trị cơ sở dữ liệu, Network devices, Security devices.
- Hỗ trợ nhiều phương thức xác thực khi đăng nhập vào hệ thống: Username/Password, RADIUS (Xác thực mạnh của hãng thứ 3: Onespan, Entrust,RSA,…), SAML.
- Tìm kiếm lại các câu lệnh SQL hoặc SSH commands và xem lại recordings: Quản trị viên sẽ dễ dàng tìm kiếm các recordings theo SQL & SSH commands, dễ dàng xem lại với video player có sẵn trên trình duyệt.

Quy hoạch địa chỉ IP cho các thành phần:

STT	Máy chủ	IP
1	Vault	10.24. x.x
2	Vault dự phòng	10.24. x.x
3	PVWA, CPM	10.24. x.x
4	PSM	10.24. x.x
5	PTA	10.24. x.x

STT	Máy chủ	IP
6	CPM, PVWA, PSM dự phòng	10.24. x.x

1.5.4.3 Phân bổ tài nguyên ảo hoá

STT	Máy chủ	Yêu cầu
1	Vault	8 Core
		8 GB RAM
		150Gb OS
		2TB Data
2	Vault dự phòng	8 Core
		8 GB RAM
		150Gb OS
		2TB Data
3	PVWA, CPM	8 Core
		16 GB RAM
		150GB OS
		500GB Data
4	PSM	16 Core
		32 GB RAM
		150GB OS
		500GB Data
5	PTA	4 Core
		16 GB RAM
		500 GB
6	CPM,PVWA, PSM dự phòng	8 Core
		16 GB RAM
		150GB OS
		500GB Data

1.5.4.4 Chính sách hệ thống

Thiết kế Safe

- Các thông tin về tài khoản đặc quyền để kết nối tới thiết bị đích (bao gồm thông tin về username, password, platform, địa chỉ IP đích…) được lưu trữ tập trung trong Safe trên Vault Server.
- Mỗi Quản trị viên được cấp một Safe để chứa danh sách tài khoản đặc quyền của cá nhân mình để truy cập tới các hệ thống đích.
- Quy tắc đặt tên safe cho các Quản trị viên: < User AD của quản trị viên >_Safe, ví dụ: Administrator_safe.

Thiết kế Platform

- Hệ thống quản lý tài khoản đặc quyền cho phép quản trị viên tuỳ chính các Platform, thêm các loại kết nối mà quản trị viên mong muốn, dùng để quản trị và truy cập các tài khoản đặc quyền.

- Quy tắc đặt tên Platform: <Tên loại thiết bị>_<Mô tả của Platform>, ví dụ: Windows_Dual_Control_01.
- Quản trị viên đặt ra chính sách mật khẩu chi tiết tới từng loại nền tảng (Platform).
- Ngoài các chính sách như tần suất đổi mật khẩu, tần suất xác minh mật khẩu được quy định ở Master Policy và các Exception, quản trị viên có thể quy định các chính sách về quản lý và chính sách độ phức tạp của mật khẩu trong phần cấu hình Platform Configuration. Các tham số được mô tả như trong bảng dưới đây:

STT	Tham số	Giải thích	Giá trị mặc định
1	VFPerformPeriodic-Verification	Thực hiện verify mật khẩu theo chu kỳ trong Master Policy	Yes
2	VFPerformPeriodic-Change	Thực hiện đổi mật khẩu theo chu kỳ trong Master Policy	Yes
3	PasswordLength	Độ dài mật khẩu được CPM sinh ra.	8
4	MinUpperCase	Số lượng tối thiểu ký tự chữ hoa.	1
5	MinLowerCase	Số lượng tối thiểu ký tự chữ thường.	1
6	MinDigit	Số lượng tối thiểu ký tự số.	1
7	MinSpecial	Số lượng tối thiểu ký tự đặc biệt.	1
8	PasswordForbiddenChars	Các ký tự ngoại trừ trong mật khẩu của các nền tảng hệ thống đích.	

Thiết kế chính sách chung

Master Policy là bộ chính sách tổng thể của hệ thống, có khả năng quản lý tập trung chính sách quản lý mật khẩu tài khoản đặc quyền và quản lý chính sách phiên truy cập

Chính sách	Mô tả	Giá trị mặc định	Giá trị khuyến nghị
Require dual control password access approval	Yêu cầu kiểm soát phân cấp phê duyệt khi sử dụng tài khoản	Active	Active
Enforce checkin/checkout exclusive access	Hạn chế quyền sử dụng đồng thời một tài khoản đặc quyền cho một người quản trị.	Inactive	Inactive
Enforce one-time password access	Áp dụng chính sách mật khẩu dùng một lần, sau khi dùng mật khẩu được đổi.	Inactive	Inactive

Chính sách	Mô tả	Giá trị mặc định	Giá trị khuyến nghị
Allow EPV transparent connections	Cho phép Quản trị viên kết nối trong suốt tới thiết bị mà không cần nhập mật khẩu.	Active	Active
Require users to specify reason for access	Yêu cầu Quản trị viên nhập vào lý do sử dụng tài khoản.	Active	Active
Require password change every X days	Cứ sau X ngày thì mật khẩu tự động được đổi	90	90 (Giá trị nên nhỏ hơn hoặc bằng 90).
Require password verification every X days	Cứ sau X ngày thì mật khẩu tự động được kiểm tra tính trùng khớp.	7	7 (Gía trị nên nhỏ hơn hoặc bằng 7)
Require privileged session monitoring and isolation	Yêu cầu các phiên kết nối phải đi qua máy chủ PSM.	Inactive	Active
Record and save session activity	Yêu cầu ghi lại và lưu trữ các phiên làm việc	Active	Active

1.5.4.5 Thiết kế phân quyền người dùng

Phân quyền User đối với hệ thống Vault

Đối với hệ thống Vault có thể thực hiện phân quyền cho User bằng cách Mapping các Group User vào các Role mặc định tương ứng thông qua giao diện PWVA, các quyền được mô tả cụ thể như sau:

Role	Mô tả
Vault Admins	Quản trị viên có quyền cấp cao nhất, có thể quản trị Vault Server
Safe managers	Quản trị viên có quyền quản lý các users, create Safes và accounts.
Auditors	Quản trị viên có quyền kiểm tra audit logs, reports và session recordings
Users	Quản trị viên mặc định, cho phép vào hệ thống nhưng không có bất kỳ quyền nào. Được phân quyền thông qua Safe.

Phân quyền với Group Vault Admins

Group Vault Admins là group bao gồm các user có full quyền với hệ thống Vault ngoài quyền Backup all safes và Restore all safes.

STT	Phân quyền	Chi tiết
1	Add safes	Quyền được tạo và chỉnh sửa cấu hình Safes
2	Audit users	Quyền được tra cứu và xem các Session được record
3	Add/Update users	Quyền được thêm user và Update thông tin users
4	Reset users'pasword	Quyền được Reset password users
5	Active users	Quyền Active users
6	Add network areas	Quyền tạo cấu hình network areas (vùng network được cho phép truy cấp tới Vault và PWVA)
7	Manage server file categories	Quyền quản lý file trên safe

Phân quyền với Group Safe Managers

Group Safe Managers là group bao gồm các quyền tạo Safes, add User member và phân quyền User với các Safes được tạo

STT	Phân quyền	Chi tiết
1	Add safes	Quyền được tạo và chỉnh sửa cấu hình Safes
2	Add/Update users	Quyền được thêm user và Update thông tin users

Phân quyền với Group Auditor

Group Auditor là group bao gồm các quyền Search và View lại các User Activity, Session Record, command log Session…

STT	Phân quyền	Chi tiết
1	Audit users	Quyền được tra cứu và xem các Session được record

Phân quyền với Group User

Group User bao gồm các người dùng bình thường không có quyền với Vault.

Phân quyền Safe

Tài khoản quản trị viên (Safe Manager)

Quản lý toàn bộ các quyền trên các Safe tại các miền: Người quản lý phòng ban nào sẽ được quyền quản lý Safe của các phòng ban (có thể thêm, sửa, xóa các tài khoản, phân quyền sử dụng…), được phân các quyền sau:

STT	Phân quyền	Chi tiết
1	Use accounts	Sử dụng các tài khoản trong safe để kết nối tới thiết bị đầu cuối.
2	List accounts	Liệt kê danh sách tài khoản trong safe
3	Add accounts	Thêm tài khoản.
4	Update account content	Cập nhật thông tin của tài khoản.
5	Update account properties	Cập nhật thuộc tính của tài khoản.

STT	Phân quyền	Chi tiết
6	Initiate CPM account management operations	Thực hiện các tác vụ quản lý tài khoản tự động sử dụng CPM.
7	Specify next password value	Chỉ định mật khẩu được đổi tự động.
8	Rename accounts	Đổi tên tài khoản.
9	Delete accounts	Xóa tài khoản.
10	Unlock accounts	Mở khóa tài khoản.
11	Manage Safe	Quản lý Safe.
12	Manage Safe Members	Quản lý các owner trên Safe.
13	View audit	Xem audit log của safe.
14	View Safe Members	Xem danh sách các thành viên trong safe.

Tài khoản của nhân sự và đối tác hỗ trợ/triển khai

STT	Phân quyền	Chi tiết
1	Use accounts	Sử dụng các tài khoản trong safe để kết nối tới thiết bị đầu cuối.
2	List accounts	Liệt kê danh sách tài khoản trong safe

Tài khoản Auditor

STT	Phân quyền	Chi tiết
1	View audit log	Xem Audit log của Safe
2	View Safe members	Xem danh sách tài khoản trong safe

Ma trận phân quyền

Ma trận phân quyền cho người dùng (User) khi truy cập hệ thống được sử dụng quyền nào trên các Safes và Accounts mà họ quản lý. Trong đó:

- Account: Tài khoản đặc quyền trên thiết bị.
- User: Username người dùng.
- Theo quy ước:
- 1 Account chỉ nằm trong 1 Safe.
- 1 Safe chứa nhiều Accounts.
- 1 Safe được gán nhiều Users.
- 1 User được gán cho nhiều Safes.

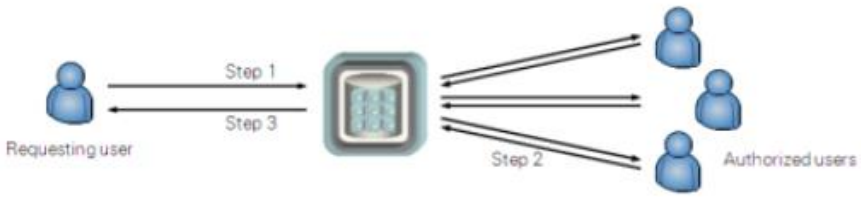
Quyền Users	Quyền trên Safe_01	Quyền trên từng Accounts trong Safe_01			
		Account01	Account02	Account03	Account04
User01	**Use Accounts** **Retrieve Account** **List Accounts** Kết nối tới thiết bị Nhìn mật khẩu account	**Use** **Retrieve** Kết nối tới thiết bị Nhìn thấy mật khẩu account	**Use** Kết nối tới thiết bị	**Retrieve** Nhìn thấy mật khẩu account	Không nhìn thấy account
User02		Không nhìn thấy account	**Use** **Retrieve**	**Use** Kết nối tới thiết bị	**Retrieve**

	Liệt kê accounts		Kết nối tới thiết bị Nhìn thấy mật khẩu account		Nhìn thấy mật khẩu account
User03		**Retrieve** Nhìn thấy mật khẩu account	Không nhìn thấy account	**Use** **Retrieve** Kết nối tới thiết bị Nhìn thấy mật khẩu account	**Use** Kết nối tới thiết bị

Thiết kế Dual Control

Dual Control là tính năng của hệ thống PAM nhằm cung cấp cơ chế kiểm soát sử dụng tài nguyên và tác động hệ thống. Chế độ Dual Control cho phép:

- Kiểm soát truy cập tới hệ thống thông qua Request. User cần truy cập cần tạo Request và phải được duyệt Request trước khi truy cập hệ thống đích.
- Kiểm soát truy cập tài nguyên với User được duyệt Request trong khoảng thời gian cho phép.
- Kiểm soát và phê duyệt truy cập và tác động theo Request thông qua các User được cấp quyền Approve.



Có các kiểm phê duyệt như sau:

- Peer Approval Process
  - Đây là cấu hình phê duyệt ngang hàng , bất kì User nào cũng có thể là người Request và cũng là người Approver với hệ thống khác nhưng không cho phép một người vừa là Request vừa là Approver với cùng một hệ thống.
- Bypass Dual Control
  - Trong trường hợp cần thiết thì một số User cần quyền ByPass Dual Control để truy cập thẳng hệ thống mà không cần phê duyệt.
  - Thông thường với các User thuộc Admin Team sẽ được cấp quyền "Access Safe without confirmation" để có thể Bypass Dual Control.
- Multi-Group Approval Process
  - Có thể cấu hình nhiều Approver ở các group khác nhau để thực hiện phê duyệt Requester.

- Trong trường hợp này thì mỗi Group cần ít nhất 1 người phê duyệt thì Requester mới có thể truy cập tới hệ thống.

- Multi-Level Approval Process
  - Với cấu hình Multi-Level Approval Process thì Active tham số "Request multi-level password access approval".
  - Bên cạnh đó có thể cấu hình "Only direct managers can approve password requests" nhằm đảm bảo chỉ có user manager mới đủ quyền phê duyệt (group được phân quyền trên AD).

1.5.4.6 Chỉ dẫn biện pháp triển khai

Chi tiết về cách thức thực hiện được thể hiện ở phụ lục 2 "Chỉ dẫn triển khai chi tiết"

1.5.4.7 Kết quả đạt được sau khi hệ thống đi vào hoạt động

Giải pháp quản lý mật khẩu/tài khoản đặc quyền được trang bị để đảm bảo an toàn đối với các mối đe dọa từ việc quản lý con người với các quyền truy cập vào hệ thống CNTT:

- Mật khẩu đặc quyền của các thiết bị mạng, hệ điều hành, CSDL, … được bảo mật tốt hơn (tự động thay đổi mật khẩu theo policy qui định) trở thành mật khẩu động.
- Các admin tham gia quản lý hệ thống IT sẽ được phân quyền cho từng nhóm thiết bị mình quản lý, mọi hoạt động của Admin liên quan đến truy vấn mật khẩu của các thiết bị đó đều được kiểm soát, trong trường hợp đặc biệt còn cần phải có sự cho phép của Admin có thẩm quyền cao hơn (Dual Control).
- Có thể giám sát mọi hoạt động của Admin khi họ làm việc với thiết bị quan trọng, mọi hoạt động sẽ bị ghi lại dưới dạng file video và được lưu lại một cách bảo mật trong hệ thống quản lý mật khẩu đặc quyền. Phục vụ cho quá trình điều tra sau này nếu thiết bị đó có sự cố
- Cung cấp công cụ giám sát, phân tích và đáp trả các hành động bất thường của quản trị viên khi thao tác với tài nguyên hệ thống.

1.5.4.8 Thống số kỹ thuật yêu cầu

Thiết kế thông số giải pháp theo yêu cầu:

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
VI	**Bản quyền giải pháp PIM/PAM**		**01**
VI.1	**Phần mềm quản lý tài khoản đặc quyền**		
Các tính năng chung			
1	Yêu cầu số lượng tài khoản được quản trị	≥ 25	
2	Cung cấp bản quyền triển khai	Cung cấp tối thiểu 01 bản quyền triển khai tại DC và có sẵn 05 bản quyền triển khai dự phòng.	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
3	Cung cấp bản quyền đầy đủ cho mục đích kiểm thử (sử dụng trong môi trường Kiểm tra & Phát triển - Test & Development)	Cung cấp 01 bộ bản quyền đầy đủ cho mục đích kiểm thử (sử dụng trong môi trường Kiểm tra & Phát triển - Test & Development)	
4	Thời hạn sử dụng bản quyền	Bản quyền không có thời hạn	
Yêu cầu kỹ thuật			
1	Có các thuật toán mã hóa	- AES-256, RSA-2048	
		- HSM integration	
		- FIPS 140-2 validated cryptography	
2	Có tính năng triển khai sẵn sàng cao	- Mô hình Clustering - Mô hình Multiple Disater Recovery sites	
3	Có các phương thức xác thực	Username and Password, LDAP, Windows authentication, RSA SecurID, Web SSO, RADIUS, PKI, SAML	
4	Có tính năng tích hợp giám sát	- Tích hợp với hệ thống SIEM	
		- Tích hợp sử dụng giao thức SNMP	
		- Tích hợp cảnh báo qua kênh Email	
5	Có tính năng quản lý và bảo vệ thông tin đặc quyền (Credential Protection and Management)	- Ngăn chặn người dùng không hợp lệ sử dụng các tài khoản đặc quyền (privileged account)	
		- Cập nhật và đồng bộ mật khẩu của tài khoản đặc quyền và các SSH key theo theo chính sách thiết lập	
		- Bảo vệ các thông tin tài khoản đặc quyền sử dụng trên các môi trường on-premise	
		- Tự động hóa các quy trình quản lý tài khoản đặc quyền, thêm mới tài khoản onboarding, phân quyền permissions granting… qua việc tích hợp với các hệ thống khác sử dụng Rest API	
6	Có tính năng kiểm soát và giám sát phiên truy cập đặc quyền (Session Isolation and Monitoring)	- Thiết lập các phiên truy cập đặc quyền riêng biệt, ghi lại hành vi thực hiện. Người dùng ko trực tiếp kết nối đến các hệ thống, giảm thiểu rủi ro lây lan mã độc từ máy tính người dùng..	
		- Cung cấp công cụ kiểm soát các phiên truy cập SSH, người dùng có thể sử dụng để kết nối đến các hệ thống hỗ trợ SSH-based.	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
		Giải pháp có khả năng kiểm soát truy cập, xác thực kép sử dụng cơ chế dual control.	
		Giải pháp có khả năng gửi báo cáo theo định kỳ.	
7	Có tính năng phân tích và phát hiện các hành vi bất thường (Privileged Analytics and Threat Detection)	- Phát hiện, cảnh báo theo thời gian thực (real-time) các hành vi nguy hại trong phiên truy cập đặc quyền của người dùng	
		- Xác định các hành vi bất thường của các tài khoản đặc quyền liên quan đến các nguy cơ tấn công vào hệ thống	
		- Sử dụng thuật toán tự học (machine learning) để tính toán các hành vi bình thường trong hệ thống và phát hiện sự thay đổi dựa trên đó	
		- Đánh giá tương quan các sự kiện ghi nhận được và đưa vào cùng một sự cố. Và trong sự cố an toàn thông tin đó có chi tiết về hệ thống ảnh hưởng, tài khoản nghi ngờ thực hiện	
8	Bảo hành và hỗ trợ kỹ thuật	≥ 24 tháng	
VI.2	**Phần mềm quản lý cơ sở dữ liệu**		
1	Cung cấp bản quyền phần mềm quản lý cơ sở dữ liệu 10 users	Đáp ứng	
2	Yêu cầu tính năng	Nhận diện các dữ liệu nhạy cảm khi truy cập Cơ sở dữ liệu	
		Tích hợp công cụ SQL Editor	
		Có tính năng Query builder	
		Cho phép so sánh các Schema/Data	
		Có công cụ thực hiện Debugger/profiler	
		Có tính năng phân tích và báo cáo về các đoạn Code (Code quality)	
		Có tính năng SQL optimization (SQL Optimizer)	
3	Thời hạn sử dụng bản quyền	Bản quyền không có thời hạn	
VI.3	**Phần mềm truy cập hệ thống từ xa**		
1	Cung cấp bản quyền phần mềm terminal truy cập hệ thống từ xa	Cấp cho 10 users phiên bản Professional	
2	Quản lý phiên truy cập	Cho phép khởi tạo phiên kết nối từ xa sử dụng các giao thức như SSH, Telnet,	

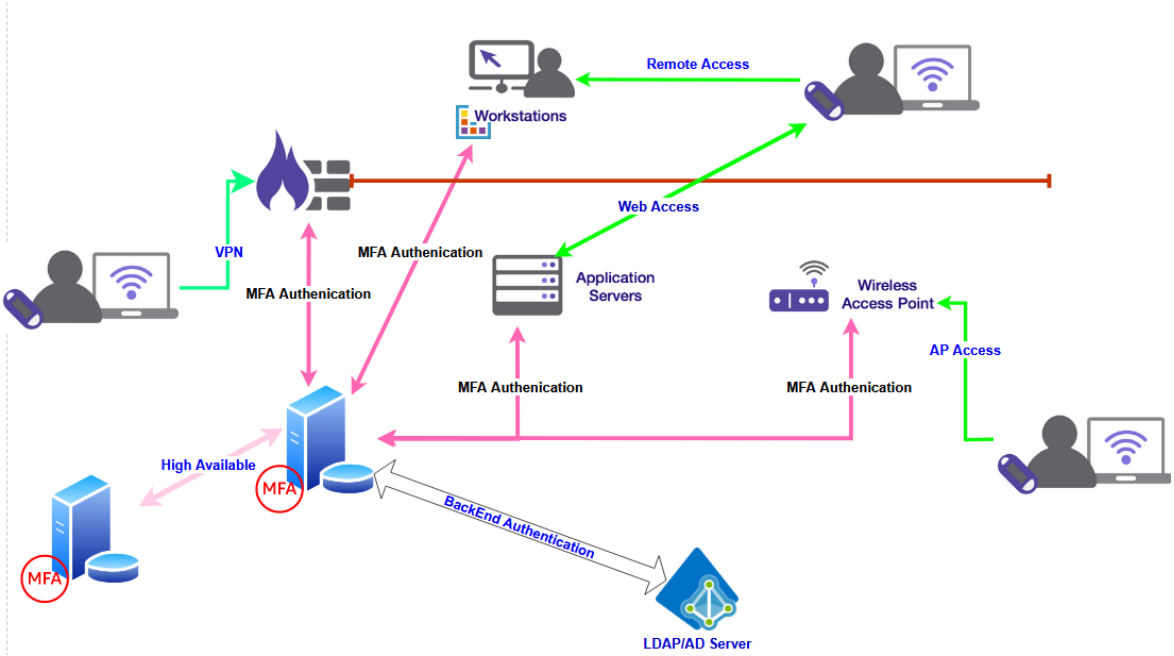
STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
		Rlogin, RDP, VNC, XDMCP, FTP, SFTP hoặc Serial… các phiên truy cập sau đó được tự động lưu và hiển thị để tiếp tục sử dụng	
3	Cung cấp giao diện truy xuất SFTP	Cung cấp giao diện truy xuất sử dụng SFTP khi sử dụng SSH để truy cập máy chủ. Cho phép thực hiện kéo và thả tập tin	
4	Hỗ trợ tính năng Multi-execution	Cho phép thực hiện cùng một câu lệnh trên nhiều máy chủ khác nhau cùng một thời điểm	
5	Hỗ trợ tính năng Remote Unix desktop (XDMCP)	Cho phép thực hiện cùng một câu lệnh trên nhiều máy chủ khác nhau cùng một thời điểm	
6	Hỗ trợ giao thức Remote Windows desktop (RDP)	Cho phép sử dụng RDP để kết nối tới máy chủ Windows	
7	Syntax highlighting in terminal	Cho phép làm nổi bật các cú pháp hoặc hiển thị theo màu sắc các từ khóa khác nhau trong cửa sổ terminal	
8	Thời hạn sử dụng bản quyền	Bản quyền không có thời hạn	
VI.4	**Bản quyền Remote Desktop Service**		
1	Cung cấp kèm bộ license Remote Desktop Service Per User CAL 25 users	Đáp ứng	
2	Yêu cầu tính năng	Cung cấp kết nối từ xa cho người dùng	
		Cho phép người dùng kết nối tới các thiết bị managed hoặc unmanaged	
		Có tính năng kết nối dưới dạng session-based hoặc virtual-machine	
3	Thời hạn sử dụng bản quyền	Bản quyền không có thời hạn	

1.5.5 Hệ thống xác thực đa yếu tố

1.5.5.1 Danh mục thiết bị lắp đặt, cài đặt

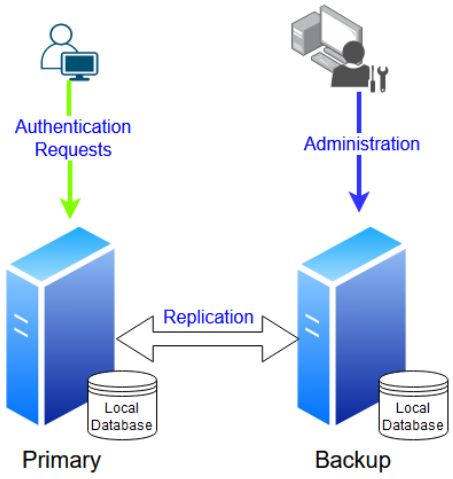
STT	TÊN HẠNG MỤC	SỐ LƯỢNG
VII	Bản quyền giải pháp 2FA	01

1.5.5.2 Mô hình thiết kế luận lý



TKTC-BV 25 Mô hình thiết kế luận lý giải pháp MFA

Mô hình gồm 2 thành phần là Primary và Secondary được cài đặt ở mô hình nâng cao. Mỗi thành phần cài ứng dụng và Database cũng được cài đặt trên bản thân máy chủ ứng dụng (Local Database).



Khi hệ thống hoạt động bình thường thì có thể cấu hình tách biệt chứ năng như trên hình vẽ:

- Máy chủ Primary sẽ chỉ xử lý các yêu cầu xác thực từ người dùng
- Máy chủ Backup sẽ được truy xuất bởi người dùng quản trị để cấu hình hay quản trị
- Hai máy chủ đồng bộ dữ liệu với nhau liên tục và đồng bộ 2 chiều.

Khi xảy ra sự cố với thành phần Primary thì hệ thống chuyển đổi dự phòng từ Primary sang Backup sẽ rất đơn giản và nhanh chóng. Hệ thống sẽ hoạt động bình thường, việc đồng bộ dữ liệu sẽ từ Backup sang Primary

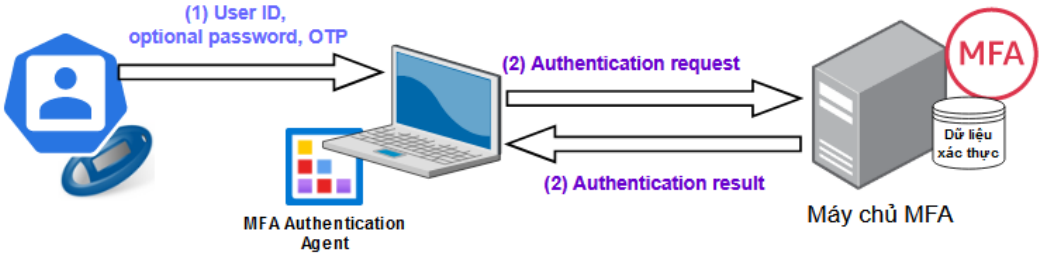
Thiết kế hệ xác thực MFA với thành phần Windows

Xác thực MFA dành cho với thành phần Windows cung cấp khả năng xác thực mạnh mẽ khi đăng nhập vào Microsoft Windows.Với kiểu xác thực này, người dùng đăng nhập vào Microsoft Windows bằng cách sử dụng thông tin sau:

- ID người dùng (ID xác thực với hệ thống MFA)
- Mật khẩu (mật khẩu xác thực với hệ thống MFA)
- Mật khẩu một lần được tạo bởi người xác thực (OTP – One Time Password)
- Mã PIN máy chủ

Thông tin xác thực MFA được gửi và xác thực trực tiếp trên hệ thống xác thực tập trung MFA thông qua MFA Authentication Agent. Giải pháp hỗ trợ xác thực trực tuyến Online khi máy chủ Client có kết nói tới được hệ thống xác thực tập trung MFA hoặc sử dụng dữ liệu xác thực ngoại tuyến Offline (OAD). Việc xác thực MFA cho đăng nhập Windows có thể được cấu hình song song cả trực tuyến và ngoại tuyến nhằm đảm bảo người dùng vẫn xác thực được trong trường hợp mất kết nối tới cụm xác thực tập trung. Việc xác thực MFA hoàn toàn trong suốt đối với người dùng , người dùng chỉ cần thực hiện đăng nhập với thông tin đăng nhập MFA mà không dùng mật khẩu Window như trước

Phương thức xác thực Online



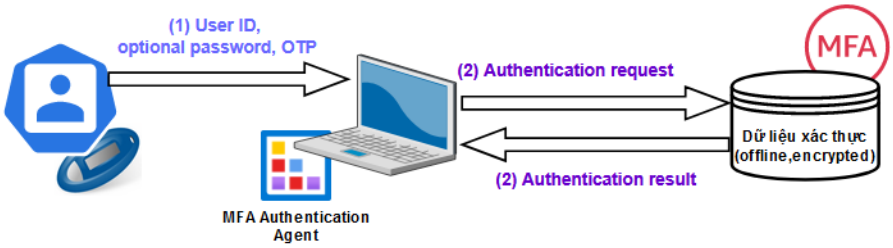
Bước 1: Người dùng gửi thông tin xác thực (User ID, Password, OTP…) thông qua MFA Authentication Agent

Bước 2: Agent gửi yêu cầu xác thực tới hệ thống Máy chủ xác thực MFA

Bước 3: Máy chủ xử lý yêu cầu xác thực thông qua việc so sánh với dữ liệu xác thực người dùng cung cấp với Dữ liệu xác thực hoặc hệ thống xác thực BackEnd

Phương thức xác thức Offline

Xác thực ngoai tuyến (Offline) xảy ra khi người dùng xác thực với Microsoft Windows bằng thông tin xác thực MFA để đăng nhập Windows khi máy Client không kết nối với mạng hoặc không thể thiết lập kết nối với máy chủ MFA. Xác thực được thực hiện dựa trên dữ liệu xác thực ngoại tuyến (được lưu trữ và mã hóa cục bộ) (OAD)



Dữ liệu xác thực ngoại tuyến được tạo bởi Máy chủ xác thực IDENTIKEY trong quá trình xác thực trực tuyến thành công. Dữ liệu được giới hạn trong một khoảng thời gian cụ thể (dựa trên thời gian) hoặc số lần xác thực (dựa trên sự kiện). Cái này yêu cầu khách hàng thực hiện xác thực trực tuyến một cách thường xuyên

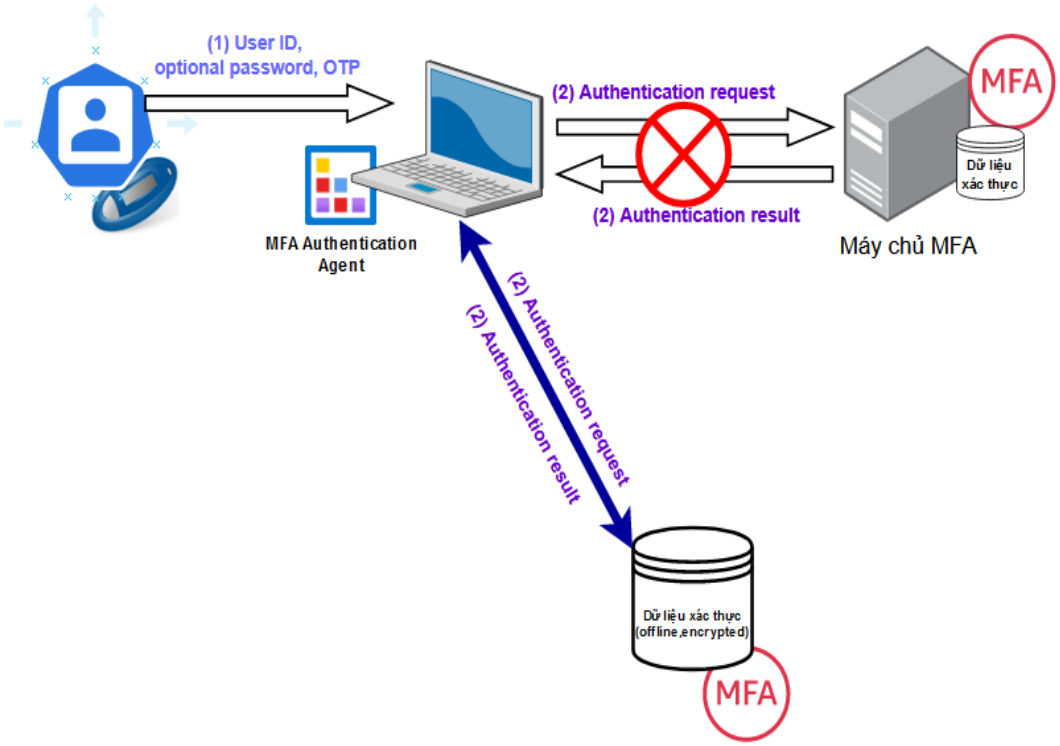
User ID, password và OTP được xác thực dựa trên dữ liệu ngoại tuyến. Dữ liệu ngoại tuyến được sinh ra sau một số lần xác thực trực tuyến thành công, dữ liệu sinh ra được mã hóa lưu trong một khoảng thời gian được cấu hình thông qua giao diện quản trị hệ thống.

Cấu hình phương án xác thực dự phòng

Để đảm bảo phương án dự phòng trong trường hợp không máy chủ Client mất kết nối tới máy chủ xác thực MFA sẽ bật song song tính năng xác thực ngoại tuyến và trực tuyến.

Khi máy chủ Client có kết nối tới hệ thống MFA người dùng xác thực trực tuyến và sinh dữ liệu xác thực ngoại tuyến sau một số lần xác thực trực tuyến được cấu hình sẵn

Khi máy chủ Client không có kết nối tới hệ thống xác thực MFA thì người dùng xác với dữ liệu xác thực ngoại tuyến như hình dưới.



Static password randomization

Nếu tính năng ngẫu nhiên hóa mật khẩu được bật, Máy chủ xác thực MFA sẽ thay thế mật khẩu Windows tĩnh bằng mật khẩu mật khẩu được tạo ngẫu nhiên cho mỗi lần đăng nhập, đồng thời tuân thủ các quy tắc với định dạng nghiêm ngặt. Chọn ngẫu nhiên mật khẩu diễn ra một cách trong suốt đối với người dùng, họ chỉ cần nhập ID người dùng và OTP để xác thực.

Khi tính năng được bật và đưa vào quy trình vận hành, người dùng sẽ không thể đăng nhập được vào các máy chưa được cài MFA Authentication Agent.

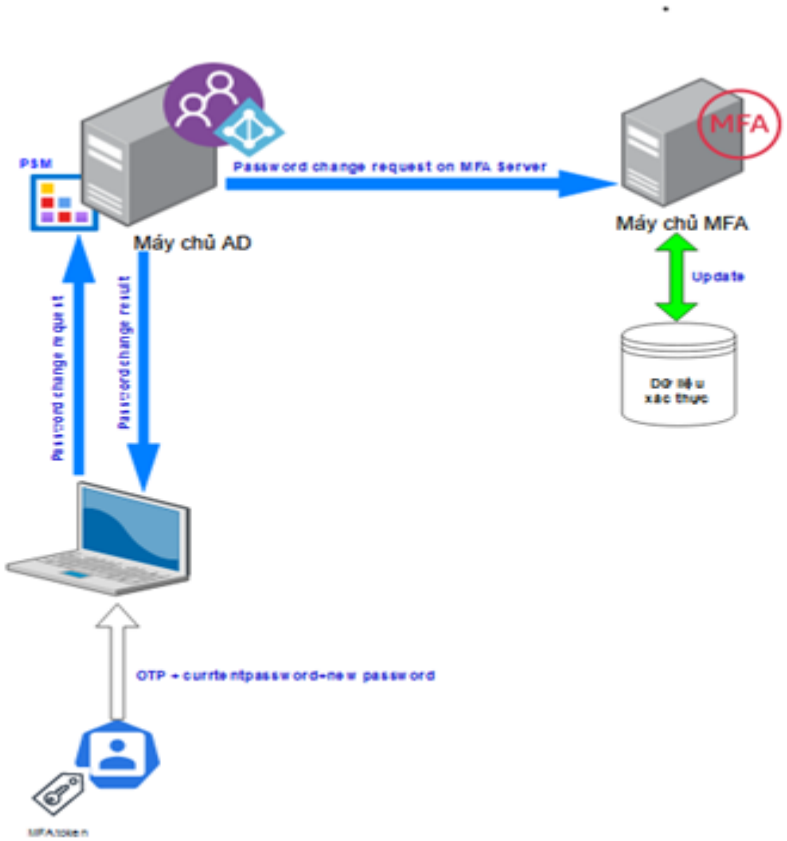
Sau khi xác thực thành công đối với Máy chủ xác thực MFA, mật khẩu ngẫu ngiên sẽ thay thế mật khẩu tĩnh được sử dụng để xác thực máy khách Windows Domain bằng mật khẩu mới được tạo. Mật khẩu này thì User sẽ không biết được và bắt buộc.
Để bật tính năng xác thực static password randomization thì cần đảm bảo:

- Xác thực Back-end với LDAP hoặc Active Directory.
- Tính năng ngẫu nhiên hóa mật khẩu được kích hoạt trong Policy

Static password synchronization

Tính năng Static password synchronization (PSM) tự động cập nhật mật khẩu Windows đã thay đổi trên máy chủ xác thực MFA. Giải pháp cài đặt trên bộ Agent PSM trên máy chủ Active Directory. Mật khẩu Windows mới sẽ được ánh xạ dưới dạng mật khẩu tĩnh trên hệ thống xác thực MFA

Khi mật khẩu Windows được thay đổi, nó sẽ được cập nhật trên AD. PSM được cài đặt trên Active Directory kiểm tra kết nối tới hệ thống xác thực MFA trước khi thực hiện quy trình cập nhật dữ liệu xác thực trên hệ thống MFA.



1.5.5.3 Phân bổ tài nguyên ảo hoá

STT	Máy chủ	Yêu cầu
1	Primary Authentication	4 Core
		8 GB RAM
		600 GB
2	Backup Authentication	4 Core
		8 GB RAM

STT	Máy chủ	Yêu cầu
		600 GB

1.5.5.4 Thông số cài đặt và cấu hình

Thông số	Giá trị
Windows Operating System	Windows Server 2016/2019
Virtualization Platform	Vmware ESXI Server
Authentication Server Primary	10.24. x.x
Authentication Server Backup	10.24. x.x
Netmask	255.255.255.0
Gateway	10.24.x.1
NTP Server	10.240. x.x 10.240. x.x 10.240. x.x

1.5.5.5 Chỉ dẫn biện pháp triển khai

Chi tiết về cách thức thực hiện được thể hiện ở phụ lục 2 "Chỉ dẫn triển khai chi tiết"

1.5.5.6 Kết quả đạt được sau khi hệ thống đi vào hoạt động

Giải pháp xác thực hai yếu tố đảm bảo xác thực 2 lớp an toàn việc truy cập/sử dụng các ứng dụng tại các máy tính trạm và máy tính chủ đều được kiểm soát. Giúp giảm thiểu rủi ro hacker, mã độc lấy cắp được mật khẩu của người sử dụng thông qua các con đường khác nhau.

Sau khi giải pháp được triển khai, cán bộ quản trị và vận hành hệ thống ngoài việc cung cấp một yếu tố là mật khẩu thì còn cần có một mã sử dụng một lần được cung cấp từ hệ thống 2FA thông qua các hình thức như tin nhắn văn bản, thông bao được gửi đến số điện thoại, thư điện tử để có thể được xác thực thành công truy cập vào hệ thống. Do vậy, kể cả khi các hacker có được mật khẩu thì cũng không thể truy cập vào hệ thống.

1.5.5.7 Thông số kỹ thuật yêu cầu

Thiết kế thông số giải pháp theo yêu cầu:

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
VII	**Bản quyền giải pháp 2FA**		**01**
1	Số lượng người dùng được quản lý	≥ 1000 user	
2	Xác thực qua token	Khả năng xác thực qua token phần cứng và khả năng cung cấp mã mới mỗi 60 giây	
		Token phần cứng hỗ trợ thuật toán AES-128 và chống giả mạo	
		Khả năng tích hợp xác thực với hệ thống VPN và ứng dụng web	
		Cơ chế xác thực dựa trên rủi ro	
		Khả năng tính điểm rủi ro động, theo thời gian thực kết hợp với yếu tố ngữ cảnh	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
3	Xác thực nâng cao	Có thành phần quản trị tập trung	
		Khả năng hiển thị cảnh báo với các chi tiết về sự kiện như thời gian, địa chỉ IP, người dùng, vị trí địa lý, địa chỉ email...	
		Khả năng triển khai theo mô hình tại chỗ	
4	Quản trị	Khả năng tích hợp với nhiều thành phần, giải pháp của bên thứ 3 như truy cập từ xa, truy cập đặc quyền, đám máy và ứng dụng đám mây, kiểm soát truy cập...	
5	Triển khai	- Khả năng hỗ trợ LDAP, RADIUS, SAML, Trusted Headers… - Thiết kế triển khai đảm bảo khả năng dự phòng	
6	Bảo hành và hỗ trợ kỹ thuật	≥ 24 tháng	

1.5.6 Hệ thống quản lý thông tin và sự kiện an ninh

1.5.6.1 Danh mục thiết bị lắp đặt, cài đặt

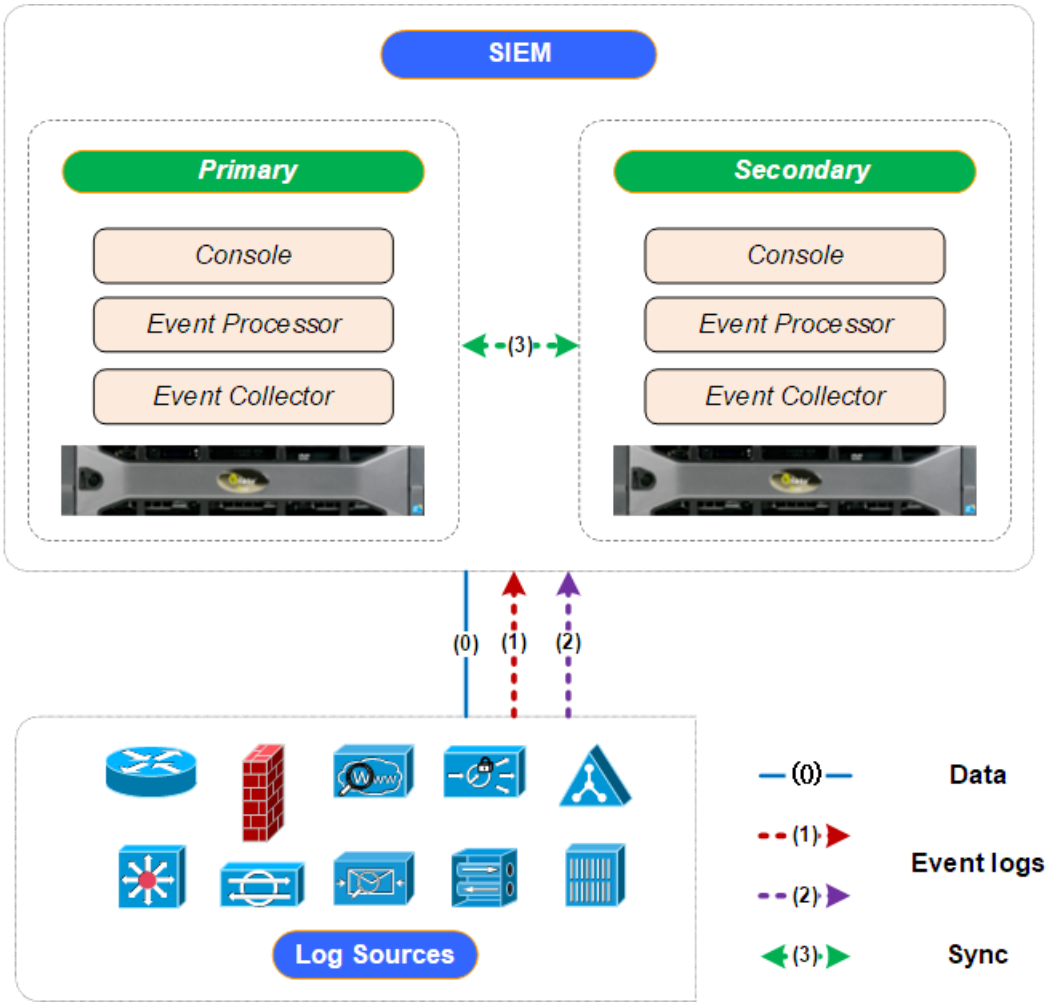
STT	TÊN HẠNG MỤC	SỐ LƯỢNG
VIII	Bản quyền giải pháp SIEM	01

1.5.6.2 Mô hình thiết kế luận lý tại TTĐK

Mô hình hệ thống SIEM bao gồm 02 thiết bị hoạt động ở chế độ dự phòng (HA), về mặt module hóa sẽ có 03 thành phần Collector, Processor và Console được cài đặt tích hợp trên cùng một thành phần gọi là SIEM All In One.

- **SIEM Event Collector**: có nhiệm vụ thu thập thông tin events, tiền xử lý chuẩn hóa và gửi về Processor để phân tích, và lưu trữ. Việc thu thập event logs được thực hiện bởi thành phần Event Collector thông qua hai cơ chế Push và Pull:
    - Cơ chế Push: dữ liệu event logs sẽ được đẩy trực tiếp từ các thiết bị thông qua giao thức Syslog, SNMP, …
    - Cơ chế Pull: dữ liệu event logs sẽ được Event Collector kết nối đến các thiết bị để lấy load về thông qua các giao thức FTP, SFTP, ..
    - Đối với mỗi chủng loại thiết bị/sản phẩm, SIEM sẽ có phương án tích hợp riêng. Event logs sau khi được thu thập sẽ được phân tích cú pháp, chuẩn hóa, tổng hợp, lọc, .. tại Event Collector trước khi đến Module lưu trữ và phân tích Processor.

- **SIEM Event Processor:** có nhiệm vụ nhận thông tin từ Collector kết hợp các thông tin từ các thành phần khác như Threat Intelligence để xử lý theo các chính sách đã thiết lập và lưu trữ sự kiện.
- **SIEM Console:** có nhiệm vụ quản lý và phát hiện sự cố theo các chính sách đã thiết lập. Đồng thời hỗ trợ cảnh báo, báo cáo, điều tra xử lý sự cố an ninh thông tin trong hệ thống.



TKTC-BV 26 Mô hình thiết kế luận lý giải pháp SIEM

Phân tích mô hình luồng dữ liệu bao gồm các loại sau:

- (0): mô tả các kết nối IP/Data từ các thành phần bên ngoài tới hệ thống.
- (1) và (2): mô tả kênh truyền sự kiện logs từ các Log Sources đến SIEM Console để xử lý, lưu trữ, phân tích tương quan nhằm tìm ra các dấu hiệu bất thường.
- (3): kênh đồng bộ (Sync) dữ liệu và cấu hình giữa 02 thiết bị SIEM HA chạy ở chế độ dự phòng

Cặp máy chủ SIEM HA khi hoạt động sẽ thu nhận dữ liệu log và flow từ các hệ thống đích (gồm các thiết bị mạng, thiết bị bảo mật, hệ điều hành, cơ sở dữ liệu, ứng dụng…). Trên SIEM, dữ liệu thu thập được sẽ trải qua các quá trình:

- ***Bóc tách***: các trường thông tin bên trong nội dung dữ liệu sẽ được bóc tách thành các trường để phục vụ tìm kiếm và phân tích

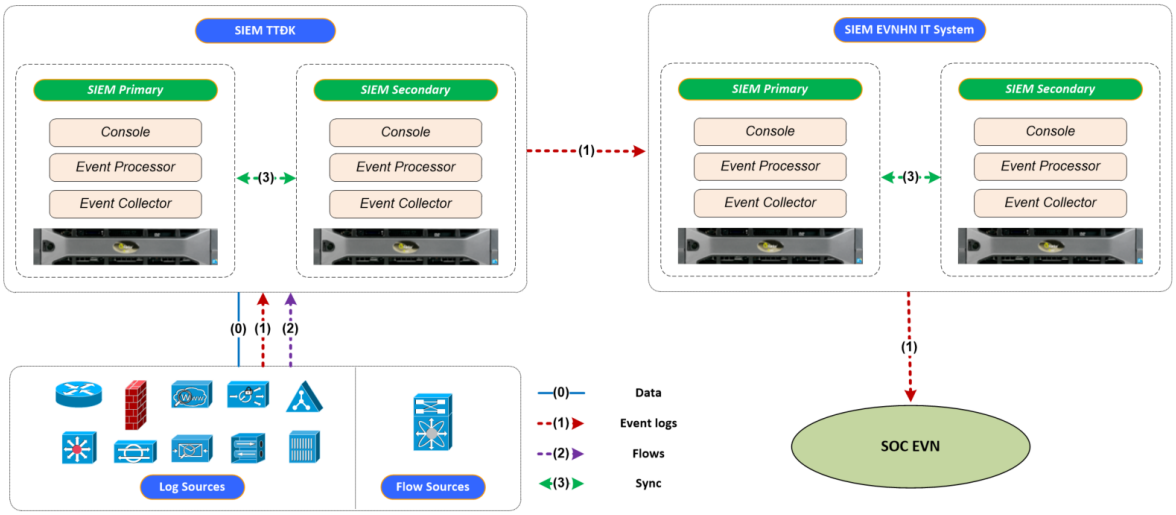
- ***Chuẩn hóa***: các trường thông tin ở những định dạng và ký hiệu khác nhau sẽ được đưa về một khuôn dạng chuẩn duy nhất, nhờ vậy dữ liệu có thể được tương quan đối sánh với nhau
- ***Phân tích***: với những thông tin nhận được, SIEM tiến hành so khớp với bộ chính sách phân tích tương quan để tìm ra những bất thường trong các hoạt động của mạng và đưa ra cảnh báo để người giám sát kịp thời xử lý
- ***Lưu trữ***: cuối cùng, dữ liệu và thông tin sẽ được lưu lại để phục vụ tìm kiếm, điều tra, phân tích khi cần

Danh mục các kết nối mà hệ thống yêu cầu:

STT	Nguồn	Đích	Dịch vụ	Ghi chú
Thu thập dữ liệu				
1	Log Sources	SIEM	Syslog/514	Thu thập dữ liệu sự kiện theo cơ chế Push
2	Log Sources	SIEM	TCP 8413	Kết nối quản trị agent

1.5.6.3 Mô hình thiết kế giải pháp tích hợp với hệ thống SOC EVN

Dưới đây là mô hình giải pháp đề xuất cho việc chia sẻ thông tin bảo mật với hệ thống SOC của EVN:



Mô tả:

- Hệ thống SIEM tại TTĐK dự kiến đầu tư trong dự án này sẽ đóng vai trò thu thập, lưu trữ, phân tích nhật ký hệ thống OT để đưa ra các cảnh báo về các mối đe dọa an ninh mạng.
- Ngoài ra, để liền mạch và thông suốt cho việc đảm bảo an toàn thông tin cho toàn bộ hệ thống ngành dọc của ngành điện, đề xuất sẽ lựa chọn các thông tin, nhật ký, sự kiện tại hệ thống OT sẽ được đẩy qua hệ thống SIEM của EVNHN thông qua đường kết nối đến hệ thống IT và sử dụng giao thức syslog, qua cổng một chiều Data Diode.
- Hệ thống SIEM của EVNHN đã được tích hợp sẵn với hệ thống SOC của EVN vậy nên chỉ cần cấu hình thêm để chuyển tiếp các thông tin từ hệ thống SIEM của OT sang mà không cần thay đổi hoặc bổ sung thêm giải pháp nào khác.

1.5.6.4 Phân bổ tài nguyên ảo hoá

Hệ thống yêu cầu tài nguyên như sau:

Thông số	Giá trị	Ghi chú
SIEM Primary		
CPU	32 Cores	
RAM	64 GB	
HDD 01 (OS)	600 GB	
HDD 02 (Data)	8.59 TB	
NIC	2 NIC	
SIEM Secondary		
CPU	32 Cores	
RAM	64 GB	
HDD 01 (OS)	600 GB	
HDD 02 (Data)	8.59 TB	
NIC	2 NIC	

1.5.6.5 Thông số cài đặt và cấu hình

Quy hoạch địa chỉ IP cho các thiết bị và thành phần được trang bị trong dự án như sau:

Hệ thống	Thông tin cấu hình	Giá trị
SIEM Primary	Hostname:	siem-01.evnhanoi.vn
	Domain:	evnhanoi.vn
	Management IP:	10.24.x.x
	Management Virtual IP:	10.24. x.x
	Management Gateway:	10.24. x.x
	NTP Server	10.240. x.x 10.240. x.x 10.240. x.x
SIEM Secondary	Hostname:	siem-01.evnhanoi.vn
	Domain:	evnhanoi.vn
	Management IP:	10.24. x.x
	Management Gateway:	10.24. x.x

1.5.6.6 Thiết kế thu thập dữ liệu

Việc thu thập event logs được thực hiện bởi thành phần Collector trên SIEM thông qua hai cơ chế Push và Pull:

- Cơ chế Push: dữ liệu event logs sẽ được đẩy trực tiếp từ các thiết bị nguồn
- Cơ chế Pull: dữ liệu event logs sẽ được Event Collector kết nối đến các thiết bị để lấy event log về

Hệ thống cần thu thập	Cơ chế	Phương thức	Ghi chú
Máy chủ Windows	Push	Agent	
Máy chủ Linux	Push	Syslog	
Thiết bị chuyển mạch	Push	Syslog	
Hệ thống Tường lửa	Push	Syslog	

Hệ thống cần thu thập	Cơ chế	Phương thức	Ghi chú
Hệ thống Bảo vệ điểm cuối	Push	Agent hoặc Syslog	
Hệ thống Quản lý tài khoản đặc quyền	Push	Syslog	
Hệ thống Xác thực đa yếu tố	Push	Syslog	

1.5.6.7 Thiết kế quản trị hệ thống

Quản lý nguồn log

Log Source Group (nhóm thiết bị) được tạo ra để quản lý event tập trung dành cho từng nhóm quản trị. Dựa trên những thông tin đã được filter đó, các quản trị viên (Administrator) có thể tiến hành đánh giá tổng quan, rồi tập trung phân tích sâu vào các lỗi, và chi tiết đến từng Log Sources.

- Phân nhóm Log Sources sẽ được áp dụng:

STT	Name	User/Group	Description	Note
1	Network	admin	Theo dõi log của các thiết bị mạng	
2	OS	admin	Theo dõi log OS của các máy chủ	
3	Security	admin	Theo dõi log của các thiết bị bảo mật	
4	Other	admin	Theo dõi log của các thiết bị chưa được phân nhóm	

- Quy tắc đặt tên log source:

  <Tên nhóm>.<Loại thiết bị>.<Tên nguồn log/hệ thống> @ <IP> @ <Hostname>

Thiết kế quản trị phân quyền và giám sát người dùng

- Các user quản trị trên hệ thống sẽ được tạo và phân quyền trên giao diện quản trị của hệ thống SIEM
- Phân nhóm và phân quyền người quản trị: SIEM cho phép việc tạo ra các User và phân quyền truy cập, cấu hình các thành phần hệ thống theo user role và security profile:
  - User Role: phân quyền thực hiện các menu thao tác quản trị
  - Security Profile: phân quyền đối với view logs từng nhóm thiết bị

STT	User/Group	Admin Permission	Note
1	admin	Được theo dõi logs của tất cả các Log Sources hệ thống Được hiển thị tất cả các Tab	
2	network-admin	Được theo dõi logs của các Log Sources của mình quản trị Được hiển thị Tab Log Activity, Reports	
3	system-admin	Được theo dõi logs của các Log Sources của mình quản trị Được hiển thị Tab Log Activity và Reports	

Thiết kế lưu trữ, sao lưu và phục hồi

- Thiết kế lưu trữ (on-line)

- Dữ liệu event logs được SIEM lưu trữ trong các Retention buckets, ở đó cho phép thực hiện các thao tác:
  - Giới hạn thời gian lưu trữ (Retention)
  - Xóa dữ liệu (Delete Policy)
- Chính sách lưu trữ đề xuất:

STT	Name	Retention	Delete Policy	Filter
	Default	12 months	Immediately after retention period ends	None

- Dữ liệu về sự cố (Offenses) được lưu trữ với thời gian xác định bởi thông số Offense Retention Period: 30 days (default).
  - Chính sách lưu trữ đề xuất: Offense Retention Period: 1 months
- Thiết kế sao lưu
  - Cấu hình hệ thống được SIEM cấu hình backup, với thời gian mặc định là nightly. Cấu hình backup hàng đêm là những cấu hình thay đổi phát sinh trong ngày hôm đó:
    - Backup hàng ngày (nightly)
    - Duy trì các bản backup (retention)
  - Chính sách backup đề xuất:

STT	Name	Time	Retention	Comment
1	Configuration	Midnight	7 days	

- Thiết kế khôi phục hệ thống
  - Khôi phục cấu hình hệ thống từ file cấu hình đã backup
  - Để khôi phục các cấu hình về Log Sources, Rules, Reports, Saved, Searches … cũng như các chính sách khác. Với việc copy file cấu hình gần nhất lên thư mục /store/backup, refresh để hệ thống nhận ra file cấu hình.

1.5.6.8 Chính sách an ninh

Chính sách giám sát là yếu tố cốt lõi của hệ thống SIEM, các chính sách này sẽ được thiết kế theo các tiêu chí:

- Phát hiện hành vi vi phạm các chính sách an toàn, an ninh thông tin được quy định trong các văn bản của EVNHANOI.
- Phát hiện các hành vi mất an toàn thông tin, các nguy cơ hệ thống bị tấn công, khai thác, phá hoại hay thất thoát dữ liệu.

STT	Nhóm chính sách	Chính sách	Tiêu chí cảnh bảo	Trường thông tin yêu cầu	Hành động
1	Giám sát Firewall	Firewall nhiều lần ngăn chặn truy cập vào hệ thống	Trong vòng 5 phút Firewall ngăn chặn quá 500 lần truy cập vào một hệ thống đích từ một địa chỉ IP nguồn	Source IP Event Name	Thông báo cho owner hệ thống. Cảnh báo trên giao diện quản trị, tiếp tục thu thập thông tin và giám sát hoạt động hệ thống đích
2		Scan cổng TCP	Trên 50 lần scan cổng TCP trong vòng 2 phút, scan nhiều cổng trên một địa chỉ IP đích	Destination Port Destination IP	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo
3			Trên 50 lần scan cổng TCP trong vòng 2 phút, scan một cổng trên nhiều địa chỉ IP đích	Destination Port Destination IP	
4		Truy cập thành công/ không thành công vào thiết bị	Khi truy cập thành công và khi trong vòng 5 phút có quá 2 lần truy cập không thành công từ một hoặc nhiều địa chỉ IP	Source IP Event Name	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo
5	Giám sát thiết bị mạng và an ninh	Sự kiện critical và lỗi của thiết bị mạng	Khi phát hiện lỗi và các sự kiện critical	Event Name Log Source Source IP	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo

STT	Nhóm chính sách	Chính sách	Tiêu chí cảnh bảo	Trường thông tin yêu cầu	Hành động
6		Thay đổi cấu hình thiết bị mạng	Khi phát hiện hành vi thay đổi	Event Name Log Source Source IP	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo
7		Truy cập thành công/ không thành công vào thiết bị mạng	Khi phát hiện truy cập thành công; Khi trong phòng 5 phút phát hiện quá 2 lần truy cập không thành công từ 1 hoặc nhiều địa chỉ IP khác nhau	Event Name Source IP	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo
8		Danh sách tổng hợp về nguồn và đích của tấn công mạng		Source IP Destination IP	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo
9		Cảnh báo của hệ thống IPS / IDS	Khi phát hiện lỗi và có cảnh báo từ hệ thống IPS/IDS	Event Name	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo
10		Cảnh báo về xâm nhập trái phép (Phát hiện ra các kết nối bất thường)	Cảnh báo khi một IP / Host nào đó bị Alert / Drop / Reject / Deny / Login failed ≥ 10 events sau đó có Accept or successful event	Event Name	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo
11		Cảnh báo về Host bị điều khiển, kết nối trái phép… (Phát hiện các địa	Cảnh báo khi có IP nào đó kết nối đến IP bên ngoài nằm trong danh sách "black listed". Hoặc khi có ≥ 5 drops events hoặc 1 Accept/Allow event to	Event Name Source IP Destination IP	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo

STT	Nhóm chính sách	Chính sách	Tiêu chí cảnh bảo	Trường thông tin yêu cầu	Hành động
		chỉ bên trong kết nối đến các địa chỉ đen "black listed". Phát hiện các địa chỉ cố gắng kết nối đến các địa chỉ đen thậm chí bị chặn (ví dụ: host cố gắng kết nối đến C&C server)	any known attacker (ví dụ: C&C IP address)		
12	Phần mềm chống virus/ mã độc hại	Các lỗi của của PM Antivirus		Event Name	Hiện thông tin trên giao diện quản trị
13		Báo cáo tổng hợp cập nhật virus signature của PM Antivirus		Event Name AV Signature	Hiện thông tin trên giao diện quản trị
14		Báo cáo tổng hợp hoạt động của virus/ mã độc hại		Event Name AV Signature Source IP	Hiện thông tin trên giao diện quản trị
15		Thay đổi cấu hình, chính sách, user/group trên PM Antivirus	Khi phát hiện sự kiện thay đổi cấu hình, chính sách, user/group trên PM Antivirus	Event Name Username	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo

STT	Nhóm chính sách	Chính sách	Tiêu chí cảnh bảo	Trường thông tin yêu cầu	Hành động
16		Cảnh báo khi phát hiện bùng nổ virus, mã độc…	Cảnh báo khi ≥ 5 Host / IP bị phát hiện cùng một virus, mã độc trong 1 ngày (hoặc vài giờ)	Event Name Source IP	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo
17	Giám sát người quản trị, người dùng đặc quyền trên các hệ thống	Truy cập thành công/ không thành công vào các hệ thống (local và remote)	Khi phát hiện người dùng đặc quyền truy cập thành công vào hệ thống; Khi trong phòng 5 phút phát hiện quá 2 lần truy cập không thành công từ 1 hoặc nhiều địa chỉ IP khác nhau	Event Name Username Source IP	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo
18		Hoạt động quản trị của người dùng đặc quyền (thay đổi chính sách trên hệ thống, thay đổi tài khoản hoặc quyền của người dùng v.v.)	Khi có sự thay đổi; Khi phiên làm việc của người dùng đặc quyền được khởi tạo hoặc đóng	Event Name Username Source IP	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo
19		Truy cập hoặc thay đổi nhật ký (log) của người dùng đặc quyền	Khi phát hiện hành vi truy cập hoặc thay đổi	Event Name Username Source IP	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo
20	Bảo vệ thông tin, cơ sở dữ liệu	Truy cập thành công/ không thành	Khi phát hiện hành vi của người dùng; Khi trong vòng 5 phút phát hiện quá 2	Event Name Username Source IP	Cảnh báo trên giao diện quản trị, đưa vào Danh

STT	Nhóm chính sách	Chính sách	Tiêu chí cảnh bảo	Trường thông tin yêu cầu	Hành động
		công vào CSDL, hệ thống CSDL	lần truy cập không thành công từ một hoặc nhiều địa chỉ IP khác nhau		mục sự kiện theo dõi để xem xét và báo cáo
21		Thay đổi cấu hình CSDL, hệ thống CSDL	Khi có sự thay đổi bởi người quản trị, người dùng đặc quyền	Event Name Username Source IP	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo
22		Lỗi và cảnh báo của CSDL, hệ thống CSDL	Khi có lỗi hoặc cảnh báo trên hệ thống	Event Name	Cảnh báo trên giao diện quản trị, đưa vào Danh mục sự kiện theo dõi để xem xét và báo cáo

1.5.6.9 Giao diện giám sát

Dưới đây là một số tiêu chí và thông số chính được đề xuất cho các màn hình giám sát phục vụ cho việc theo dõi thời gian thực

Categories	Dashboard Name	Property
1. Log Sources		
	Log Sources Status	Log Source Name Log Source Status Last Event Timestamp
2. Threat Intelligence		
	Vulnerability Management	Asset name Vulnerability ID Last seen
	Threat Model: Campaign, Actor, TTPs	Top Campaign Name Top Actor Top TTP
3. Incidents		
	Security Incidents	Top Severe Incidents Top Incident Sources
4. System Availability		
	System Status	Current EPS Failed Services Critical disk partitions free space
	Application/Database Status	Last Event Seen Top Authentication Success/Failure Unauthorized Access

1.5.6.10 Chỉ dẫn biện pháp triển khai

Chi tiết về cách thức thực hiện được thể hiện ở phụ lục 2 "Chỉ dẫn triển khai chi tiết"

1.5.6.11Kết quả đạt được sau khi hệ thống đi vào hoạt động

Sau khi hệ thống SIEM được triển khai thành công và đi vào hoạt động theo đúng thiết kế, sẽ mang lại các hiệu quả và lợi ích như sau:

- **Mang lại khả năng hiển thị tập trung và toàn diện**: có thể tổng hợp dữ liệu từ rất nhiều nguồn khác nhau và từ nhiều hãng khác nhau sau đó chuẩn hoá lại theo 1 định dạng chung để tiện cho việc đánh giá và phân tích cũng như giúp mở rộng hết khả năng làm việc và phối hợp của các sản phẩm giải pháp khác mà doanh nghiệp đang sử dụng.
- **Tự động hóa giúp nhanh chóng phát hiện các mối đe dọa**: Hệ thống SIEM tự động phân tích và tương quan các hoạt động tới từ nhiều nguồn khác nhau để vẽ ra bức tranh toàn cảnh, từ các mảnh vụn rời rạc sẽ xác định ra được kịch bản tấn công cho các giải pháp khác và rồi các giải pháp đó sẽ đưa tới cách xử lý chính xác hơn. Ngoài ra việc QRadar có sẵn hàng trăm use cases, thuật toán phát hiện

sự bất thường và các rules sẽ giúp phát hiện known và unknown malware ở mức real-time cũng như phân loại chính xác các loại hình tấn công.

- **Xác định hoạt động bất thường của mạng, người dùng và ứng dụng**: các tấn công ngày càng phức tạp nên cần phải nhận ra sớm từ những sự bất thường nhỏ nhất tới từ hành vi của mạng, user hay hệ thống, có như vậy thì hệ thống của doanh nghiệp mới đảm bảo được an toàn trước khi tấn công kịp xảy ra.
- **Quản lý tuân thủ tốt hơn với bộ quy tắc và báo cáo có sẵn**: SIEM mang lại tính minh bạch, khả năng giám sát và đo lường tối quan trọng đối với sự thành công trong việc quản lý và báo cáo về tuân thủ. Giải pháp vừa có thể cung cấp số liệu đầy đủ cho việc báo cáo rủi ro CNTT đối với kiểm toán lại vừa có thể xử lý hàng nghìn báo cáo tuân thủ một cách tự động hóa và chuyên nghiệp.
- **Triển khai đa dạng và dễ dàng mở rộng**: SIEM có đa dạng các loại hình triển khai phù hợp với quy mô của doanh nghiệp. Ngoài ra khi cần nâng cấp về sức mạnh của thiết bị thì chỉ cần lấy thêm các module con chứ không cần thay đổi trên thiết bị đã có sẵn.

1.5.6.12 Tính toán thông số kỹ thuật

Thông thường, khi sizing 1 hệ thống, ta có thể theo nhiều phương pháp khác nhau, có thể dựa trên số liệu về traffic thực tế, dựa trên số liệu băng thông đường truyền, số sự kiện xảy ra trong 1 thời gian hoặc dựa trên bài toán kinh nghiệm khi triển khai cho 1 môi trường nhỏ, vừa, lớn.

Để xác định được tổng số sự kiện bảo mật có trong 1 site, ta dựa trên thống kê cho bài toán thống kê liên quan đến các sự kiện bảo mật như sau.

Basic EPS Estimator				
	Device Type	**Qty.**	**Factor**	**Total**
Events	AD/Auth, DHCP, DNS, ESX	1	25	25
	Web and Mail Servers, O365		10	-
	Windows General Purpose Servers	122	2	244
	Linux/Unix General Purpose Servers	8	0.5	4
	Antivirus, Anti-Malware Servers	1	20	20
	Database Servers		1	-
	Proxy Servers, Edge/Small Firewalls	60	25	1,500
	Core/Large Firewalls	4	150	600
	IDS, IPS, VPN, WAF, DAM, DLP, LB		5	-
	Routers, Switches, Wireless	332	0.25	83
	EDR, AWS, etc. (indicate event rate)		0.05	-
	Other? (Indicate event rate)		0.05	-
	Other? (Indicate event rate)		0.05	-
	On-Line Log Retention Req. (Mo)	3	**Est. Peak EPS**	**2,476**

Trong đó, dung lượng dữ liệu được thống kê như sau:

RAW Event ~ 700 bytes

Retention	**Retention Requirements - Assuming 30 day Average = 1/3 Peak**			
	Avg. Log Size (Bytes)	**700**	**Log Disk Space (TB)**	**0.00**

Theo khảo sát với EVNHN OT có số lượng thiết bị như sau, để đảm bảo năng lực hệ thống đáp ứng, ta lấy số liệu max của từng dòng theo bảng trên.

Basic EPS Estimator				
	Device Type	Qty.	Factor	Total
Events	AD/Auth, DHCP, DNS, ESX	1	25	25
	Web and Mail Servers, O365		10	-
	Windows General Purpose Servers	122	2	244
	Linux/Unix General Purpose Servers	8	0.5	4
	Antivirus, Anti-Malware Servers	1	20	20
	Database Servers		1	-
	Proxy Servers, Edge/Small Firewalls	60	25	1,500
	Core/Large Firewalls	4	150	600
	IDS, IPS, VPN, WAF, DAM, DLP, LB		5	-
	Routers, Switches, Wireless	332	0.25	83
	EDR, AWS, etc. (indicate event rate)		0.05	-
	Other? (Indicate event rate)		0.05	-
	Other? (Indicate event rate)		0.05	-
	On-Line Log Retention Req. (Mo)	3	**Est. Peak EPS**	**2,476**

Tính toán dung lượng lưu trữ log trong 12 tháng:

	On-Line Log Retention Req. (Mo)	12	**Est. Peak EPS**	**2,476**
Retention	**Retention Requirements - Assuming 30 day Average = 1/3 Peak**			
	Avg. Log Size (Bytes)	**700**	**Log Disk Space (TB)**	**8.59**
Growth	**Growth Planning Considerations - Appliance support = 5 Years from date of purchase**			
	Anticipated Annual Growth	**5%**	**Time (Years)**	**5**
	Projected EPS License Required	**3,160**	**Log Disk (TB)**	**10.97**

Cấu hình đề xuất:

STT	Máy chủ	Yêu cầu
1	Máy chủ Active	32 Core
		64GB RAM
		600GB OS
		8.59TB Data
		Network adapter (1Gb) for Management Network cross link (10Gb) for HA
2	Máy chủ Stanby	32 Core
		64GB RAM
		600GB OS
		8.59TB Data
		Network adapter (1Gb) for Management Network cross link (10Gb) for HA

02 máy chủ hoạt động theo cấu hình dự phòng Active-Standby.

1.5.6.13Thông số kỹ thuật yêu cầu

Thiết kế thông số giải pháp theo yêu cầu:

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
VIII	**Bản quyền giải pháp SIEM**		**01**

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
1	License EPS hoặc tương đương	Tối thiểu 2500EPS	
2	Tính sẵn sàng	Thiết kế triển khai đảm bảo dự phòng HA	
3	Tính năng thu thập	Thu nhập nhật ký bao gồm các loại như:thiết bị mạng (Router, Switch...), thiết bị an ninh (Firewall, IDS/IPS, Database firewall, Antivirus...), hệ điều hành (Operating systems), ứng dụng (Application), cơ sở dữ liệu (Database)... Thu thập dữ liệu lưu lượng mạng bao gồm Netflow, Jflow, Sflow Thu thập nhật ký theo dạng Agen-less	
4	Tính năng truyền log	Lưu trữ nhật ký tạm thời; truyền trên kênh an toàn giữa các thành phần; lọc, tích hợp dữ liệu nhật ký trong khi thu thập (Filtering, Aggregation of data logs); quản lý băng thông sử dụng để truyền nhật ký từ thành phần thu thập đến các thành phần lưu trữ, phân tích; kết hợp các sự kiện (Aggregate events)	
5	Tính năng giám sát (Monitor)	Hỗ trợ giám sát (Monitor)	
6	Phân tích các trường thông tin (Field Sets)	Hỗ trợ phân tích các trường thông tin (Field Sets)	
7	Dữ liệu thu thập từ các thiết bị trong hệ thống mạng phải được phân tích bằng lược đồ chuẩn hóa (normalized schema).	Hỗ trợ dữ liệu thu thập từ các thiết bị trong hệ thống mạng phải được phân tích bằng lược đồ chuẩn hóa (normalized schema).	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
8	Cho phép người quản trị thực hiện & tương tác với các trường sự kiện bao gồm: tạo mới, thay đổi, chia sẻ hay xóa bỏ	Hỗ trợ cho phép người quản trị thực hiện & tương tác với các trường sự kiện bao gồm: tạo mới, thay đổi, chia sẻ hay xóa bỏ	
9	Các luật và phân tích sự tương quan (Rules & Correlation)	+ Cho phép phát hiện các hành động nghi ngờ và phá hoại (suspicious and malicious behavior) + Thực hiện phân tích sự tương quan (correlation) phải dựa vào mẫu (Signature) và phân tích sự bất thường của hành vi (behavior anomaly). + Thực hiện chức năng phân tích tính tương quan đối với dữ liệu theo thời gian thực (real-time) và dữ liệu trong quá khứ (historical data). + Các luật (rules) phải hỗ trợ thực hiện các hành động như sau: Gửi thông báo, tạo lập hồ sơ sự cố, đưa vào danh sách theo dõi…	
10	Bảo hành và hỗ trợ kỹ thuật	≥ 24 tháng	

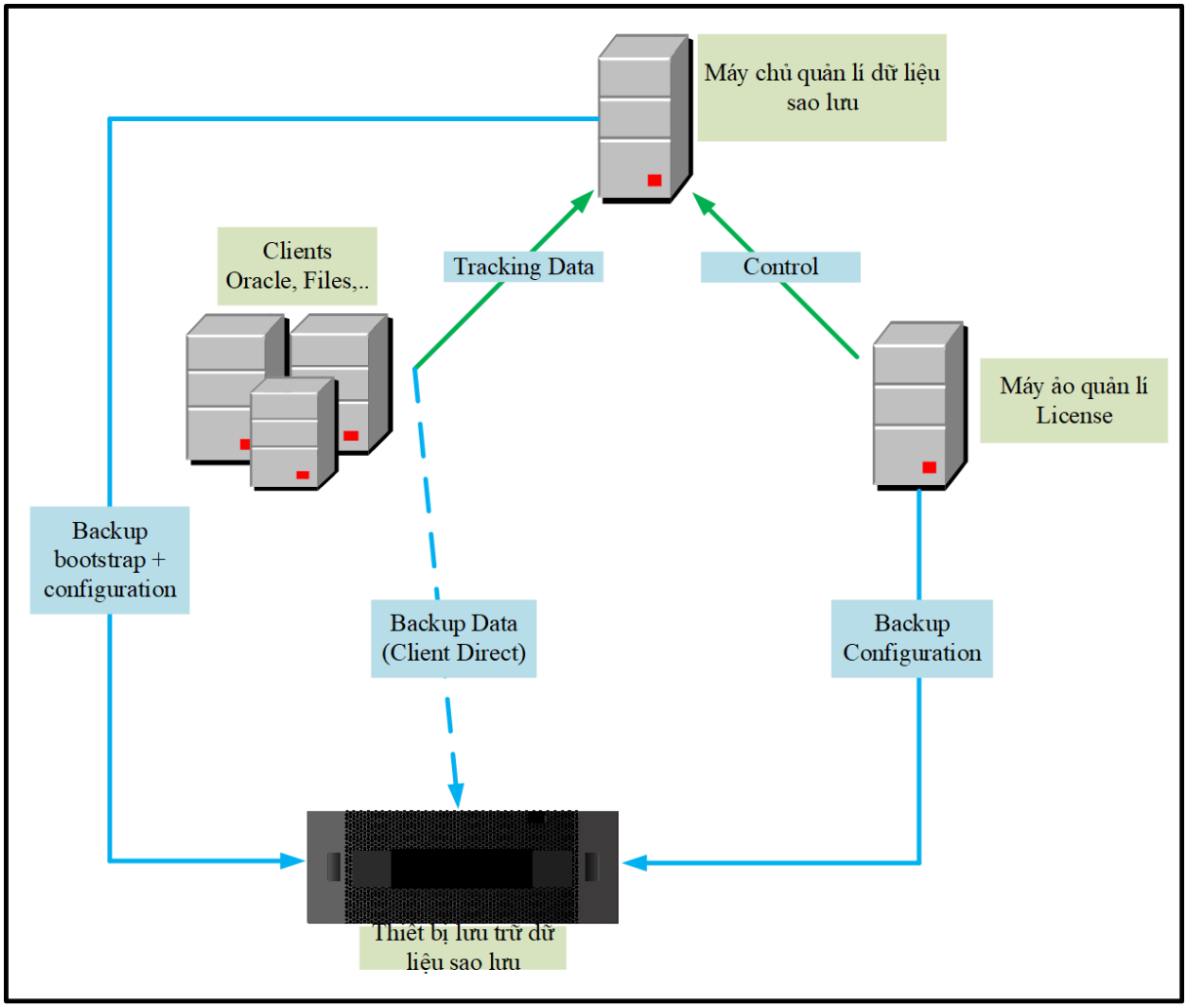
1.5.7 Hệ thống sao lưu và phục hồi dữ liệu

1.5.7.1 Danh mục thiết bị lắp đặt, cài đặt

STT	TÊN HẠNG MỤC	SỐ LƯỢNG
IX	Giải pháp backup	01

1.5.7.2 Mô hình thiết kế luận lý

Luồng dữ liệu backup

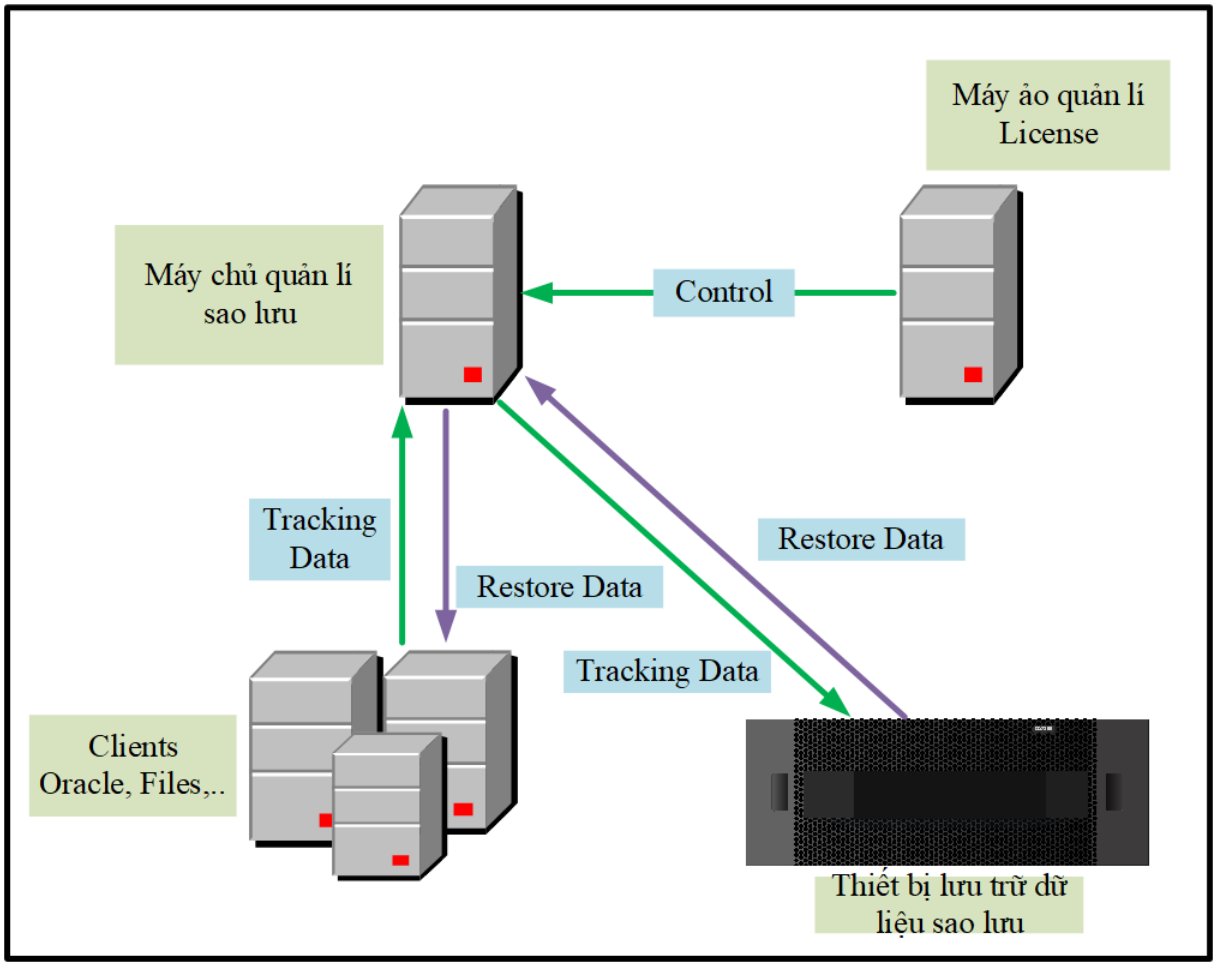


TKTC-BV 27 Mô hình kết nối luận lý giải pháp Backup

Luồng dữ liệu của hệ thống sao lưu dữ liệu sẽ hoạt động theo cơ chế như sau:

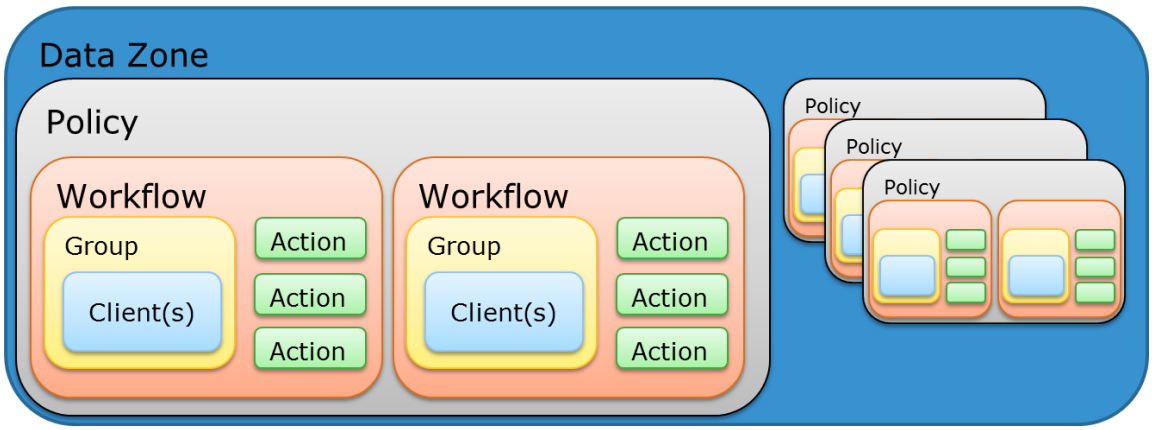
- Máy chủ quản lí sao lưu sẽ truyền lệnh backup tới các client cần backup theo lịch đã được cấu hình sẵn.
- Backup data (dữ liệu backup) tại client sẽ được truyền trực tiếp qua đường Ethernet (backup qua LAN) về thiết bị lưu trữ dữ liệu sao lưu.
- Metadata update vào máy chủ quản lí sao lưu cũng sẽ được backup sang thiếu bị lưu trữ dữ liệu sao lưu như các Clients khác.
- Cần cài đặt thêm License Server phục vụ cho việc quản lí license backup, máy chủ này cũng sẽ được backup theo lịch định kì xuống thiết bị lưu trữ dữ liệu sao lưu để đảm bảo an toàn.
- Máy chủ quản lí sao lưu sẽ chịu trách nhiệm quản lí Server, các thao tác cấu hình, lập lịch,… cho hệ thống sẽ được thực hiện thông qua giao diện.
- Máy chủ quản lí cũng sẽ được backup đến thiết bị lưu trữ dữ liệu sao lưu.

Luồng dữ liệu restore



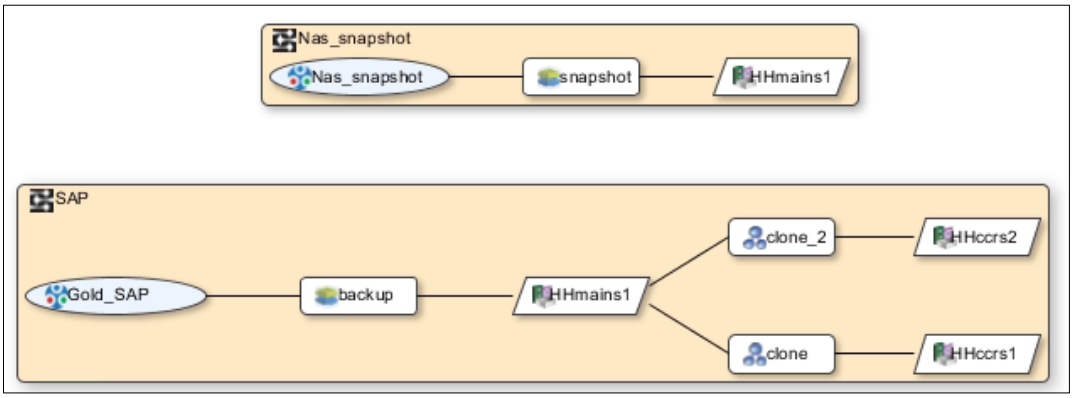
TKTC-BV 28 Mô hình luồng dữ liệu giải pháp Backup

- Máy chủ quản lí ra lệnh restore dữ liệu từ thiết bị lưu trữ dữ liệu sao lưu, sau đó query đến Database để tìm kiếm Metadata của dữ liệu cần restore.
- Sau khi tìm kiếm được thông tin về Metadata của dữ liệu cần restore, máy chủ quản lí sao lưu gửi sẽ query tới thiết bị lưu trữ dữ liệu sao lưu để xác định dữ liệu cần restore.
- Sau khi xác định được dữ liệu cần restore, Device sẽ được mount để sẵn sàng quá trình restore dữ liệu từ thiết bị lưu trữ dữ liệu sao lưu.
- Dữ liệu cần restore sau khi được xác định sẽ được chuyển qua Device gắn với máy chủ quản lí sao lưu, sau đó chuyển tới vị trí lưu trữ bản phục hồi dữ liệu mong muốn. Đồng thời máy chủ đảm nhận nhiệm vụ trung chuyển dữ liệu cũng sẽ gửi lại tracklog tới máy chủ quản lí sao lưu để có thể theo dõi tiến trình trên đó.
- Sau khi hoàn tất update tracklog, quá trình restore dữ liệu từ thiết bị lưu trữ dữ liệu sao lưu hoàn thành
- Hoạt động sao lưu dữ liệu dựa trên các policy, chỉ rõ các hoạt động cần thực hiện và cách thức thực hiện hoạt động để bảo vệ dữ liệu.



Mỗi policy bao gồm 4 thành phần:

- Bản thân Policy, chứa thông tin đảm bảo Service Level, RTO/RPO.
- Mỗi policy chứa một hoặc nhiều workflow; thường dùng mỗi workflow cho 1 loại dữ liệu.
- Mỗi workflow chứa 1 group, gồm một hoặc nhiều client kèm theo các nội dung cần backup tương ứng.
- Mỗi workflow các action chỉ rõ hoạt động cần thực hiện với dữ liệu, ví dụ như backup vào tủ backup, clone từ pool1 sang pool2, replicate từ DC sang DR sau khi backup xong… Các action có thể hoạt động lần lượt hoặc đồng thời.



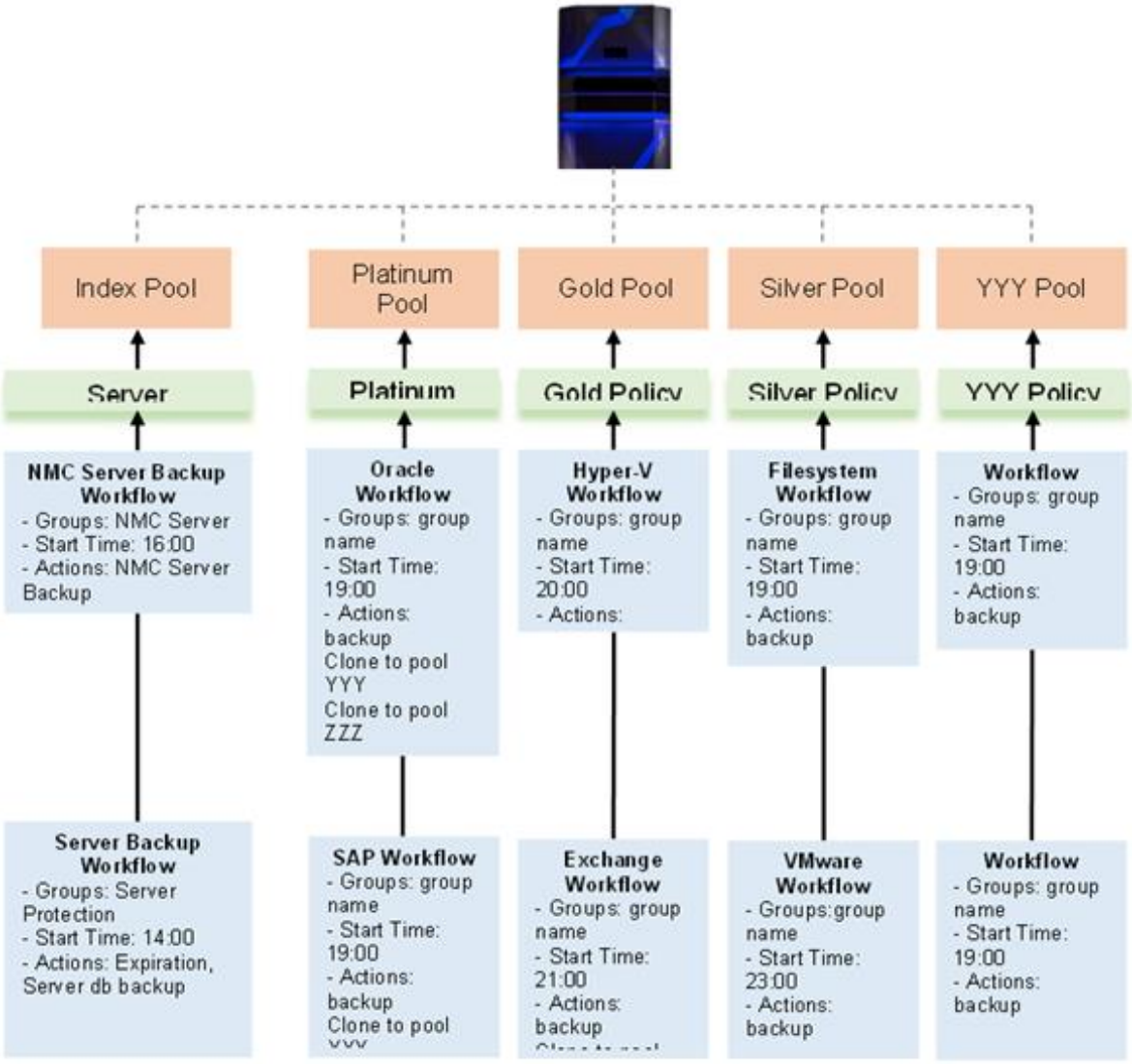
Quản lý thiết bị với Pools và Devices

Máy chủ quản lí sao lưu chứa các dữ liệu backup được lưu trữ trong các pool, các dữ liệu trong pool có thể được clone sang các pool khác. Máy chủ quản lí đọc ghi dữ liệu trong các pool thông qua các device.

Một pool có thể chứa nhiều loại media, tape vật lý, VTL, nhưng để tối ưu nhất thì mỗi pool chỉ nên chứa 1 loại media.

Mỗi device trong máy chủ quản lí sao lưu được dùng để quản lý các media trong đó, không phân biệt là tape vật lý hay tape ảo, hoặc là disk device hay ddboost device. Mỗi lần muốn thực hiện một action liên quan tới device trong pool đều phải thực hiện qua device tương ứng.

Dưới đây là minh họa về một cấu hình các policy để bảo vệ dữ liệu tại EVN. Một số policy chỉ chứa action backup, một số policy khác chứa cả action clone sau khi backup. Lưu ý, đây chỉ là ví dụ minh họa, thực tế áp dụng cho mô hình của EVN sẽ có trong thiết kế chi tiết



Quy tắc đặt tên thiết bị theo quy chuẩn của EVN như sau:

Thiết bị	Ký hiệu
DR + NAME TB + #	DR-xxx-01

Cụ thể các thiết bị được sử dụng trong dự án như sau:

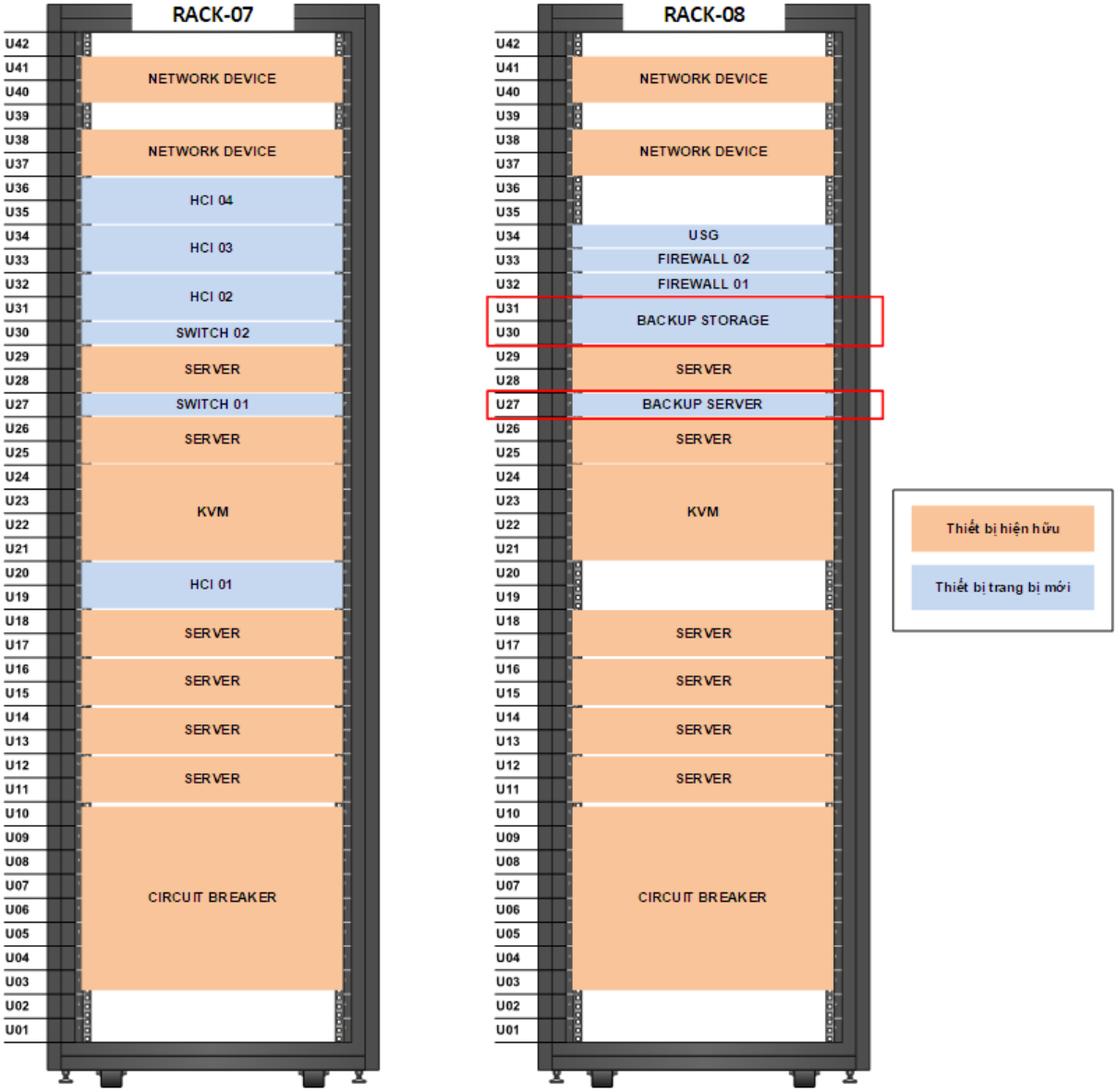
Vai Trò	Tên thiết bị	Model
Storage Backup	backup-storage-01	
Server Backup	backup-server-01	

1.5.7.3 Mô hình thiết kế vật lý

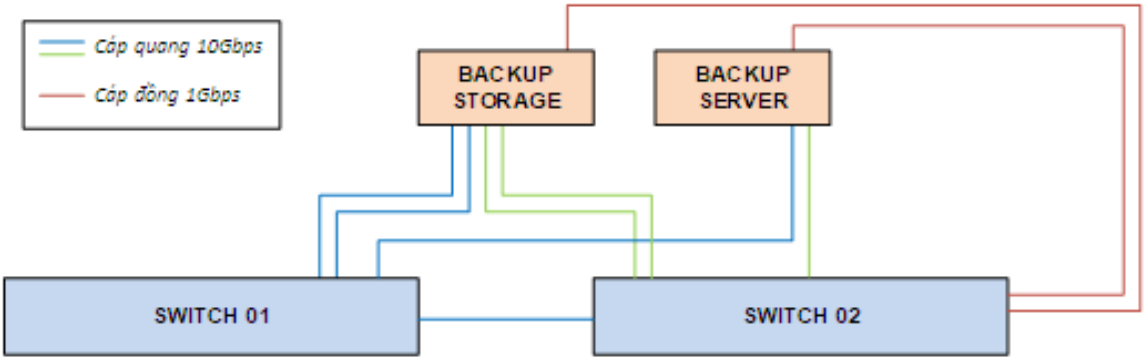
Hệ thống sao lưu và phục hồi dữ liệu sẽ được lắp đặt trên rack tại vị trí như sau:

Rack	U	Tên thiết bị
Rack 08	U27	BACKUP SERVER
Rack 08	U30-31	BACKUP STORAGE

Sơ đồ lắp rack như sau:



Sơ đồ đấu nối vật lý



Thiết bị lưu trữ dữ liệu sao lưu

- Thiết bị sử dụng 04 kết nối quang 10Gbps tới hệ thống thiết bị chuyển mạch, phục vụ truyền dữ liệu lưu trữ sao lưu (data).
- Ngoài ra, thiết bị sử dụng 01 đường kết nối đồng 1Gbps để kết nối tới thiết bị chuyển mạch, phục vụ quản trị phần cứng thiết bị (management).

Máy chủ quản lí sao lưu

- Thiết bị sử dụng 02 kết nối quang 10Gbps tới hệ thống thiết bị chuyển mạch, phục vụ truyền dữ liệu quản lý sao lưu (data)
- Ngoài ra, thiết bị sử dụng 01 đường kết nối đồng 1Gbps để kết nối tới thiết bị chuyển mạch, phục vụ quản trị phần cứng thiết bị (management).

Bảng đấu nối vật lý

STT	Điểm đầu					Điểm cuối				Ghi chú
	R-U	Thiết bị	Cổng	Cáp	Tốc độ	R-U	Thiết bị	Cổng	Mode	
1	R8U30-31	BK-STR	E1	Quang	10Gbps	R7U27	SW01	Eth11	Auto	
2	R8U30-31	BK-STR	E2	Quang	10Gbps	R7U27	SW01	Eth12	Auto	
3	R8U30-31	BK-STR	E3	Quang	10Gbps	R7U30	SW02	Eth11	Auto	
4	R8U30-31	BK-STR	E4	Quang	10Gbps	R7U30	SW02	Eth12	Auto	
5	R8U30-31	BK-STR	MGMT	Đồng	1Gbps	R7U30	SW02	Eth17	Auto	
6	R8U27	BK-SRV	E1	Quang	10Gbps	R7U27	SW01	Eth13	Auto	
7	R8U27	BK-SRV	E2	Quang	10Gbps	R7U30	SW02	Eth13	Auto	
8	R8U27	BK-SRV	MGMT	Đồng	1Gbps	R7U30	SW02	Eth18	Auto	

1.5.7.4 Phân bổ tài nguyên ảo hoá

Máy chủ quản trị tập trung của hệ thống yêu cầu tài nguyên như sau:

Máy chủ	Thông số	Giá trị	Ghi chú
Backup Server	CPU	8 Core	
	RAM	64GB RAM	
	HDD	200 GB	
	NIC	1Gbps và 10 Gbps	
Backup Management	CPU	8 Core	
	RAM	48GB RAM	
	HDD	200 GB	
	NIC	1Gbps	

1.5.7.5 Thông số cài đặt và cấu hình

DD6400 configuration details:

Thông số	Giá trị
Location	TTDK
Name	san01
Domain name (Local)	evnhanoi.vn
DDOS Version	(latest)
Interface DATA	10Gb đồng: Eth2a, Eth2b, Eth2c, Eth2d 10Gb quang: Eth3a, Eth3b, Eth3c, Eth3d
Bonding	LACP hash XOR-L2: Eth2a, Eth2b, Eth2c, Eth2d Eth3a, Eth3b, Eth3c, Eth3d
IP Address	10.24.x.x
Netmask	255.255.255.0
Gateway	10.24.x.x
Media	Fiber 10Gbs Copper 10Gbs
NTP Server	10.240. x.x 10.240. x.x 10.240. x.x

Thông tin DDboost:

Thông số	Giá trị
DDBoost User	admin
DDBoost Password	
Interface Group	Default
IP Address	10.24. x.x

Thiết bị quản lí sao lưu

Thông số	Giá trị
Location	TTDK
Hostname (FQDN)	backup-mgmt.evnhanoi.vn

Operating System	Windows 2022 Standard
CPU	02 x Intel® Xeon® Gold 5317 3G
RAM	256GB
HDD Space	4 x 1.92TB SSD
NetWorker Version	19.9.0.1
IP Address	10.24. x.x
Netmask	255.255.255.0
Gateway	10.24. x.x

1.5.7.6 Chính sách sao lưu và phục hồi

Thiết kế policy

STT	Vai trò	Hostname	IP	Cách thức backup	Source backup	Tần suất backup	Thời gian lưu trữ	Policy Name	Thời gian chạy backup	Pool backup
1	SIEM	siem-01	172.16.253.61	Backup Filesystem Backup Vmware Backup DB Online	/u01 D:\	Full T7 Incre hàng ngày	7days / 14days	SIEM	Daily	Default
2	UDW Server A	Hnpas01		Backup Filesystem Backup Vmware Backup DB Online	/etc /home /root /srv /usr (/usr/local only, nothing else) /var (except /var/run, /var/cache, /var/tmp)	Full T7 Incre hàng ngày	7days / 14days	UDW	Daily	Default
3	UDW Server B	Hnpas02		Backup Filesystem Backup Vmware Backup DB Online		Full T7 Incre hàng ngày	7days / 14days		Daily	Default

4	DB 01	Hnpdb01		Backup Data file/ Backup file	/prodhst/disk1/df1.dbf /sby1hst/disk2/df1.dbf	Full T7 Incre hàng ngày	7days / 14days	DB	Daily	Default
5	DB 02	Hnpdb02		Backup Data file/ Backup file		Full T7 Incre hàng ngày	7days / 14days		Daily	Default

1.5.7.7 Chỉ dẫn biện pháp triển khai

Chi tiết về cách thức thực hiện được thể hiện ở phụ lục 2 "Chỉ dẫn triển khai chi tiết"

1.5.7.8 Kết quả đạt được sau khi hệ thống đi vào hoạt động

Sau khi hệ thống SIEM được triển khai thành công và đi vào hoạt động theo đúng thiết kế, sẽ mang lại các hiệu quả và lợi ích như sau:

- Toàn bộ dữ liệu của hệ thống OT gồm: hệ điều hành; dữ liệu cấu hình các thiết bị switch, router, firewall; cơ sở dữ liệu online/offline hệ thống SCADA; các thư mục, file quan trọng sẽ được bảo vệ. Có rất nhiều bản sao của dữ liệu được lưu trên hệ thống backup, người quản trị có thể lựa chọn ngày (trong vòng 1 tháng) để khôi phục lại dữ liệu. Khi cần khôi phục, hệ thống backup chuyên dụng giúp việc khôi phục diễn ra dễ dàng và nhanh chóng, đảm bảo toàn vẹn dữ liệu.
- Giải pháp Sao lưu và phục hồi dữ liệu còn giúp tăng mức độ an ninh an toàn dữ liệu cho toàn bộ hệ thống, đảm bảo khả năng khôi phục dữ liệu khi xảy ra sự cố tấn công mạng hay mã độc Ransomware/Cyber-attack.

1.5.7.9 Tính toán thông số kỹ thuật

Theo như hiện trạng ở trên thì như cầu dữ liệu cần bảo vệ (đã tính cả mở rộng trong tương lai) là 11TB.

Chính sách sao lưu khuyến nghị là:

- Backup full hàng tuần, lưu trong vòng 4 tuần. Ta cần tới 5 bản full tất cả (mỗi bản full có dung lượng bằng với dung lượng cần bảo vệ tức 11TB). Khi đó tổng dung lượng lưu trữ Full cần là: 5 x 11 ~ 55TB.

- Backup incremental hàng ngày, lưu trong vòng 30 ngày. Ta cần tới 30 bản Incremental tất cả. Giả sử mỗi ngày dữ liệu thay đổi 1% thì tổng dung lượng lưu trữ cần cho lưu Incremental là: 11 * (1.01)^30 ~ 15TB

Tổng dung lượng cần lưu trữ cho hệ thống backup là: 55+15 ~ 70TB.

Do giải pháp Backup và tủ đĩa lưu trữ backup đều có sẵn tính năng chống trùng lặp nên dung lượng tủ đĩa cần để lưu trữ thực tế sẽ thấp hơn dung lượng yêu cầu là 70TB. Giả sử tỉ lệ chống trùng lặp của hệ thống đạt tỉ lệ 3:1 thì dung lượng của tủ đã yêu cầu là: 70 : 3 ~ 24TB.

Đối với hệ thống backup cần 01 máy chủ Media/Backup Server và 01 máy Backup Management Server với cấu hình như sau:

STT	Máy chủ	Yêu cầu
1	Backup Servver	8 Core
		64GB RAM
		200GB OS
		Network adapter (1Gb) for Management và 10GbE cho Data Network
2	Backup management	8 Core
		48GB RAM
		200GB OS
		Network adapter (1Gb) for Management

Dự phòng cho các thành phần:

- Sử dụng máy ảo để cài đặt thành phần backup server và backup management server.
- Khả năng dự phòng của máy ảo sẽ dùng trên giải pháp ảo hóa bao gồm tính năng High Availability (cho phép máy ảo tự động khởi động trên một máy chủ vật lý khác khi máy chủ vật lý gốc bị lỗi).
- Khả năng dự phòng về lưu trữ: theo khả năng dự phòng của giải pháp ảo hóa, có các cơ chế RAID cho phép lỗi 01 ổ cứng đồng thời hoặc 01 node đồng thời (mô hình HCI) mà không ảnh hưởng tới dữ liệu và dịch vụ đang chạy.

1.5.7.10 Thông số kỹ thuật yêu cầu

Thiết kế thông số giải pháp theo yêu cầu:

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
IX	**Bản quyền giải pháp backup**		**1**
1	Thiết bị sao lưu chuyên dụng	Thiết bị dạng Appliance được tích hợp, cấu hình sẵn phần cứng, phần mềm với đầy đủ bản quyền phần mềm đi kèm.	
		Thiết bị có cấu hình tối thiểu:	
		- Khả dụng với dung lượng ≥ 24 TB khả dụng (Raid 6); cho phép mở rộng tới 1.5 PB dung lượng logical.	
		- Tốc độ sao lưu tối đa của thiết bị hỗ trợ ≥ 7TB/giờ	
		- 4 cổng mạng Ethernet tốc độ 1Gb.	
		- 2 cổng mạng Ethernet quang tốc độ 10Gb	
		- Tính năng yêu cầu:	
		+ Chống trùng lặp dữ diệu tại nguồn (source deduplication)	
		+ Tính năng chống trùng lặp dữ liệu deduplication phải được thực hiện thông qua việc cắt dữ liệu thành các đoạn biến thiên, variable-length segment, giúp tăng tỷ lệ chống trùng lặp và hiệu suất sao lưu.	
		+ Khả năng chống trùng lặp dữ liệu hiệu suất cao lên tới 40:1	

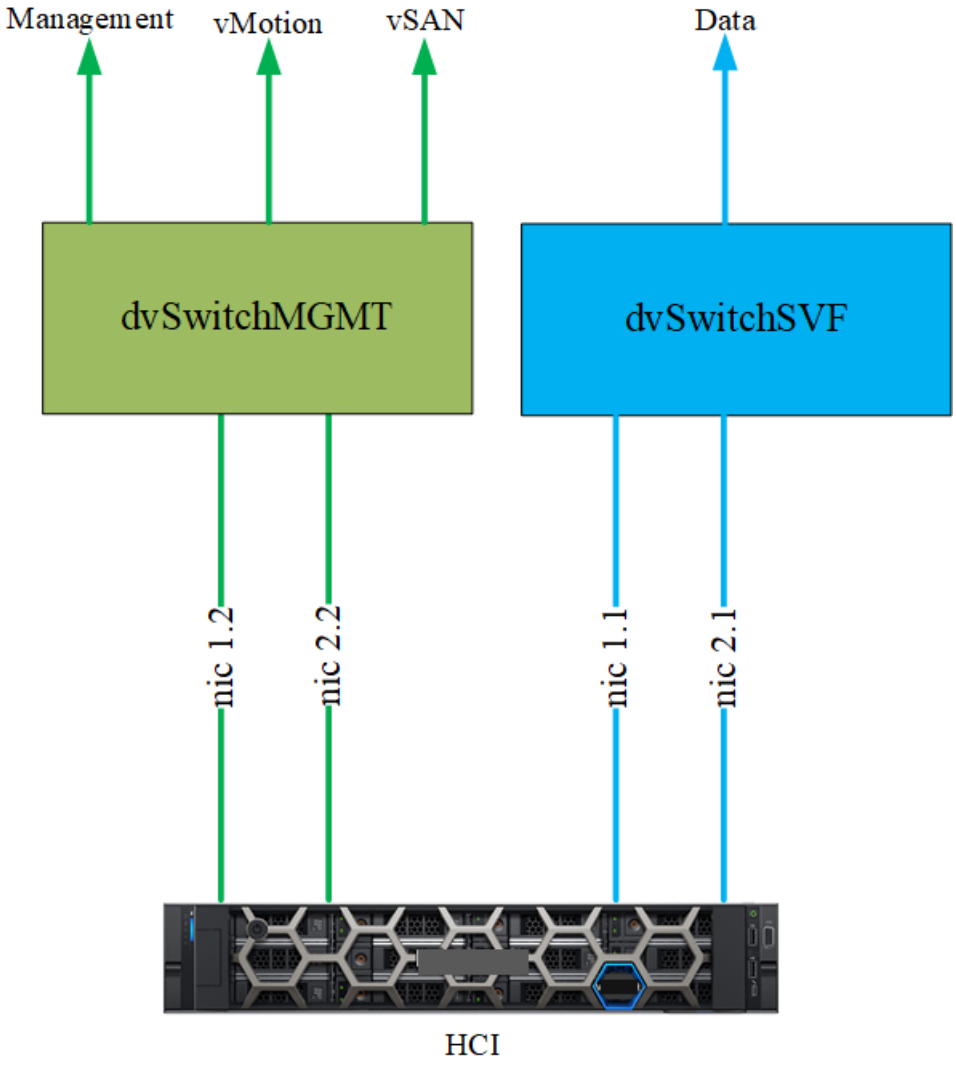
STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
		+ Khả năng mã hóa dữ liệu sao lưu (Encryption): Dữ liệu sẽ được mã hoá ngay trong quá trình sao lưu.	
		+ Bảo vệ dữ liệu sao lưu: có cơ chế chống lại Ransomware. Có sẵn cơ chế khóa bảo vệ dữ liệu khỏi sự sửa đổi, can thiệp, …bằng phần mềm của thiết bị sao lưu chuyên dụng..	
		- Tối thiểu 02 nguồn dự phòng, nguồn 220VAC	
		- Bảo hành và hỗ trợ kỹ thuật 3 năm	
2	Bản quyền phần mềm (tối thiểu 5 năm sử dụng)	Bản quyền sao lưu, khôi phục đáp ứng dung lượng dữ liệu nguồn hệ thống SCADA hiện nay (11TB), không giới hạn các loại dữ liệu sao lưu (hệ điều hành, files, databases Orcale, SQL, ứng dụng…), không giới hạn số node (máy chủ, máy trạm, thiết bị mạng…).	
		- Phần mềm đề xuất phải tương thích hoàn toàn với thiết bị sao lưu chuyên dụng (mục trên), là môt giải pháp tổng thể đồng nhất phần mềm và phần cứng của cùng hãng công nghệ để đảm bảo hạn chế rủi ro tích hợp và bảo hành bảo trì.	
		- Đáp ứng đầy đủ yêu cầu bảo vệ dữ liệu, khả năng sao lưu, khôi phục, chống trùng lặp.	
		- Giao diện quản lý tập trung trên nền Web	
		- Đặt lịch sao lưu theo điều kiện, sự kiện.	

1.5.8 Hệ thống máy chủ, máy trạm

1.5.8.1 Danh mục thiết bị lắp đặt, cài đặt

STT	TÊN HẠNG MỤC	SỐ LƯỢNG
X	Máy chủ HCI Hyper Converge	
A	Phần cứng	04
B	Bản quyền phần mềm	04
XI	Thiết bị Switch back-end	02
XII	Máy trạm	04

1.5.8.2 Mô hình thiết kế luận lý



TKTC-BV 29: Thiết kế luận lý hệ thống máy chủ

Mỗi máy chủ HCI có 04 port mạng 10Gb, đề xuất sử dụng hết để tận dụng hết tài nguyên của phần cứng.

Mỗi máy chủ HCI có 04 port Ethernet 10 Gb dành cho kết nối mạng, được chia thành các cặp đảm nhiệm vai trò khác nhau, đảm bảo khả năng dự phòng và chia tải đối

với từng vai trò. Mỗi máy chủ HCI sẽ có 02 Distributed Switch sử dụng 04 card Ethernet 10Gb làm đường kết nối đến Mgmt, VM guest network, vSAN, vMotion.

Distributed Switch thứ nhất cung cấp kết nối VM guest network (Data) sử dụng nic 1.2 và nic 2.2 với kết nối 10 Gb. Trên switch ảo này sẽ tạo 1 Vmkernel port để cấu hình địa chỉ quản trị cho host. 2 port 10Gb này sẽ được cấu hình bonding active – stanby.

Distributed Switch thứ hai cung cấp kết nối cho dịch vụ quản trị management, vMotion và vSAN, sử dụng nic 1.1 và nic 2.1 với kết nối 10 Gb. Trên switch ảo này sẽ tạo 1 Vmkernel port để cấu hình traffic vSAN. 2 port 10Gb này sẽ được cấu hình bonding active – stanby.

Bảng quy hoạch chi tiết thông tin IP và VLAN cho các dịch vụ như sau:

IP	**Mgmt**	**vMotion**	**vSAN**	**Vm guest network (VLAN)**
HCI 01	10.24. x.x			
HCI 02	10.24. x.x			
HCI 03	10.24. x.x			
HCI 04	10.24. x.x			
HCI Manager	10.24. x.x	x	x	x
DSRS		x	x	x

Quy tắc đặt tên thiết bị theo quy chuẩn của EVN như sau:

Thiết bị	**Ký hiệu**
DR + NAME TB + #	DR-HCI -01

Cụ thể các thiết bị được sử dụng trong dự án như sau:

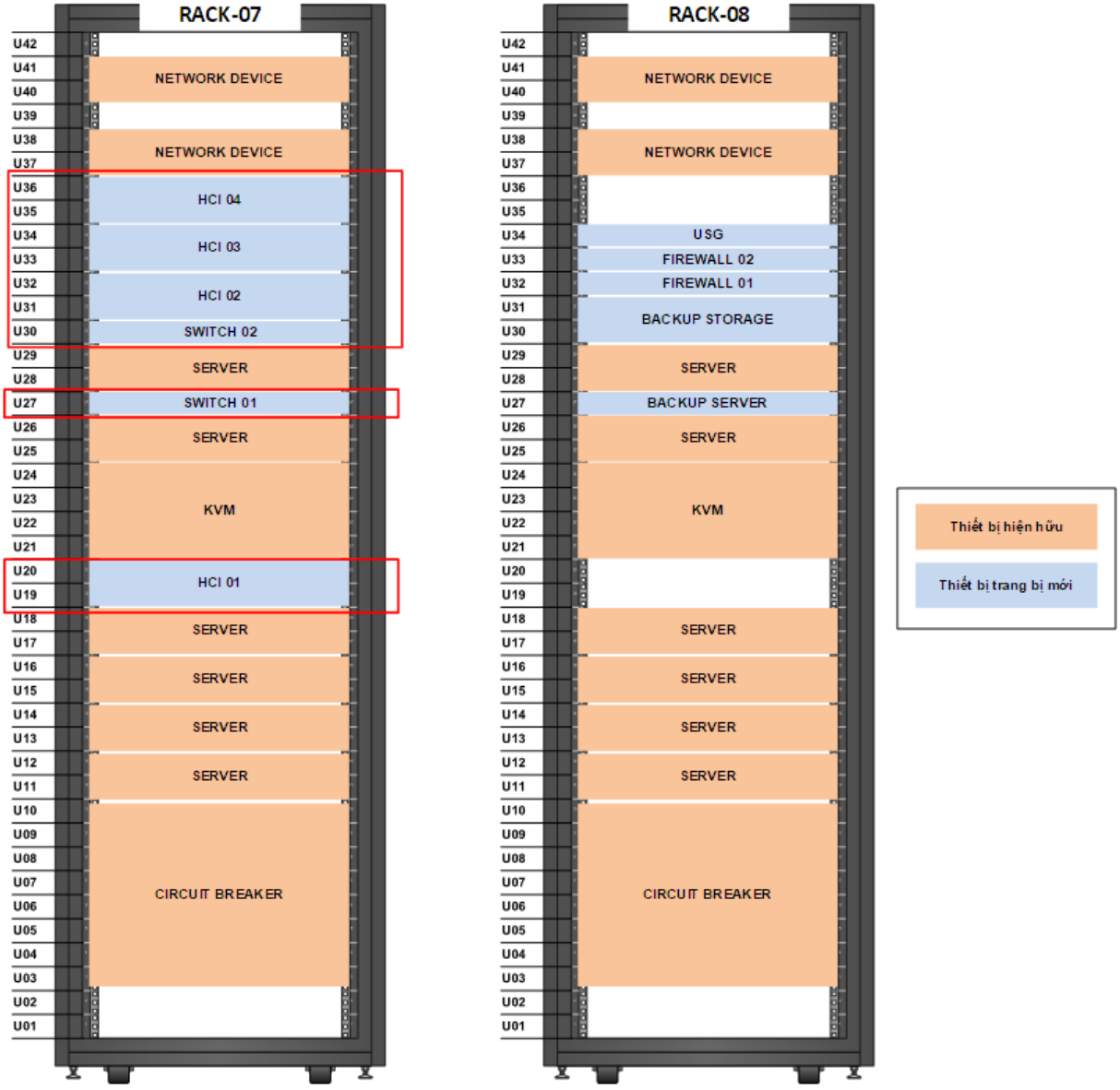
Vai Trò	**Tên thiết bị**	**Ghi chú**
HCI 01	hci-01.evnhanoi.vn	
HCI 02	hci-02.evnhanoi.vn	
HCI 03	hci-03.evnhanoi.vn	
HCI 04	hci-04.evnhanoi.vn	

1.5.8.3 Mô hình thiết kế vật lý

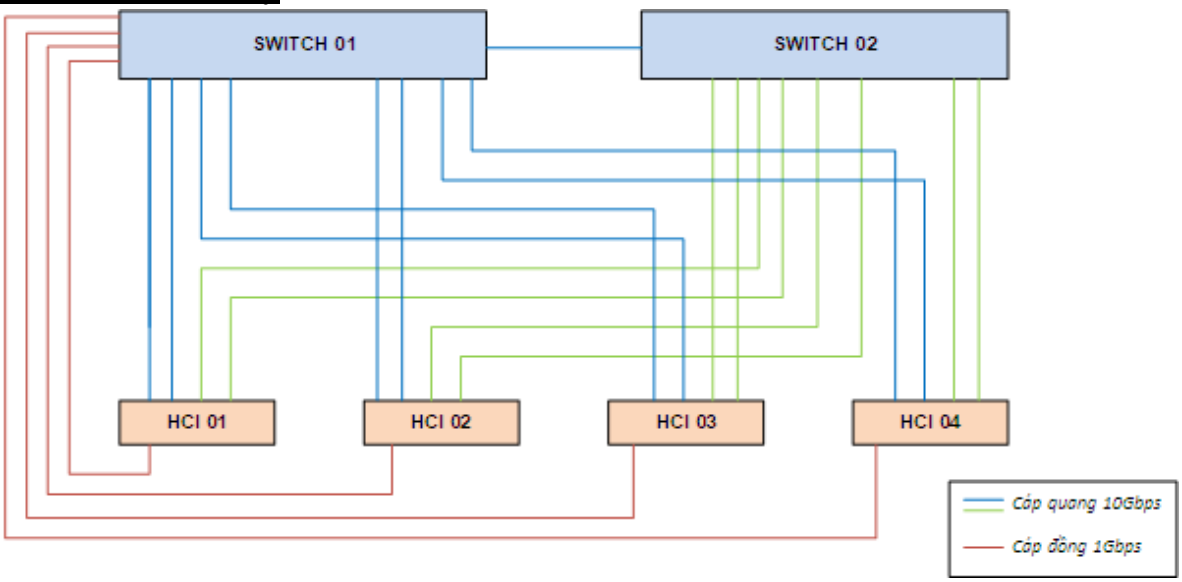
Sơ đồ bố trí tủ rack

Các thiết bị mới được trang bị trong dự án này sẽ được lắp đặt toàn bộ tại site TTĐK, chi tiết vị trí lắp đặt được mô tả như hình dưới:

Rack	**U**	**Tên thiết bị**
Rack 08	U19-20	HCI 01
Rack 08	U27	SWITCH 01
Rack 08	U30	SWITCH 02
Rack 08	U31-32	HCI 02
Rack 08	U33-34	HCI 03
Rack 08	U35-36	HCI 04



Sơ đồ đấu nối vật lý



Các thiết bị HCI trong dự án được đấu nối uplink tới cặp switch: SW 01 và SW 02 để đảm bảo tính dự phòng. Trong đó:

- Cặp switch được cấu hình vPC đảm bảo dự phòng
- Máy chủ HCI được kết nối đến cặp SW 01 và SW 02 thông qua 04 đường 10Gb.

Cổng quản trị phần cứng hỗ trợ việc cấu hình thiết bị từ xa (bao gồm cả việc tắt/bật khi thiết bị có lỗi hay bị tắt đột ngột, theo dõi tình trạng hoạt động các thành phần trong thiết bị …)

- Các kết nối cho cổng quản trị phần cứng có tốc độ 1Gb, sử dụng port đồng RJ45.

Mỗi cổng trên các thiết bị HCI sẽ được kết nối đến cặp swich quản trị MGMT Switch.

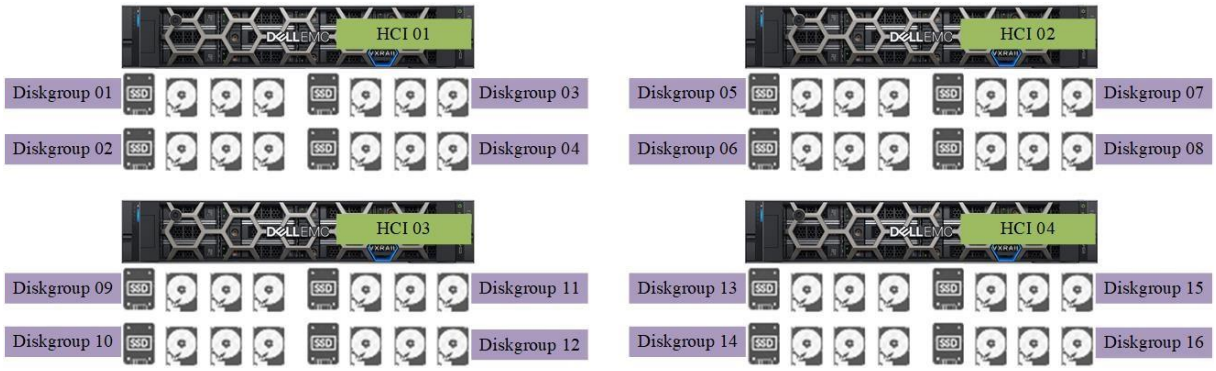
Bảng đấu nối vật lý

STT	Điểm đầu					Điểm cuối				Ghi chú
	R-U	Thiết bị	Cổng	Cáp	Tốc độ	R-U	Thiết bị	Cổng	Mode	
1	R7U19-20	HCI 01	E1	Quang	10Gbps	R7U27	SW01	Eth3	Auto	
2	R7U19-20	HCI 01	E2	Quang	10Gbps	R7U27	SW01	Eth4	Auto	
3	R7U19-20	HCI 01	E3	Quang	10Gbps	R7U30	SW02	Eth3	Auto	
4	R7U19-20	HCI 01	E4	Quang	10Gbps	R7U30	SW02	Eth4	Auto	
5	R7U19-20	HCI 01	MGMT	Đồng	1Gbps	R7U27	SW01	Eth15	Auto	
6	R7U31-32	HCI 02	E1	Quang	10Gbps	R7U27	SW01	Eth5	Auto	
7	R7U31-32	HCI 02	E2	Quang	10Gbps	R7U27	SW01	Eth6	Auto	
8	R7U31-32	HCI 02	E3	Quang	10Gbps	R7U30	SW02	Eth5	Auto	
9	R7U31-32	HCI 02	E4	Quang	10Gbps	R7U30	SW02	Eth6	Auto	
10	R7U31-32	HCI 02	MGMT	Đồng	1Gbps	R7U27	SW01	Eth16	Auto	
11	R7U33-34	HCI 03	E1	Quang	10Gbps	R7U27	SW01	Eth7	Auto	
12	R7U33-34	HCI 03	E2	Quang	10Gbps	R7U27	SW01	Eth8	Auto	
13	R7U33-34	HCI 03	E3	Quang	10Gbps	R7U30	SW02	Eth7	Auto	
14	R7U33-34	HCI 03	E4	Quang	10Gbps	R7U30	SW02	Eth8	Auto	
15	R7U35-36	HCI 03	MGMT	Đồng	1Gbps	R7U27	SW01	Eth17	Auto	
16	R7U35-36	HCI 04	E1	Quang	10Gbps	R7U27	SW01	Eth9	Auto	
17	R7U35-36	HCI 04	E2	Quang	10Gbps	R7U27	SW01	Eth10	Auto	
18	R7U35-36	HCI 04	E3	Quang	10Gbps	R7U30	SW02	Eth9	Auto	
19	R7U35-36	HCI 04	E4	Quang	10Gbps	R7U30	SW02	Eth10	Auto	
20	R7U35-36	HCI 04	MGMT	Đồng	1Gbps	R7U27	SW01	Eth18	Auto	

1.5.8.4 Thiết kế disk group

Trong cluster HCI, HCI node sẽ đóng góp các ổ cứng của mình vào một LUN lưu trữ duy nhất gọi là vSAN Datastore, trong đó các ổ SSD sẽ làm lớp cache, các ổ HDD sẽ làm lớp capacity. vSAN Datastore này sẽ cấp dung lượng đến cho từng VM kèm theo policy phù hợp như là raid 1, raid 0 …

Mỗi HCI node có tối đa 4 diskgroup, mỗi diskgroup yêu cầu 1 ổ cứng SSD và tối đa là 3 ổ cứng HHD. Mỗi máy chủ HCI có 12 ổ cứng 12TB HDD và 04 ổ cứng 1.6 SSD. Để tận dụng tối đa tài nguyên và đạt được hiệu năng tốt, đề nghị mỗi Host sẽ sử dụng 4 Diskgroup, mỗi Diskgroup bao gồm 01 ổ cứng SSD và 03 ổ cứng HDD.



1.5.8.5 Quy hoạch tài nguyên ảo hoá

STT	System	VM Name	CPU	RAM	HDD OS	HDD Data
1	Hệ thống tường lửa	FW-MGMT	32	128	3000	
2	Hệ thống bảo vệ điểm cuối	EPS-MGMT	8	16	1000	
3	Hệ thống quản lý tài khoản đặc quyền	PIM-VAULT	8	8	150	2000
4		PIM-VAULT-BK	8	8	150	2000
5		PIM-PVWA-CPM	8	16	150	500
6		PIM-PSM	16	32	150	500
7		PIM-PTA	4	16	500	
8		PIM-BK	8	16	150	500
9	Hệ thống xác thực đa yếu tố	MFA-01	4	8	600	
10		MFA-02	4	8	600	
11	Hệ thống quản lý thông tin và sự kiện an ninh	SIEM-01	32	64	600	8590
12		SIEM-02	32	64	600	8590
13	Hệ thống	BACKUP-SRV	8	64	200	

STT	System	VM Name	CPU	RAM	HDD OS	HDD Data
14	sao lưu và phục hồi dữ liệu	BACKUP-MGMT	8	48	200	

1.5.8.6 Chỉ dẫn biện pháp triển khai

Chi tiết về cách thức thực hiện được thể hiện ở phụ lục 2 "Chỉ dẫn triển khai chi tiết"

1.5.8.7 Kết quả đạt được sau khi hệ thống đi vào hoạt động

Những lợi ích nổi trội mà HCI mang lại bao gồm: đơn giản hóa việc thiết kế và tích hợp hệ thống, giảm thiểu rủi ro về tính bất tương đồng của những thành phần phần cứng và phần mềm, tiết kiệm thời gian và chi phí đầu tư, nâng cao hiệu quả vận hành của hạ tầng CNTT tại EVNHANOI. Đây là những đặc tính thiết yếu để giải quyết vấn đề đau đầu của đội ngũ lãnh đạo của doanh nghiệp hay các nhà khai thác TTĐK, đó là làm sao giảm thiểu chi phí và thời gian khởi tạo hạ tầng, nhanh chóng đưa tài nguyên đến tay người dùng để biến CNTT thành lợi thế cạnh tranh và sớm mang lại hiệu quả, biến chi phí thành lợi nhuận.

- Giao diện quản lý hội tụ dễ sử dụng: Quy trình vận hành của Data Center ngày càng trở nên phức tạp với nhiều tác vụ đòi hỏi tài nguyên hệ thống cực cao – một trong những tính năng quan trọng của HCI là làm việc quản lý tài nguyên trở nên đơn giản hơn. Với hệ thống HCI, quản trị viên đã có trong giao diện "hội tụ" và trực quan, giúp tối thiểu số lượng cán bộ vận hành hệ thống.
- Tiết kiệm chi phí: Nếu tính toán kỹ thì chi phí giải pháp của HCI sẽ tốt hơn hơ so với các Storage và Controller của mô hình truyền thống. Vì hệ sinh thái cho các thiết bị x86 đã được sẵn sàng, chi phí mua và support cũng tiết kiệm hơn.
- Tăng cường năng lực bảo mật: HCI có khả năng "điều khiển hội tụ" (Unified Point of Control), được tích hợp các biện pháp bảo vệ data tốt nhất, bao gồm: Access Control, Mã hoá – Encryption, Remote Data Replication, các quy trình Backup và Disaster Recovery, Applied System-wide software.
- Giảm thiểu rủi ro: Giải pháp siêu hội tụ không đòi hỏi số lượng nhân viên quản trị nhiều và quá chuyên sâu- Những yêu cầu này trước đây là bắt buộc, vì như vậy mới tối ưu hoá được hệ thống, hiệu suất mới đảm bảo. Hệ thống đã tự động trong hầu hết các thao tác mà người quản trị phải làm trước đây, theo cơ chế tối ưu mà máy tự học từ các hệ thống toàn cầu cũng như chính quá trình vận hành của hệ thống (AI, Machine Learning).

1.5.8.8 Tính toán thông số kỹ thuật

Thông tin hệ điều hành sử dung cho các giải pháp như sau

GIẢI PHÁP	VMS	Hệ ĐIỀU HÀNH
FW mgmt	1	Linux
EPS	1	Windows server
2FA	1	Linux
SIEM	2	Linux

GIẢI PHÁP	VMS	Hệ ĐIỀU HÀNH
PAM	6	05 Windows Server, 4 license Remote Desktop CAL. 01 Linux.
Backup Management	1	Windows Server
Máy chủ quản trị ảo hóa	1	Windows server

Dưới đây là yêu cầu về tài nguyên máy chủ tính toán và lưu trữ cho hệ thống đảm bảo an ninh, an toàn thông tin cho hệ thống giám sát, điều khiển và tự động hóa lưới điện của EVNHANOI.

Bảng 1: Yêu cầu năng lực máy chủ cho từng giải pháp

GIẢI PHÁP	VMS	PROCESSOR (VIRTUAL CORES)	RAM (GB)	HDD (TB)
FW mgmt	1	32	128	3
EPS	1	8	12	1
2FA	2	8	16	1.2
SIEM	2	64	128	17.18
PAM	6	64	96	6.75
Backup Server	1	8	32	0.2
Backup management	1	8	48	0.2
Máy chủ quản trị ảo hóa	1	4	19	0.2
NFS share cho lưu trữ file patch, firmware, ISO…				5
Tổng	**15**	**196**	**531**	**34.73**

Các thiết bị hoạt động ở ngưỡng an toàn yêu cầu CPU, RAM, HDD hoạt động ở dưới 80% năng lực, đảm bảo thiết bị không bị hoạt động quá tải. Số core yêu cầu = 196/ 0.8 ~ 245 (core). Bộ nhớ yêu cầu = 531/0.8 ~ 664 (GB). Dung lượng HDD yêu cầu = 34.73/ 0.8 ~ 44 (TB).

Khi đó yêu cầu tài nguyên để đảm bảo các thiết bị luôn hoạt động ở ngưỡng an toàn:

YÊU CẦU NĂNG LỰC	VMS	PROCESSOR (VIRTUAL CORES)	RAM (GB)	HDD (TB)
Tổng	15	245	664	44

Quy đổi từ vCPU (virtual core) sang pCPU (CPU core vật lý): thông thường tỉ lệ vCPU: pCPU được lấy từ ngưỡng 1:1 cho tới 3:1 được đánh giá là an toàn, và tối ưu trong quá trình tính toán định cỡ. Lấy tỉ lệ vCPU: pCPU là 2:1 , khi đó số core vật lý yêu cầu là: 245/2 ~ 123 core.

Để đảm bảo dự phòng N+1, ở đây với số máy chủ là 3 thì cần thêm 1 máy chủ dự phòng (tỉ lệ dành dự phòng là 25%). Như vậy yêu cầu năng lực với CPU, RAM để hệ thống đảm bảo dự phòng là: Core vật lý yêu cầu = 123 * 1.25 ~ 154 core. RAM yêu cầu là 598 * 1.33 ~ 830GB. Riêng phần HDD trên HCI đã có sẵn cơ chế dự phòng (dùng cơ chế đồng bộ Replication/ RAID) nên không cần tính thêm 25% dự phòng cho HDD.

Phần dữ liệu HDD lưu trữ chủ yếu là log sự kiện của các phần mềm về SIEM và PAM. Giả định tăng trưởng phần lưu trữ mỗi năm là 30% thì dung lượng HDD yêu cầu tính cho 5 năm = HDD yêu cầu * 1.3^5 = 44 *1.3^5 ~ 164TB.

Dựa vào các yêu cầu phần cứng máy chủ cho mỗi giải pháp, đồng thời tính toán tăng trưởng dữ liệu, dự phòng máy chủ, chúng tôi đưa ra thông số kỹ thuật đề xuất cho giải pháp máy chủ HCI như sau:

Bảng 14: Thông số kỹ thuật đề xuất cho giải pháp máy chủ HCI

YÊU CẦU NĂNG LỰC	VMS	PROCESSOR (PHYSICAL CORES)	RAM (GB)	HDD (TB)
Tổng	15	≥ 154	≥ 830	≥ 164

Với cấu hình 04 node HCI thì mỗi node cấu hình tối thiểu:

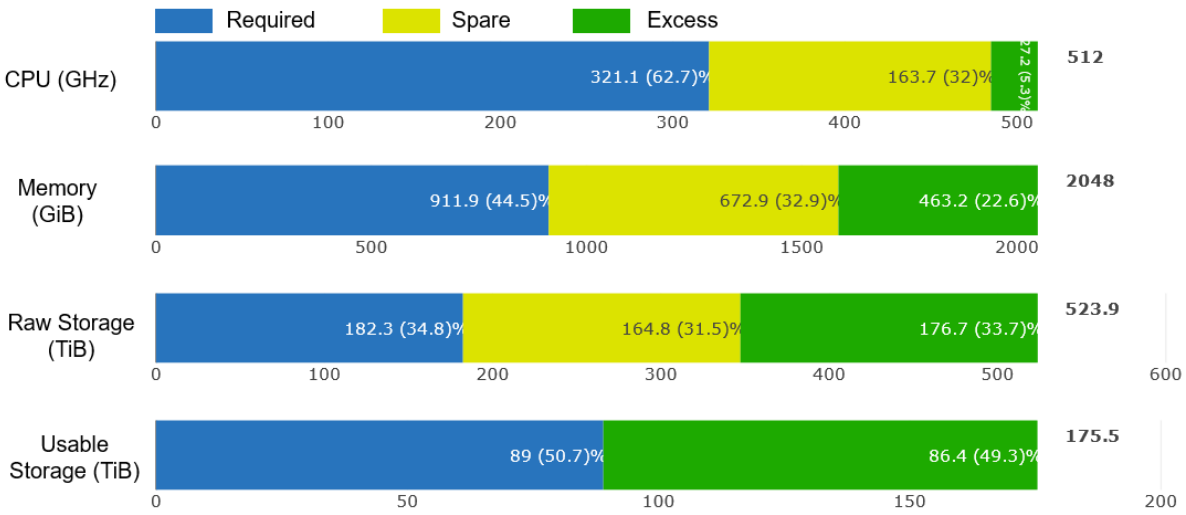
- 154/4 ~ 39 core vật lý tức mỗi server bao gồm tối thiểu 02 chip, mỗi chip 20 core vật lý. Để đảm bảo dự phòng và đáp ứng mở rộng trong tương lai, chúng tôi đề xuất mỗi node gồm tối thiểu 02 chíp Intel 32-core.
- 830/4 ~ 208GB RAM, tức cần tối thiểu 8 thanh RAM 32GB. Để đảm bảo dự phòng và đáp ứng mở rộng trong tương lai, chúng tôi đề xuất mỗi node gồm tối thiểu 16 thanh RAM 32GB.
- 164/ 4 ~ 41TB Usable Disk. Nếu sử dụng cấu hình Mirror/ Fault tolerant = 1 (tương ứng Overhead là 50%) và hệ số format là 0.9, khi đó tổng dung lượng RAW yêu cầu cho mỗi node = 41/ 0.5/0.9 ~ 92TB RAW Disk. Nếu sử dụng ổ HDD có dung lượng 12TB thì mỗi node cần tối thiểu: 92/12~ 8 ổ. Để đảm bảo dự phòng và đáp ứng mở rộng trong tương lai, chúng tôi đề xuất mỗi node gồm tối thiểu 12 ổ 12TB HDD.

Tham khảo cấu hình Sizing HCI 04 node từ tool sizing của một số hãng như sau:

	HCI - 4 Nodes	**Socket/DG**	**Node**	**Cluster**
CPU	Intel 6338 (Gold, 32C, 2GHz)	1 Per Socket	2 (64 Cores - 128 GHz)	8 (256 Cores - 512 GHz)
Memory	32 GB DIMMs	8 Per Socket (256 GiB)	16 (512 GiB)	64 (2 TiB)

Cache	1600 GB NVMe - (13% ratio) Endurance Class: D Performance Class: F	1 Per DG	4	16
Storage	12 TB 7.2K HDD (33% excess) 0 free capacity slots	3 Per DG (32.7 TiB)	12 (131 TiB)	48 (523.9 TiB)
Network			NIC 1: 4 x 10 GbE	NIC 1: 16 x 10 GbE

	Required Capacity	Min #nodes	Required Spare/HA	Excess Capacity	Total Configured
CPU (Cores)	152.9 @ 2.1	N/A	N/A	N/A	256 @ 2 GHz
CPU (GHz)	321.1	4	163.7	27.2	512
Memory (GiB)	911.9	4	672.9	463.2	2048
Raw Storage (TiB)	182.3	3	164.8	176.7	523.9
Usable Storage (TiB)	89	N/A	N/A	86.4	175.4



Máy trạm:

Hệ thống cần tối thiểu 04 máy trạm dành cho các chức năng sau:

- 01 máy trạm làm nhiệm vụ cập nhật bản vá, phiên bản mới nhất cho các phần mềm, hệ điều hành và firmware cho các thiết bị.
- 01 máy trạm thực hiện nhiệm vụ Monitor, tìm kiếm, phân tích, theo dõi sự kiện an ninh cho toàn bộ hệ thống SIEM.
- 01 máy trạm phục vụ xử lý sự cố (chuyên gia), đảm nhiệm nhiều chức năng xử lý sự cố từ xa như VPN…
- 01 máy trạm phục vụ việc truy cập từ xa qua giao diện Web GUI vào các hệ thống cần quản lý

1.5.8.9 Thông số kỹ thuật yêu cầu

Thiết kế thông số giải pháp theo yêu cầu:

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
X	**Máy chủ HCI Hyper Converge**		
A	**Phần cứng**		**4**
1	Chủng loại	Hyper-Conveged Appliance	
2	Kiểu dáng	Rack 2U	
3	Bộ vi xử lý	02 x Intel CPU 32C 2.0 Ghz hoặc cao hơn	
4	Bộ nhớ	≥ 16 x 32 GB RDIMM Hỗ trợ 32 DDR4 DIMMs/ Dung lượng RAM tối đa hỗ trợ: ≥4096GB	
5	Lưu trữ cho OS/ Hypervisor	≥ 2 x 480GB SSD SATA M.2 /RAID 1	
6	Lưu trữ: Caching Tier	Tối thiểu 04 x 1600GB SSD cho mỗi node.	
7	Capacity Tier	Tối thiểu 12 x 12TB SAS Hot-Plug cho mỗi node hoặc tương đương về dung lượng	
8	Khay đĩa cứng	≥ 12 LFF Hot Plug Hard Drive	
9	Card mạng:	4x10 GbE SFP+ / Khả năng nâng cấp tối đa 12x10 GbE SFP+	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
		Các card mạng: có đầy đủ SFP+ SR 10Gbps, dây nhảy đi kèm	
10	Cổng quản trị	1x1 GbE RJ45	
11	Số nốt tối đa trên 1 cluster	≥ 32	
12	Phần mềm tích hợp sẵn	Bảng hiển thị mức độ sử dụng storage, CPU và memory trong toàn bộ cluster, trong từng appliance node	
		Hướng dẫn người quản trị thêm node vào cluster, tự động nhận biết node khi online.	
		Theo dõi các sự kiện hệ thống và cung cấp các thông báo toàn diện đang diễn ra về trạng thái của môi trường ảo và phần cứng thiết bị.	
13	Tích hợp sẵn các dịch vụ dữ liệu cao cấp	- Toàn bộ dịch vụ này tích hợp sẵn trong thiết bị HCI appliance - Dịch vụ chẩn đoán, sửa chữa từ xa. - Dịch vụ bảo mật dữ liệu tích hợp sẵn trong Appliance bao gồm phần mềm cho phép sao lưu, khôi phục mức VM, tại chỗ hoặc từ xa thông qua replicate	
15	Bảo hành	≥ 36 tháng	
B	**Phần mềm**		**04**
1	Phần mềm ảo hóa máy chủ (Hypervisor)	- License phần mềm ảo hóa máy chủ cho 02 CPU, hỗ trợ kỹ thuật 3 năm - Có khả năng quản lý mạng tập trung và mã hóa máy chủ ảo.	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
2	Phần mềm ảo hóa lưu trữ (Storage virtualization)	- Phần mềm ảo hóa lưu trữ (Storage virtualization) tích hợp ngay trong kernel của phần mềm ảo hóa máy chủ, bản quyền cho 02 CPU hoặc toàn bộ dung lượng của thiết bị tại yêu cầu Storage - Capacity. - Có khả năng chống trùng lặp và nén dữ liệu	
3	Phần mềm ghi nhật ký (logging)	- License phần mềm ghi nhật ký của toàn bộ hạ tầng ảo hóa cho 02 CPU, hỗ trợ kỹ thuật 3 năm. Thu thập, quản lý nhật ký của toàn bộ môi trường, từ OS, apps, storage,…	
4	Phần mềm sao lưu máy chủ ảo	Backup software license for 5 VM licenses per node, khả năng sao lưu nội bộ hoặc giữa các site.	
5	Bảo hành	≥ 36 tháng	
XI	**Thiết bị Switch back-end**		**2**
1	Thiết bị Switch 10GbE đi kèm	Yêu cầu cặp switch layer 3. Cấu hình mỗi switch: - Số lượng port ≥ 24 port 1/10GbE - Transceiver đi kèm: ≥ 14 x 10GbE SFP+ SR và ≥ 04 x 1GbE RJ45	
2	Bảo hành	≥ 36 tháng	
XII	**Yêu cầu cho máy tính trạm**		**04**
1	Số lượng thiết bị	Tổng số ≥ 4 thiết bị đi kèm màn hình, bàn phím	
2	Chíp xử lý	Intel Core i7-11700k (2.5GHz turbo up to 4.9Ghz, 8 nhân 16 luồng, 16MB Cache, 65W) hoặc hiệu năng cao hơn	
3	Bộ nhớ Ram	1x16GB DDR4 3200 Mhz UDIMM non-ECC Memory, 4 UDIMM slots, Max 128 GB hoặc dung lượng cao hơn	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
4	Ổ đĩa cứng	1TB HDD 3.5" Sata (x2 HDD 3.5" Sata + x1 SSD M2 PCIE NVME) hoặc dung lượng cao hơn	
5	Card đồ họa	Nvidia P2000 NVIDIA Quadro 5GB DDR5 - 4x mDP to DP hoặc hiệu năng cao hơn	
6	Ổ đĩa quang (DVD)	8x DVD+/-RW	
7	Cổng xuất hình	2x DisplayPort 1.4, HDMI	
8	Kết nối mạng LAN	10/100/1000 Mb/s	
9	Bảo hành	36 tháng	

1.5.9 Thông số kỹ thuật yêu cầu tổng hợp

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
I	**Firewall tại TTĐK**		**02**
1	Thông lượng khi bật các tính năng phòng chống tấn công Threat Prevention (Application, IPS, Antivirus, Antispyware, File blocking, DNS security, logging)	≥ 10 Gbps	
2	Thông lượng Next Generation Firewall/ tường lửa ứng dụng	≥ 10 Gbps	
3	Thông lượng IPSEC	≥ 10 Gbps	
4	Số lượng VLAN hỗ trợ	≥ 3000	
5	Số security zone	≥ 200	
6	Cổng kết nối dữ liệu (Có sẵn trên thiết bị)	≥ 02 cổng 1G RJ45 + 01 cổng 10G SFP+ dành riêng cho cấu hình HA	
		≥ 04 cổng 1GbE RJ45	
		≥ 04 cổng quang 1GbE/10GE SFP	
7	Cổng quản trị thiết bị	≥ 1 RJ45 Mgmt	
8	Giao diện quản trị	Web, CLI, API/REST API	
9	Tính năng HA	Active/active, Active/passive	
10	Hỗ trợ các giao thức định tuyến	OSPF, BGP, RIP, PIM (SM , SSM), IGMP	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
11	Đảm bảo khả năng kiểm soát và nhận dạng các ứng dụng ICS/SCADA như sau:	Modbus, IEC-60870-5-104, IEC 60870-6 (ICCP), OPC DA & UA, DNP3, IEC 61850; BACnet, ABB Network Manager, ABB-RP570, ICCP, IP EtherNet, IP MTConnect, Cygnet SCADA, R-GOOSE, CIP EtherNet IP, Profinet, Schneider OASyS, Schneider Wonderware Suitelink, Schweitzer Engineering SEL Fast Messaging, Siemens FactoryLink, Siemens Profinet IO, Siemens-P2, Siemens S7, Siemens S7-Comm-Plus, DLMS, GE-Historian, GE-Eterra-SCADA.	
12	Tính năng bảo mật	- Có sẵn các tính năng dưới đây hoặc tương đương Stateful firewall , , IPSec VPN, Application Control, IPS, Antivirus	
		- Trên một chính sách bảo mật có thể thiết lập theo các thành tố như ứng dụng, người dùng, device, zone và bật các tính năng antivirus, ips, antispyware, lọc file.	
		- Có nhiều cơ chế định danh người dùng như Server monitoring, Port mapping, syslog, XFF Header, Username Header Insertion, Authentication policy, XML API, Client probing	
13	Tính năng ngăn chặn tấn công	Phát hiện và ngăn chặn các kết nối C2C, sử dụng DNS sinkholing để xác định các máy bị lây nhiễm	
		Phát hiện và ngăn chặn các loại mã độc, các tấn công khai thác lỗ hổng bảo mật	
14	Bản quyền sử dụng các tính năng bảo mật có sẵn	≥ 24 tháng	
15	Nguồn điện	Đảm bảo 02 nguồn dự phòng, điện áp 220VAC	
16	Bảo hành và hỗ trợ kỹ thuật	≥ 24 tháng	
II	**Firewall tại các TBA**		**66**
1	Thông lượng Threat Prevention (Application, IPS, Antivirus, Antispyware, File	≥ 400 Mbps	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
	blocking, DNS security, logging)		
2	Thông lượng Next Generation Firewall/tường lửa ứng dụng	≥ 400 Mbps	
3	Thông lượng IPSEC VPN	≥ 400 Mbps	
4	Số lượng VLAN hỗ trợ	≥ 3000	
5	Số security zone	≥ 50	
6	Cổng kết nối dữ liệu (Có sẵn trên thiết bị)	≥ 08 cổng 1GE RJ-45	
7	Cổng quản trị thiết bị	≥ 1 RJ45 Mgmt	
8	Giao diện quản trị	Web, CLI	
9	Tính năng HA	Active/active, Active/passive	
10	Hỗ trợ các phương thức định tuyến	OSPF, BGP, RIP, PIM (SM, SSM), IGMP	
11	Đảm bảo khả năng kiểm soát và nhận dạng các ứng dụng ICS/SCADA như sau:	Modbus, IEC-60870-5-104, IEC 60870-6 (ICCP), OPC DA & UA, DNP3, IEC 61850; BACnet, ABB Network Manager, ABB-RP570, ICCP, IP EtherNet, IP MTConnect, Cygnet SCADA, R-GOOSE, CIP EtherNet IP, Profinet, Schneider OASyS, Schneider Wonderware Suitelink, Schweitzer Engineering SEL Fast Messaging, Siemens FactoryLink, Siemens Profinet IO, Siemens-P2, Siemens S7, Siemens S7-Comm-Plus, DLMS, GE-Historian, GE-Eterra-SCADA.	
12	Tính năng bảo mật	- Có sẵn các tính năng dưới đây hoặc tương đương Stateful firewall , IPSec VPN, Application Control, IPS, Antivirus	
		- Trên một chính sách bảo mật có thể thiết lập theo các thành tố như ứng dụng, người dùng, device, zone và bật các tính năng antivirus, ips, antispyware, lọc file.	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
		- Có nhiều cơ chế định danh người dùng như Server monitoring, Port mapping, syslog, XFF Header, Username Header Insertion, Authentication policy, XML API, Client probing	
13	Tính năng ngăn chặn tấn công	Phát hiện và ngăn chặn các kết nối C2C, sử dụng DNS sinkholing để xác định các máy bị lây nhiễm	
		Phát hiện và ngăn chặn các loại mã độc, các tấn công khai thác lỗ hổng bảo mật	
14	Bản quyền sử dụng các tính năng bảo mật có sẵn	≥ 24 tháng	
15	Nguồn điện	Đảm bảo 02 nguồn dự phòng, điện áp 220VAC	
16	Bảo hành và hỗ trợ kỹ thuật	≥ 24 tháng	
III	**Giải pháp quản lý tường lửa tập trung**		**01**
1	Bản quyền phần mềm	Theo số lượng tường lửa thực tế	
2	Tương thích với thiết bị tường lửa	Phần mềm quản lý tường lửa tập trung phải cùng hãng sản xuất và hoàn toàn tương thích với thiết bị tường lửa cung cấp ở trên	
3	Khả năng mở rộng số lượng thiết bị quản lý	≥ 1000	
4	Giao diện quản trị	Giao diện Web/ CLI / API	
5	Môi trường triển khai	Một trong các môi trường ảo hoá sau: VMware ESXi, KVM, và Microsoft Hyper-V	
6	Quản lý tập trung	- Có khả năng quản trị tập trung cấu hình chính sách các tường lửa	
		- Có khả năng quản lý hệ điều hành của các thiết bị - centralized device software installation.	
		- Quản lý chính sách theo nhóm thiết bị, mô hình phân cấp	
		- Tích hợp đồng thời cả tính năng quản trị cấu hình và quản lý tập trung log	
7	Tính năng quản trị network	Tự động hóa (Automation): - Có cơ chế tự động triển khai nhanh hoặc cùng lúc nhiều thiết bị	
		Phân tích (analyze) - Có khả năng giám sát hiệu năng của các thiết bị, giám sát các vấn đề về hiệu năng	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
		- Có khả năng giám sát tốc độ kết của các thiết bị tường lửa	
8	Tính năng quản trị thiết bị firewall	Tạo và quản lý tập trung các chính sách bảo mật thông qua một giao diện duy nhất. Quản trị tập trung với duy nhất một giao diện console cho tất cả các tính năng bảo mật như Firewall, VPN, IPS, Application Control.	
		Hiển thị số lần truy cập thông qua policy theo thời gian thực.	
		Có khả năng thiết lập tự động tag người dùng, địa chỉ IP theo các điều kiện lọc log ngay trên thiết bị, có thể tự động đưa người dùng, IP vào danh sách nhóm chặn khi phát sinh các rủi ro.	
		Có khả năng tự động phân tích các sự kiện trong hệ thống mạng để xác định các đối tượng bị thoả hiệp trong hệ thống mạng.	
		Hiển thị nơi các mối đe dọa bắt nguồn.	
		Có tính năng chuyển đổi các signature của Snort và Suricata signature sang signature cho tường lửa	
		Thiết bị quản lý tập trung có khả năng phân phối lại các thông tin như IP User Mappings, IP Tags, User Tags, Quarantine List đến các tường lửa được quản lý	
		Giám sát sức khoẻ của firewall: - Sử dụng CPU - Sử dụng bộ nhớ	
		Sytem logs được chuyển tiếp đến thông tin bảo mật và quản lý sự kiện (SIEM).	
9	Báo cáo và cảnh báo	Các báo cáo được tạo ra và được gửi tự động qua e-mail	
		Có khả năng tuỳ biến các báo cáo	
10	Bảo hành và hỗ trợ với phần mềm	≥ 24 tháng	
IV	**Giải pháp cổng một chiều (USG)**		**01**
1	Throughput	≥ 1Gbps	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
2	Giải pháp phải vận hành	Theo phương thức cho phép thông tin theo luồng một chiều từ thiết bị truyền dành riêng (dedicated transmit -TX module) tới thiết bị thu dành riêng (dedicated receiver - RX module) được đảm bảo qua đặc tính điện hoặc vật lý mà vai trò kênh truyền không bị đảo lại hoặc bị chuyển mạch bởi cấu hình phần mềm	
3	Giao thức hỗ trợ	S-FTP, TFTP,FTP-S, CIFS	
4	Yêu cầu hỗ trợ việc replicate Database	Oracle, MySQL, MSSQL.	
5	Tính sẵn sàng	Giải pháp hỗ trợ tuỳ chọn mở rộng sẵn sàng cao (High-Availability).	
6	Thiết kế module	Thiết bị gateway một chiều (cabinet) có thể chứa các host module và các module phát TX, module thu RX trong cùng phần cứng kích thức 1U	
7	Bảo hành và hỗ trợ kỹ thuật	≥ 24 tháng	
V	**Bản quyền giải pháp EPS**		**270**
1	Quản lý tập trung	Giải pháp cung cấp quản lý tập trung tất cả các máy trạm, thiết bị; phần mềm bảo mật đầu cuối; chính sách bảo mật; theo dõi giám sát.	
2	Tích hợp và nền tảng mở	Mở rộng giải pháp Symantec hiện có hoặc một giải pháp mới tương đương.	
3	Loại hiết bị được bảo vệ	Thiết bị bao gồm máy chủ, máy trạm.	
4	Quản trị	Có hệ thống quản trị tại chỗ (on-premised)	
		Hỗ trợ khả năng báo cáo, tìm kiếm thông tin theo thời gian thực, trong quá khứ và dữ liệu theo yêu cầu	
		Tích hợp với các hệ thống SIEM như IBM Qrada, Splunk	
5	Tính năng bảo mật	Phát hiện và ngăn chặn các loại mã độc: malware, ransomware, malicious scripts, unknown và new threats	
		Phát hiện và ngăn chặn mã độc chưa biết với công nghệ Signature-less bao gồm machine learning, behavioral analysis,...	
		Tích hợp tường lửa - Firewall	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
		Tích hợp tính năng phát hiện và phòng chống xâm nhập – Host Intrusion Prevention System	
		Tích hợp bảo vệ và lọc web - Web Filter	
		Tích hợp quản lý ứng dụng và thiết bị - Application and Device Control	
		Tự động phục hồi sự thay đổi gây ra bởi mã độc và đảm bảo hệ thống hoạt động ở trạng thái khoẻ mạnh gần nhất	
6	Hệ điều hành được hỗ trợ	Windows, MAC, Linux	
7	Phương thức quét	Hỗ trợ nhiều phương thức quét: Full Scan, Quick scan, Auto Protect, v.v…	
		Hỗ trợ thực hiện Quick scan 1 ngày / lần, Full scan 1 tuần/lần	
		Hỗ trợ tự động quét mã độc trên các file mới xuất hiện trên hệ thống (Từ các vật mang tin từ bên ngoài, dữ liệu được tải xuống từ internet, v.v…)	
8	Bảo hành và hỗ trợ kỹ thuật	≥ 24 tháng	
VI	**Bản quyền giải pháp PIM/PAM**		**01**
VI.1	**Phần mềm quản lý tài khoản đặc quyền**		
Các tính năng chung			
1	Yêu cầu số lượng tài khoản được quản trị	≥ 25	
2	Cung cấp bản quyền triển khai	Cung cấp tối thiểu 01 bản quyền triển khai tại DC và có sẵn 05 bản quyền triển khai dự phòng.	
3	Cung cấp bản quyền đầy đủ cho mục đích kiểm thử (sử dụng trong môi trường Kiểm tra & Phát triển - Test & Development)	Cung cấp 01 bộ bản quyền đầy đủ cho mục đích kiểm thử (sử dụng trong môi trường Kiểm tra & Phát triển - Test & Development)	
4	Thời hạn sử dụng bản quyền	Bản quyền không có thời hạn	
Yêu cầu kỹ thuật			
1	Có các thuật toán mã hóa	- AES-256, RSA-2048	
		- HSM integration	
		- FIPS 140-2 validated cryptography	
2	Có tính năng triển khai sẵn sàng cao	- Mô hình Clustering - Mô hình Multiple Disater Recovery sites	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
3	Có các phương thức xác thực	Username and Password, LDAP, Windows authentication, RSA SecurID, Web SSO, RADIUS, PKI, SAML	
4	Có tính năng tích hợp giám sát	- Tích hợp với hệ thống SIEM	
		- Tích hợp sử dụng giao thức SNMP	
		- Tích hợp cảnh báo qua kênh Email	
5	Có tính năng quản lý và bảo vệ thông tin đặc quyền (Credential Protection and Management)	- Ngăn chặn người dùng không hợp lệ sử dụng các tài khoản đặc quyền (privileged account)	
		- Cập nhật và đồng bộ mật khẩu của tài khoản đặc quyền và các SSH key theo theo chính sách thiết lập	
		- Bảo vệ các thông tin tài khoản đặc quyền sử dụng trên các môi trường on-premise	
		- Tự động hóa các quy trình quản lý tài khoản đặc quyền, thêm mới tài khoản onboarding, phân quyền permissions granting… qua việc tích hợp với các hệ thống khác sử dụng Rest API	
6	Có tính năng kiểm soát và giám sát phiên truy cập đặc quyền (Session Isolation and Monitoring)	- Thiết lập các phiên truy cập đặc quyền riêng biệt, ghi lại hành vi thực hiện. Người dùng ko trực tiếp kết nối đến các hệ thống, giảm thiểu rủi ro lây lan mã độc từ máy tính người dùng..	
		- Cung cấp công cụ kiểm soát các phiên truy cập SSH, người dùng có thể sử dụng để kết nối đến các hệ thống hỗ trợ SSH-based.	
		Giải pháp có khả năng kiểm soát truy cập, xác thực kép sử dụng cơ chế dual control.	
		Giải pháp có khả năng gửi báo cáo theo định kỳ.	
7	Có tính năng phân tích và phát hiện các hành vi bất thường (Privileged Analytics and Threat Detection)	- Phát hiện, cảnh báo theo thời gian thực (real-time) các hành vi nguy hại trong phiên truy cập đặc quyền của người dùng	
		- Xác định các hành vi bất thường của các tài khoản đặc quyền liên quan đến các nguy cơ tấn công vào hệ thống	
		- Sử dụng thuật toán tự học (machine learning) để tính toán các hành vi bình thường trong hệ thống và phát hiện sự thay đổi dựa trên đó	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
		- Đánh giá tương quan các sự kiện ghi nhận được và đưa vào cùng một sự cố. Và trong sự cố an toàn thông tin đó có chi tiết về hệ thống ảnh hưởng, tài khoản nghi ngờ thực hiện	
8	Bảo hành và hỗ trợ kỹ thuật	≥ 24 tháng	
VI.2	**Phần mềm quản lý cơ sở dữ liệu**		
1	Cung cấp bản quyền phần mềm quản lý cơ sở dữ liệu 10 users	Đáp ứng	
2	Yêu cầu tính năng	Nhận diện các dữ liệu nhạy cảm khi truy cập Cơ sở dữ liệu	
		Tích hợp công cụ SQL Editor	
		Có tính năng Query builder	
		Cho phép so sánh các Schema/Data	
		Có công cụ thực hiện Debugger/profiler	
		Có tính năng phân tích và báo cáo về các đoạn Code (Code quality)	
		Có tính năng SQL optimization (SQL Optimizer)	
3	Thời hạn sử dụng bản quyền	Bản quyền không có thời hạn	
VI.3	**Phần mềm truy cập hệ thống từ xa**		
1	Cung cấp bản quyền phần mềm terminal truy cập hệ thống từ xa	Cấp cho 10 users phiên bản Professional	
2	Quản lý phiên truy cập	Cho phép khởi tạo phiên kết nối từ xa sử dụng các giao thức như SSH, Telnet, Rlogin, RDP, VNC, XDMCP, FTP, SFTP hoặc Serial… các phiên truy cập sau đó được tự động lưu và hiển thị để tiếp tục sử dụng	
3	Cung cấp giao diện truy xuất SFTP	Cung cấp giao diện truy xuất sử dụng SFTP khi sử dụng SSH để truy cập máy chủ. Cho phép thực hiện kéo và thả tập tin	
4	Hỗ trợ tính năng Multi-execution	Cho phép thực hiện cùng một câu lệnh trên nhiều máy chủ khác nhau cùng một thời điểm	
5	Hỗ trợ tính năng Remote Unix desktop (XDMCP)	Cho phép thực hiện cùng một câu lệnh trên nhiều máy chủ khác nhau cùng một thời điểm	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
6	Hỗ trợ giao thức Remote Windows desktop (RDP)	Cho phép sử dụng RDP để kết nối tới máy chủ Windows	
7	Syntax highlighting in terminal	Cho phép làm nổi bật các cú pháp hoặc hiển thị theo màu sắc các từ khóa khác nhau trong cửa sổ terminal	
8	Thời hạn sử dụng bản quyền	Bản quyền không có thời hạn	
VI.4	**Bản quyền Remote Desktop Service**		
1	Cung cấp kèm bộ license Remote Desktop Service Per User CAL 25 users	Đáp ứng	
2	Yêu cầu tính năng	Cung cấp kết nối từ xa cho người dùng	
		Cho phép người dùng kết nối tới các thiết bị managed hoặc unmanaged	
		Có tính năng kết nối dưới dạng session-based hoặc virtual-machine	
3	Thời hạn sử dụng bản quyền	Bản quyền không có thời hạn	
VII	**Bản quyền giải pháp 2FA**		**01**
1	Số lượng người dùng được quản lý	≥ 1000 user	
2	Xác thực qua token	Khả năng xác thực qua token phần cứng và khả năng cung cấp mã mới mỗi 60 giây	
		Token phần cứng hỗ trợ thuật toán AES-128 và chống giả mạo	
		Khả năng tích hợp xác thực với hệ thống VPN và ứng dụng web	
		Cơ chế xác thực dựa trên rủi ro	
		Khả năng tính điểm rủi ro động, theo thời gian thực kết hợp với yếu tố ngữ cảnh	
3	Xác thực nâng cao	Có thành phần quản trị tập trung	
		Khả năng hiển thị cảnh báo với các chi tiết về sự kiện như thời gian, địa chỉ IP, người dùng, vị trí địa lý, địa chỉ email...	
		Khả năng triển khai theo mô hình tại chỗ	
4	Quản trị	Khả năng tích hợp với nhiều thành phần, giải pháp của bên thứ 3 như truy cập từ xa, truy cập đặc quyền, đám máy và ứng dụng đám mây, kiểm soát truy cập...	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
5	Triển khai	- Khả năng hỗ trợ LDAP, RADIUS, SAML, Trusted Headers… - Thiết kế triển khai đảm bảo khả năng dự phòng	
6	Bảo hành và hỗ trợ kỹ thuật	≥ 24 tháng	
VIII	**Bản quyền giải pháp SIEM**		**01**
1	License EPS hoặc tương đương	Tối thiểu 2500EPS	
2	Tính sẵn sàng	Thiết kế triển khai đảm bảo dự phòng HA	
3	Tính năng thu thập	Thu nhập nhật ký bao gồm các loại như:thiết bị mạng (Router, Switch...), thiết bị an ninh (Firewall, IDS/IPS, Database firewall, Antivirus...), hệ điều hành (Operating systems), ứng dụng (Application), cơ sở dữ liệu (Database)... Thu thập dữ liệu lưu lượng mạng bao gồm Netflow, Jflow, Sflow Thu thập nhật ký theo dạng Agen-less	
4	Tính năng truyền log	Lưu trữ nhật ký tạm thời, truyền trên kênh an toàn giữa các thành phần; lọc, tích hợp dữ liệu nhật ký trong khi thu thập (Filtering, Aggregation of data logs); quản lý băng thông sử dụng để truyền nhật ký từ thành phần thu thập đến các thành phần lưu trữ, phân tích; kết hợp các sự kiện (Aggregate events)	
5	Tính năng giám sát (Monitor)	Hỗ trợ giám sát (Monitor)	
6	Phân tích các trường thông tin (Field Sets)	Hỗ trợ phân tích các trường thông tin (Field Sets)	
7	Dữ liệu thu thập từ các thiết bị trong hệ thống mạng phải được phân tích bằng lược đồ chuẩn hóa (normalized schema).	Hỗ trợ dữ liệu thu thập từ các thiết bị trong hệ thống mạng phải được phân tích bằng lược đồ chuẩn hóa (normalized schema).	
8	Cho phép người quản trị thực hiện & tương tác với các trường sự kiện bao gồm: tạo mới, thay đổi, chia sẻ hay xóa bỏ	Hỗ trợ cho phép người quản trị thực hiện & tương tác với các trường sự kiện bao gồm: tạo mới, thay đổi, chia sẻ hay xóa bỏ	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
9	Các luật và phân tích sự tương quan (Rules & Correlation)	+ Cho phép phát hiện các hành động nghi ngờ và phá hoại (suspicious and malicious behavior) + Thực hiện phân tích sự tương quan (correlation) phải dựa vào mẫu (Signature) và phân tích sự bất thường của hành vi (behavior anomaly). + Thực hiện chức năng phân tích tính tương quan đối với dữ liệu theo thời gian thực (real-time) và dữ liệu trong quá khứ (historical data). + Các luật (rules) phải hỗ trợ thực hiện các hành động như sau: Gửi thông báo, thực thi một lệnh, tạo lập hồ sơ sự cố, đưa vào danh sách theo dõi…	
10	Bảo hành và hỗ trợ kỹ thuật	≥ 24 tháng	
IX	**Bản quyền giải pháp backup**		**01**
1	Thiết bị sao lưu chuyên dụng	Thiết bị dạng Appliance được tích hợp, cấu hình sẵn phần cứng, phần mềm với đầy đủ bản quyền phần mềm đi kèm.	
		Thiết bị có cấu hình tối thiểu: - Khả dụng với dung lượng ≥ 24 TB khả dụng (Raid 6); cho phép mở rộng tới 1.5 PB dung lượng logical. - Tốc độ sao lưu tối đa của thiết bị hỗ trợ ≥ 7TB/giờ - 4 cổng mạng Ethernet tốc độ 1Gb. - 2 cổng mạng Ethernet quang tốc độ 10Gb	
		- Tính năng yêu cầu: + Chống trùng lặp dữ diệu tại nguồn (source deduplication)	
		+ Tính năng chống trùng lặp dữ liệu deduplication phải được thực hiện thông qua việc cắt dữ liệu thành các đoạn biến thiên, variable-length segment, giúp tăng tỷ lệ chống trùng lặp và hiệu suất sao lưu.	
		+ Khả năng chống trùng lặp dữ liệu hiệu suất cao lên tới 40:1	
		+ Khả năng mã hóa dữ liệu sao lưu (Encryption): Dữ liệu sẽ được mã hoá ngay trong quá trình sao lưu.	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
		+ Bảo vệ dữ liệu sao lưu: có cơ chế chống lại Ransomware. Có sẵn cơ chế khóa bảo vệ dữ liệu khỏi sự sửa đổi, can thiệp, …bằng phần mềm của thiết bị sao lưu chuyên dụng.	
		- Tối thiểu 02 nguồn dự phòng, nguồn 220VAC	
		- Bảo hành và hỗ trợ kỹ thuật 3 năm	
2	Bản quyền phần mềm (tối thiểu 5 năm sử dụng)	Bản quyền sao lưu, khôi phục đáp ứng dung lượng dữ liệu nguồn hệ thống SCADA hiện nay (11TB), không giới hạn các loại dữ liệu sao lưu (hệ điều hành, files, databases Orcale, SQL, ứng dụng…), không giới hạn số node (máy chủ, máy trạm, thiết bị mạng…).	
		- Phần mềm đề xuất phải tương thích hoàn toàn với thiết bị sao lưu chuyên dụng (mục trên), là môt giải pháp tổng thể đồng nhất phần mềm và phần cứng của cùng hãng công nghệ để đảm bảo hạn chế rủi ro tích hợp và bảo hành bảo trì.	
		- Đáp ứng đầy đủ yêu cầu bảo vệ dữ liệu, khả năng sao lưu, khôi phục, chống trùng lặp.	
		- Giao diện quản lý tập trung trên nền Web	
		- Đặt lịch sao lưu theo điều kiện, sự kiện.	
X	**Yêu cầu máy chủ HCI**		
X.1	**Thiết bị Hyper Converge**		**04**
1	Chủng loại	Hyper-Conveged Appliance. Fully integrated, preconfigured, and tested hyper-converged infrastructure appliance	
2	Kiểu dáng	Rack 2U	
3	Bộ vi xử lý	02 x Intel CPU 32C 2.0 Ghz hoặc cao hơn	
4	Bộ nhớ	≥ 16 x 32 GB RDIMM Hỗ trợ 32 DDR4 DIMMs/ Dung lượng RAM tối đa hỗ trợ: ≥4096GB	
5	Lưu trữ cho OS/ Hypervisor	≥ 2 x 480GB SSD SATA M.2 /RAID 1	
6	Lưu trữ: Caching Tier	Tối thiểu 04 x 1600GB SSD cho mỗi node.	
7	Capacity Tier	Tối thiểu 12 x 12TB SAS Hot-Plug	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
8	Khay đĩa cứng	≥ 12 Hot Plug Hard Drive	
9	Card mạng:	4x10 GbE SFP+ / Khả năng nâng cấp tối đa 12x10 GbE SFP+ Các card mạng: có đầy đủ SFP+ SR 10Gbps, dây nhảy đi kèm	
10	Cổng quản trị	1x1 GbE RJ45	
11	Số nốt tối đa trên 1 cluster:	≥ 32	
12	Phần mềm tích hợp sẵn:	- Bảng hiển thị mức độ sử dụng storage, CPU và memory trong toàn bộ cluster, trong từng appliance node - Hướng dẫn người quản trị thêm node vào cluster, tự động nhận biết node khi online. - Theo dõi các sự kiện hệ thống và cung cấp các thông báo toàn diện đang diễn ra về trạng thái của môi trường ảo và phần cứng thiết bị.	
13	Tích hợp sẵn các dịch vụ dữ liệu cao cấp	- Toàn bộ dịch vụ này tích hợp sẵn trong thiết bị HCI appliance - Dịch vụ chẩn đoán, sửa chữa từ xa. - Dịch vụ bảo mật dữ liệu tích hợp sẵn trong Appliance bao gồm phần mềm cho phép sao lưu, khôi phục mức VM, tại chỗ hoặc từ xa thông qua replicate	
14	Bảo hành	≥ 36 tháng	
X.2	**Bản quyền phần mềm đối với mỗi thiết bị Hyper Converge**		
1	Phần mềm ảo hóa máy chủ (Hypervisor)	- License phần mềm ảo hóa máy chủ cho 02 CPU, hỗ trợ kỹ thuật 3 năm - Có khả năng quản lý mạng tập trung và mã hóa máy chủ ảo.	
2	Phần mềm ảo hóa lưu trữ (Storage virtualization)	- Phần mềm ảo hóa lưu trữ (Storage virtualization) tích hợp ngay trong kernel của phần mềm ảo hóa máy chủ, bản quyền cho 02 CPU hoặc toàn bộ dung lượng của thiết bị tại yêu cầu Storage - Capacity. - Có khả năng chống trùng lặp và nén dữ liệu	
3	Phần mềm ghi nhật ký (logging)	- License phần mềm ghi nhật ký của toàn bộ hạ tầng ảo hóa cho 02 CPU, hỗ trợ kỹ thuật 3 năm. Thu thập, quản lý nhật ký của toàn bộ môi trường, từ OS, apps, storage,…	
4	Phần mềm sao lưu máy chủ ảo	Backup software license for 5 VM licenses per node, khả năng sao lưu nội bộ hoặc giữa các site.	

STT	TÊN HẠNG MỤC	YÊU CẦU	SỐ LƯỢNG
5	Bảo hành	≥ 36 tháng	
XI	**Thiết bị Switch back-end**		**02**
1	Thiết bị Switch 10GbE đi kèm	Cấu hình mỗi cặp switch layer 3: - Số lượng port ≥ 24 port 1/10GbE - Transceiver đi kèm: ≥ 14 x 10GbE SFP+ SR và ≥ 04 x 1GbE RJ45	
2	Bảo hành	≥ 36 tháng	
XII	**Yêu cầu cho máy tính trạm**		**04**
1	Số lượng thiết bị	≥ 4 thiết bị đi kèm màn hình, bàn phím	
2	Chíp xử lý	Intel Core i7-11700k (2.5GHz turbo up to 4.9Ghz, 8 nhân 16 luồng, 16MB Cache, 65W) hoặc hiệu năng cao hơn	
3	Bộ nhớ Ram	1x16GB DDR4 3200 Mhz UDIMM non-ECC Memory, 4 UDIMM slots, Max 128 GB hoặc dung lượng cao hơn	
4	Ổ đĩa cứng	1TB HDD 3.5" Sata (x2 HDD 3.5" Sata + x1 SSD M2 PCIE NVME) hoặc dung lượng cao hơn	
5	Card đồ họa	Nvidia P2000 NVIDIA Quadro 5GB DDR5 - 4x mDP to DP hoặc hiệu năng cao hơn	
6	Ổ đĩa quang (DVD)	8x DVD+/-RW	
7	Cổng xuất hình	2x DisplayPort 1.4, HDMI	
8	Kết nối mạng LAN	10/100/1000 Mb/s	
9	Bảo hành	36 tháng	

1.6 Thiết kế phương án triển khai, đào tạo, vận hành

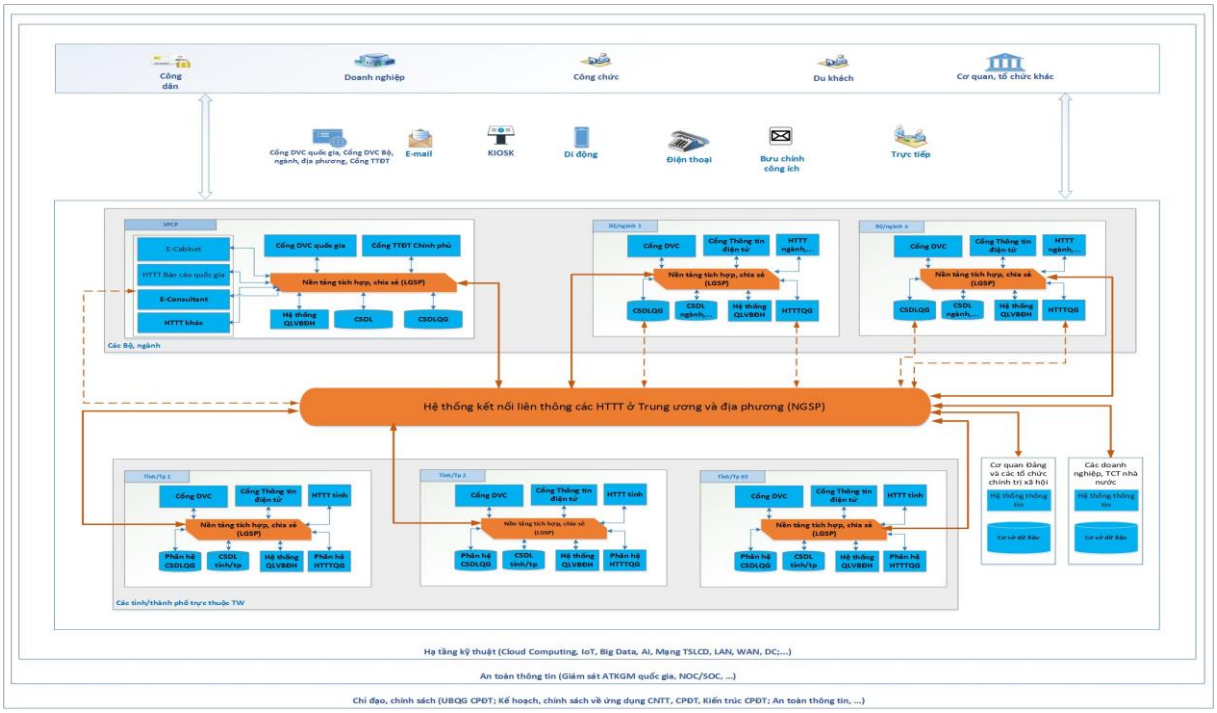
1.6.1 Đánh giá sự tuân thủ theo Khung Kiến trúc Chính phủ điện tử

Ngày 31/12/2019, Bộ Thông tin và Truyền thông đã ban hành Quyết định số 2323/QĐ-BTTTT Ban hành Khung Kiến trúc Chính phủ điện tử Việt Nam, phiên bản 2.0, nhằm hướng dẫn các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, UBND các tỉnh, thành phố trực thuộc Trung ương xây dựng Kiến trúc Chính phủ/Chính quyền điện tử; hình thành và triển khai áp dụng đồng bộ hệ thống Kiến trúc Chính phủ điện tử từ Trung ương đến địa phương.

Trong đó, các thành phần cơ bản của Kiến trúc Chính phủ điện tử bao gồm:

- Kiến trúc nghiệp vụ;
- Kiến trúc dữ liệu;
- Kiến trúc ứng dụng;
- Kiến trúc công nghệ;
- Kiến trúc an toàn thông tin.

Sơ đồ khái quát Kiến trúc Chính phủ điện tử Việt Nam:



Mô hình Kiến trúc Chính phủ điện tử, phiên bản 2.0

Trong đó dự án "Giải pháp an toàn, an ninh thông tin cho hệ thống giám sát, điều khiển và tự động hoá tại EVNHANOI" nhằm bảo đảm ATTT cho hệ thống SCADA – phục vụ cho sản xuất, kinh doanh tại EVNHANOI tuân thủ theo mô hình tham chiếu ATTT theo Kiến trúc CPĐT như sau:

STT	Mô hình tham chiếu ATTT theo Kiến trúc CPĐT	Mức độ tuân thủ hệ thống ATTT cho Hệ thống điều khiển trung tâm tại EVNHANOI
1	**Mục tiêu (SRM001)**	
	SRM001 bảo đảm ATTT đối với hệ thống thành phần trong Kiến trúc CPĐT được xác định là việc thực hiện bảo vệ hệ thống thông tin tuân thủ các quy định của pháp luật, căn cứ vào cấp độ an toàn của hệ thống thông tin, yêu cầu an toàn tối thiểu và phương án bảo vệ. Trên cơ sở đó, SRM001 bao gồm 02 hợp phần: (1) Quy định pháp lý và (2) Hồ sơ cấp độ.	Dự án nhằm bảo đảm ATTT cho hệ thống Điều khiển trung tâm – phục vụ cho sản xuất, kinh doanh tại EVNHANOI
a	SRM001.001 Quy định pháp lý SRM001.001.001 Luật SRM001.001.002 Nghị định SRM001.001.003 Thông tư hướng dẫn	Dự án được xây dựng căn cứ và tuân thủ theo: - Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ - Thông tư số 12/2022/TT-BTTTT

STT	Mô hình tham chiếu ATTT theo Kiến trúc CPĐT	Mức độ tuân thủ hệ thống ATTT cho Hệ thống điều khiển trung tâm tại EVNHANOI
	SRM001.001.004 Tiêu chuẩn, quy chuẩn kỹ thuật SRM001.001.005 Văn bản hướng dẫn	- Quyết định số 168/QĐ-EVN ngày 23/02/2023 của Tập đoàn Điện lực Việt Nam - Tiêu chuẩn TCVN 11930:2017/BTTTT
b	SRM001.002 Hồ sơ cấp độ SRM001.002.001 Cấp độ an toàn hệ thống thông tin SRM001.002.002 Phương án bảo vệ	Dự án nhằm đảm bảo hệ thống Điều khiển trung tâm đáp ứng cấp độ an toàn hệ thống thông tin cấp độ 3.
2	**Rủi ro (SRM002)**	
	Rủi ro mô tả các nguy cơ, rủi ro mất an toàn thông tin và biện pháp kiểm soát	
a	SRM002.001 Nguy cơ, rủi ro	
	- SRM002.001.001 Các nguy cơ, rủi ro mất an toàn thông tin xuất pháp từ bên ngoài hệ thống: Các nguy cơ, rủi ro mất an toàn thông tin xuất pháp từ bên ngoài hệ thống như: Tấn công DoS/DDoS, tấn công Deface, tấn công khai thác điểm yếu lỗ hổng bảo mật từ bên ngoài	Các nguy cơ, rủi ro mất an toàn thông tin xuất pháp từ bên ngoài hệ thống: - Các cuộc tấn công thông qua đường kết nối giữa hệ thống IT và OT. - Tấn công thông qua đường kết nối đến các nhà máy điện và trạm biến áp. - Các cuộc tấn công thông qua mạng đường trục WAN - Tấn công qua đường kết nối của nhà cung cấp dịch vụ Internet (Với hệ thống kết nối sử dụng VPN 3G VNPT) - Các cuộc tấn công có thể thực hiện bởi kẻ tấn công bên ngoài hoặc kẻ tấn công bên trong đặc biệt tại các thiết bị HMI máy trạm/ máy chủ đang sử dụng mật khẩu yếu .Những cuộc tấn công bên trong như vậy có thể hiện thực hóa thành một cuộc tấn công cố ý hoặc tạo ra một tổn thất do sai sót của con người.

STT	Mô hình tham chiếu ATTT theo Kiến trúc CPĐT	Mức độ tuân thủ hệ thống ATTT cho Hệ thống điều khiển trung tâm tại EVNHANOI
	- SRM002.001.002 Các nguy cơ, rủi ra mất an toàn thông tin xuất pháp từ bên trong hệ thống như: Tấn công mã độc, tấn công nghe lén, đánh cắp, lộ lọt thông tin, tấn công thông qua môi trường vật lý…	Các nguy cơ, rủi ra mất an toàn thông tin xuất pháp từ bên trong hệ thống như: - Các cuộc tấn công thông qua chuỗi cung cấp thiết bị mới (ví dụ lây nhiễm một RTU mới được lắp đặt trên mạng)
	- SRM002.001.003 Các nguy cơ, rủi ro mất an toàn thông tin khác theo đặc trưng của từng hệ thống cụ thể	Các nguy cơ, rủi ro mất an toàn thông tin khác theo đặc trưng của hệ thống OT tại EVNHANOI: - Hệ thống SCADA/DMS cao thế, mạng EVN-WAN giao tiếp với các trạm biến áp qua giao thức IEC-60870-5-104 (hay IEC-104) tồn tại nhiều điểm yếu bảo mật, chưa có bảo vệ cho giao thức IEC-104: Thiếu tính bảo mật: Nội dung thông điệp không được mã hóa dẫn đến giao thức IEC-104 có thể bị tấn công bằng cách nghe lén (sniffer) để đánh cắp thông tin, sửa mã lệnh điều khiển làm thay đổi vận hành của hệ thống, tấn công trên đường truyền của giao thức. Thiếu tính xác thực: Các thiết bị sử dụng giao thức IEC-104 không cần xác thực khi kết nối vào mạng, do đó có thể bị tấn công MITM (Man-In-The-Middle) từ cách này có thể tấn công chiếm quyền điều khiển thiết bị vận hành như BCU... Độ dài khung truyền ngắn là nguyên nhân có thể bị tấn công làm tràn bộ đệm (buffer overflow) của thiết bị. Cụ thể, độ dài khung truyền tối đa giao thức IEC-104 là 255 Byte hoàn toàn có thể bị tấn công làm tràn bộ đệm làm thiết bị trong hệ thống dừng hoạt động

STT	Mô hình tham chiếu ATTT theo Kiến trúc CPĐT	Mức độ tuân thủ hệ thống ATTT cho Hệ thống điều khiển trung tâm tại EVNHANOI
b	SRM002.002 Biện pháp kiểm soát	
	- SRM002.002.001 Thực thi phương án bảo vệ theo Hồ sơ cấp độ được phê duyệt để đáp ứng các yêu cầu cơ bản về quản lý và kỹ thuật.	- Các giải pháp ATTT trong Dự án đang bám sát yêu cầu theo thông tư 12/2022/TT-BTTTT dành cho hệ thống cấp độ 3 và tập trung vào giải quyết các rủi ro trước mắt như đã phân tích ở trên. - Xây dựng Hồ sơ cấp độ 3 cho hệ thống Điều khiển trung tâm để cán bộ chuyên trách của EVNHANOI phê duyệt, ban hành và hướng dẫn cho các đơn vị thực thi. (Tham khảo phụ lục: Thuyết minh phương án đảm bảo an toàn hệ thống thông tin cấp độ 3)
	- SRM002.002.002 Kiểm tra, đánh giá an toàn thông tin – Việc thực hiện kiểm tra, đánh giá an toàn thông tin, thử nghiệm xâm nhập hệ thống nhằm phát hiện mã độc, lỗ hổng, điểm yếu và các nguy cơ, rủi ro mất an toàn thông tin khác có thể xảy ra với hệ thống.	Phạm vi việc thực hiện kiểm tra, đánh giá an toàn thông tin, thử nghiệm xâm nhập hệ thống không bao gồm trong Dự án mua sắm "Giải pháp an toàn, an ninh thông tin cho hệ thống giám sát, điều khiển và tự động hoá tại EVNHANOI" Đơn vị tư vấn đề xuất EVNHANOI tối thiểu mỗi năm một lần (đối với các hệ thống được phê duyệt cấp độ 3) cử cán bộ chuyên trách hoặc thuê đơn vị độc lập chuyên nghiệp tiến hành: - Kiểm tra, rà soát trên các thiết bị máy chủ nhằm xác định các dấu vết tấn công và xâm nhập (Compromise Assessment) đang diễn ra hoặc đã xảy ra trong quá khứ trên hệ thống OT của EVNHANOI, đánh giá quy mô thiệt hại, xác định tài sản bị ảnh hưởng và cách thức xảy ra. - Kiểm thử tấn công xâm nhập (Pentest) nhằm xác định tất cả các lỗ hổng bảo mật, các nguy cơ tồn tại

STT	Mô hình tham chiếu ATTT theo Kiến trúc CPĐT	Mức độ tuân thủ hệ thống ATTT cho Hệ thống điều khiển trung tâm tại EVNHANOI
		trên hệ thống/ứng dụng theo phạm vi được chỉ định và đánh giá mức độ rủi ro, mức độ ảnh hưởng tồn tại đồng thời đưa ra phương án khắc phục, giảm thiểu rủi ro. Lưu ý: Cần đánh giá khả năng gián đoạn ứng dụng trong quá trình kiểm thử, chỉ nên tiến hành kiểm thử trên các ứng dụng IT. - Kiểm tra, đánh giá cấu hình (Audit) các thiết bị mạng, bảo mật, máy chủ để đánh giá các rủi ro mất an toàn thông tin khác có thể xảy ra với hệ thống.
	- SRM002.002.003 Giám sát an toàn thông tin – Triển khai phương án giám sát an toàn thông tin nhằm phát hiện sớm nhất các cuộc tấn công mạng đối với hệ thống của mình.	Phạm vi việc thực hiện giám sát an toàn thông tin nhằm phát hiện sớm nhất các cuộc tấn công mạng đối với hệ thống không bao gồm trong Dự án mua sắm "Giải pháp an toàn, an ninh thông tin cho hệ thống giám sát, điều khiển và tự động hoá tại EVNHANOI" Đơn vị tư vấn đề xuất EVNHANOI thành lập đội cán bộ chuyên trách về giám sát ATTT (SOC) hoặc thuê đơn vị độc lập chuyên nghiệp tiến hành: - Giám sát và cảnh báo ATTT 24/7 cho hệ thống OT tại EVNHANOI. - Ứng cứu, xử lý sự cố ATTT cho hệ thống OT tại EVNHANOI nhằm đảm bảo hệ thống có thể khôi phục hoạt động bình thường sớm nhất có thể sau sự cố.
	- SRM002.002.004 Xây dựng hệ thống phương án ứng cứu, xử lý sự cố - Xây dựng hệ thống phương án ứng cứu, xử lý sự cố nhằm đảm bảo hệ thống có thể khôi phục hoạt động	Phạm vi việc thực hiện giám sát an toàn thông tin nhằm phát hiện sớm nhất các cuộc tấn công mạng đối với hệ thống không bao gồm trong Dự án mua sắm "Giải pháp an toàn, an

STT	Mô hình tham chiếu ATTT theo Kiến trúc CPĐT	Mức độ tuân thủ hệ thống ATTT cho Hệ thống điều khiển trung tâm tại EVNHANOI
	bình thường sớm nhất có thể sau sự cố.	ninh thông tin cho hệ thống giám sát, điều khiển và tự động hoá tại EVNHANOI" Đơn vị tư vấn đề xuất EVNHANOI thành lập đội cán bộ chuyên trách về giám sát ATTT (SOC) hoặc thuê đơn vị độc lập chuyên nghiệp tiến hành: - Giám sát và cảnh báo ATTT 24/7 cho hệ thống OT tại EVNHANOI. - Ứng cứu, xử lý sự cố ATTT cho hệ thống OT tại EVNHANOI nhằm đảm bảo hệ thống có thể khôi phục hoạt động bình thường sớm nhất có thể sau sự cố.

1.6.2 Giải pháp về tính sẵn sàng với IPv6

- Hệ thống phần cứng, phần mềm trong Dự án "Giải pháp an toàn, an ninh thông tin cho hệ thống giám sát, điều khiển và tự động hoá tại EVNHANOI", sẽ không có kết nối và giao dịch trực tiếp với Internet. Do vậy, các ứng dụng và các thiết bị tại đây hoàn toàn sử dụng các địa chỉ IPv4 mạng nội bộ cho tất cả các trạm máy chủ, thiết bị mạng, bảo mật và PC bên trong các TTDL.
- Tuy nhiên, với sự tồn tại của các trạm IPv6 trên Internet hiện nay, một số yếu tố và đặc tính liên quan đến IPv6 có thể được biểu diễn trong các dữ liệu liên quan đến vận hành hệ thống ứng dụng sẽ được thu thập và phân tích, xử lý. Các yếu tố này bao gồm địa chỉ nguồn dạng IPv6 trong các dữ liệu nhật ký truy cập (access logs) hay các địa chỉ IPv6 được phân giải từ bản ghi AAA truy vấn từ máy chủ tên miền DNS, cũng trong các nhật ký (logs) lưu trữ thông tin giao dịch dữ liệu. Ngoài ra, các dữ liệu liên quan đến IPv6 còn có thể xuất hiện trong các URL trỏ tới các trang web sử dụng địa chỉ này, hoặc các phương pháp xác định vị trí dựa trên IP (IP Geolocation).
- Để đảm bảo cho việc vận hành ứng dụng trong môi trường tồn tại thông tin IPv6 như vừa nêu được liền lạc, các ứng dụng có liên quan đến truy vấn, xử lý các thông tin có thể xuất hiện dữ liệu IPv6 sẽ được lưu ý sử dụng các thư viện hỗ trợ IPv6 (IPv6 ready library). Toàn bộ các sản phẩm phần mềm thương mại được sử dụng trong hệ thống cũng sẽ được kiểm tra đảm bảo tiêu chí hỗ trợ IPv6 này.

1.6.3 Đào tạo hướng dẫn sử dụng

1.6.3.1 Phương pháp đào tạo, chuyển giao công nghệ

Việc đào tạo chuyển giao công nghệ được thực hiện dựa trên các khóa chuẩn của hãng cung cấp và bởi các giảng viên được công nhận của hãng cung cấp. Sau khi kết thúc khóa học, học viên được cấp chứng chỉ tham dự khóa học.

Học viên được đào tạo theo mô hình lý thuyết và thực hành xen kẽ.

Khóa học sẽ đưa ra các ví dụ, hình ảnh minh họa cụ thể, các bài tập tình huống, câu hỏi ôn tập trắc nghiệm kiến thức và giải đáp câu hỏi. Giáo trình, chương trình và việc giảng dạy cho phép trao đổi, tương tác linh hoạt giữa giảng viên -học viên, học viên- học viên và học viên-chương trình làm tăng khả năng ghi nhớ so với cách tiếp cận tự học bình thường. Ngoài ra việc tự đọc trước tài liệu ở nhà và khả năng làm việc nhóm sẽ được khuyến khích để giúp tiết kiệm thời gian học và cho phép học viên chia sẻ các kiến thức, kinh nghiệm và hỗ trợ nhau trong suốt quá trình học tập.

Sau khoá học, giảng viên sẽ tiến hành đánh giá kết quả học tập của học viên, đồng thời lấy nhận xét của học viên về nội dung khoá học, phương pháp giảng dạy, nội dung đào tạo... để tổng kết rút kinh nghiệm cho giảng viên và đơn vị trong công tác tổ chức đào tạo.

1.6.3.2 Hình thức đào tạo

Đào tạo tập trung ngắn hạn, các khóa học được chia ra thành từng phần học hợp lý. Tùy theo khảo sát đánh giá trên lớp của giáo viên về nhu cầu công tác thực tế và kinh nghiệm làm việc của học viên, thời lượng giữa các phần học có thể được điều chỉnh linh hoạt nhằm trong cùng một thời gian có thể giúp học viên lĩnh hội được những kiến thức và khả năng thực hành phù hợp nhất. Kiểm tra đánh giá: Việc kiểm tra vào cuối lớp học, thông qua những bài kiểm tra giúp học viên nắm được những kiến thức cơ bản của từng bài học:

- Tài liệu giảng dạy: học viên được cung cấp tài liệu học đầy đủ dạng điện tử hoặc dạng in tùy thuộc vào khóa học.
- Giáo viên giảng dạy: Mỗi lớp học có 01 giảng viên chính và 02 trợ giảng
- Đào tạo trong quá trình triển khai (on-the-jobtraining), đào tạo trong quá trình quản lý, vận hành:
- Hướng dẫn thực hiện khi có sự cố thực tế, cách khắc phục, điều tra
- Đào tạo trong quá trình cùng làm việc.

1.6.3.3 Nội dung đào tạo, chuyển giao công nghệ

1.6.3.3.1 Khóa đào tạo nhận thức về ATTT

a. Đối tượng đào tạo:

- Các cán bộ điều độ, các cán bộ chuyên trách CNTT tại EVNHANOI.
- Các cán bộ khác có thao tác, kết nối vào hệ thống Điều khiển trung tâm.

b. Mục tiêu khóa học:

- Nâng cao nhận thức về ATTT cho các cán bộ điều độ, các cán bộ chuyên trách CNTT tại EVNHANOI.

- Giúp học viên hiểu được tầm quan trọng của ATTT cũng như các hậu quả một khi ATTT không được tuân thủ. Khoá học không chỉ cung cấp một cái nhìn toàn cảnh về ATTT mà còn cung cấp các kiến thức cần thiết cho một cuộc sống số an toàn hơn.

c. Tổ chức khóa học:

- Nội dung được tổ chức thành 01 khóa học
- Đào tạo tối thiểu 05 ngày làm việc cho mỗi khóa

d. Nội dung khóa học:

- Nhận biết các hiểm họa và rủi ro ATTT thường trực đe dọa hoạt động và tài sản của tổ chức trong hoạt động thường ngày, sử dụng ngân sách hợp lý hơn cho việc đảm bảo An ninh thông tin và hoạt động thông suốt của tổ chức.
- Một số kiểu tấn công nguy hiểm nhất nhắm vào doanh nghiệp:
  - Social Engineering là gì? Các thủ đoạn Social Engineering thường gặp
  - Phishing
  - Tìm hiểu về tấn công có chủ đích (APT)
  - Tấn công mã hóa dữ liệu và tống tiền
- Một số chỉ dẫn căn bản và thiết thực về ATTT dành cho người dùng cuối
- Một số kỹ năng ATTT thiết yếu trong công việc hàng ngày và cuộc sống số:
  - Phần mềm diệt Virus
  - Mật khẩu và quản lý Mật khẩu
  - Sử dụng Email an toàn
  - Sử dụng Web an toàn
  - Mẹo an toàn cho Shopping và Banking trực tuyến
  - An toàn trên mạng xã hội
  - An toàn khi sử dụng thiết bị di động (tải ứng dụng, quản lý thiết bị...)
  - An toàn khi sử dụng mạng không dây
- Phối hợp tốt hơn với các bộ phận liên quan khi đề xuất, phê duyệt, triển khai các dự án về ATTT

1.6.3.3.2 Khóa đào tạo nâng cao hiểu biết về ATTT

a. Đối tượng đào tạo:

- Các cán bộ quản trị mạng và quản trị hệ thống
- Các cán bộ phụ trách ATTT
- Số lượng học viên: Tối đa 12 học viên mỗi lớp.

b. Mục tiêu khóa học:

- Nâng cao hiểu biết về ATTT cho các cán bộ chuyên trách về CNTT tại EVNHANOI.
- Cung cấp các kiến thức cơ bản về ATTT bao gồm các nguyên tắc bảo mật mạng cần thiết và quản lý rủi ro cũng như nguy cơ mất an ninh hệ thống mạng.

c. Tổ chức khóa học:

- Nội dung được tổ chức thành 02 khóa học
- Đào tạo tối thiểu 1 tuần (07 ngày làm việc) cho mỗi khóa

d. Nội dung khóa học:

Nội dung khóa 01 như sau:

- Xác định các chiến lược tấn công mạng và máy chủ bởi các đối thủ mạng và đề xuất các biện pháp phòng chống.
- Nắm rõ các quy tắc về an ninh tổ chức và các yếu tố của chính sách bảo mật hiệu quả.
- Hiểu về những công nghệ và cách sử dụng của các tiêu chuẩn và sản phẩm mã hóa.
- Cài đặt và cấu hình các công nghệ bảo mật dựa trên mạng và máy chủ.
- Nội dung khóa 02 như sau:
- Mô tả cách cách thức bảo mật từ xa và bảo mật không dây.
- Mô tả các tiêu chuẩn và sản phẩm được sử dụng để thực thi bảo mật dựa trên các công nghệ web và truyền thông.
- Xác định các chiến lược nhằm đảm bảo tính liên tục trong kinh doanh và phục hồi sau thảm họa.
- Giới thiệu các lỗ hổng bảo mật và ứng dụng đồng thời đề xuất các biện pháp triển khai nhằm hạn chế nguy cơ mất an ninh mạng.

1.6.3.3.3 Khóa đào tạo thực thi, vận hành hệ thống

a. Đối tượng đào tạo:

- Các cán bộ quản trị mạng và quản trị hệ thống
- Các cán bộ phụ trách ATTT
- Số lượng học viên: Tối đa 12 học viên mỗi lớp.

b. Mục tiêu khóa học:

Khóa học này sẽ cung cấp cho học viên những cơ sở lý thuyết và hướng dẫn thực tiễn trong việc thiết kế, thiết lập cấu hình các luồng thông tin liên lạc và quản lý các nguồn dữ liệu của các firewall, của các công cụ an toàn bảo mật khác. Học viên sẽ hiểu cách làm để thực hiện một cách có hiệu quả việc kiểm soát trong một môi trường phức tạp để hiệu chỉnh và bảo trì hệ thống an toàn bảo mật.

c. Tổ chức khóa học:

- Nội dung được tổ chức thành 06 khóa học
- Đào tạo tối thiểu 05 ngày làm việc cho mỗi khóa

d. Nội dung khóa học:

Giới thiệu các bài học về giao diện và hướng dẫn trực tiếp, trong đó học viên sẽ hiểu được các khái niệm vận hành kiến trúc hệ thống, vấn đề triển khai mạng, phương pháp điều tra của các công cụ an toàn bảo mật.

Các nội dung chính sẽ bao gồm trong khóa học này là:

Nội dung 01: Giới thiệu thổng quan

- Giới thiệu tổng quan về hệ thống bao gồm các giải pháp bảo mật tường lửa (Firewall), Giải pháp cổng một chiều USG/Datadiode, Giải pháp phòng chống mã độc cho điểm cuối (EPS), Giải pháp quản lý mật khẩu/ tài khoản đặc quyền PIM/PAM, Giải pháp xác thực đa yếu tố (MFA), Giải pháp quản lý thông tin và

sự kiện an ninh mạng (SIEM). Mô tả kiến trúc bảo mật mạng doanh nghiệp, bao gồm mục đích và chức năng của VPN, bảo mật nội dung, ghi nhật ký, bảo mật điểm cuối, tường lửa và các tính năng bảo mật khác.

- Các thuật ngữ cơ bản, giới thiệu từng giải pháp
- Kiến trúc, tính năng của từng giải pháp

Nội dung 02: Vận hành hệ thống mạng (Firewall, USG, Switch)

- Triển khai kiến trúc và mạng: Cài đặt và định cấu hình các thành phần mạng, cả phần cứng và phần mềm, để hỗ trợ bảo mật tổ chức.
- Mục đích và tính năng của các thiết bị mạng
- Lựa chọn thành phần, thiết bị mạng theo đặc tả
- Sử dụng mô hình OSI, TCP/IP và các giao thức liên quan để giải thích dòng chảy dữ liệu trong mạng máy tính
- Các ứng dụng mạng phổ biến
- Mục đích và các hoạt động cơ bản của các giao thức trong mô hình OSI và TCP.
- Đọc sơ đồ mạng
- Xác định đường đi giữa 2 host trong mạng
- Các thành phần cần thiết cho liên lạc mạng và Internet
- Xác định và sửa lỗi mạng tại các tầng 1,2,3 và 7 theo phương pháp mô hình 7 lớp mạng
- Phân biệt hoạt động và tính năng giữa 2 mạng LAN và WAN
- Cấu hình địa chỉ IP và dịch vụ IP phù hợp với mạng văn phòng cỡ vừa
- Hoạt động và tính năng của địa chỉ IP cá nhân, công cộng
- Hoạt động và tính năng của DHCP
- Cấu hình, kiểm tra và sửa lỗi DHCP và DNS (bao gồm CLI/SDM)
- Xác định các nguy cơ bảo mật mạng và giải pháp tương ứng
- Chính sách bảo mật tổng thể để giảm thiểu nguy cơ
- Các phương pháp cơ bản để giảm thiểu nguy cơ bảo mật trên các thiết bị mạng, host và ứng dụng

Nội dung 03: Vận hành hệ thống SIEM

- Tạo ra quy tắc tương quan và chính sách của hệ thống (hiệu chỉnh hệ thống): Giải thích các quy trình và khái niệm quản lý rủi ro, đưa ra các chính sách cho hệ thống, Tóm tắt các khái niệm cơ bản về pháp y.
- Thu thập sự cố và điều tra tương quan sự cố: Đưa ra một số tình huống, khắc phục sự cố bảo mật phổ biến, Đưa ra một số kịch bản, phân tích và diễn giải đầu ra từ các công nghệ bảo mật.
- Phát hiện xâm nhập, ngăn ngừa các bước làm giảm nhẹ tổn thất: Đưa ra một số kịch bản, tuân theo các quy trình ứng phó sự cố. Đưa ra một số tình huống, thực hiện các phương pháp bảo mật dữ liệu và quyền riêng tư.
- Cập nhật hệ thống (cập nhật dựa trên các dấu hiệu, thông tin tình báo).

Nội dung 04: Vận hành hệ thống Backup

- Cách thức vận hành thành phần phần cứng, cấu hình mạng

- Cách thức sử dụng phần mềm để đặt lịch, cấu hình sao lưu, khôi phục dữ liệu
- Sử dụng các tính năng đảm bảo tính bảo mật của dữ liệu.
- Cấu hình tích hợp và quản lý thiết bị lưu trữ, tape

Nội dung 05: Vận hành hệ thống Endpoint, MFA, PAM

- Cách thức cài đặt, cấu hình, các giải pháp
- Áp dụng các giải pháp vào quy trình vận hành

Khóa 06: Vận hành hệ thống HCI

- Cách thức vận hành máy chủ vật lý, hiểu biết các thành phần phần cứng và công cụ quản trị.
- Nội dung cơ bản về phần mềm ảo hóa
- Cách thức sử dụng công cụ quản trị ảo hóa để tạo máy ảo, cấu hình, quản trị mạng ảo, cấu hình và quản trị storge ảo, giám sát và quản lý tài nguyên.

1.6.3.3.4 Khoá đào tạo bảo trì

a. Đối tượng đào tạo:

- Các cán bộ quản trị mạng và quản trị hệ thống
- Các cán bộ phụ trách ATTT
- Số lượng học viên: Tối đa 12 học viên mỗi lớp

b. Mục tiêu khóa học:

- Cung cấp kiến thức cần thiết để duy trì các chức năng vận hành của hệ thống.

c. Tổ chức khóa học:

- Nội dung được tổ chức thành 04 khóa học
- Đào tạo tối thiểu 05 ngày làm việc cho mỗi khóa

d. Nội dung đào tạo:

Đào tạo tối thiểu 05 ngày với các nội dung sau:

- Làm quen phần cứng hệ thống, hiểu kiến trúc hệ thống và các luồng dữ liệu có thể thực hiện được bảo trì hệ thống.
- Có thể chạy được, kiểm tra được hệ thống cơ bản bao gồm hệ thống HCI, hệ thống sao lưu dữ liệu, hệ thống Firewall và quản lý Firewall tập trung.
- Có thể thu thập được các log của hệ thống, thay đổi mức hiệu chỉnh và làm việc với các ứng dụng bảo trì chính, cấu hình Syslog.

Nội dung 01: Giải pháp Firewall, USG

- Bảo trì và cập nhật phần mềm về hệ thống phòng thủ bao gồm các giải pháp bảo mật tường lửa (Firewall), Giải pháp cổng một chiều USG/Datadiode

Nội dung 02: Giải pháp HCI, backup

- Bảo trì và cập nhật phần mềm về các giải pháp HCI, backup.

Nội dung 03: Giải pháp SIEM

- Bảo trì và cập nhật phần mềm về hệ thống phòng thủ bao gồm các giải pháp bảo mật: Giải pháp quản lý thông tin và sự kiện an ninh mạng (SIEM).
- *Nội dung 04: Các giải pháp còn lại bao gồm: MFA, EPS, PAM*

- Bảo trì và cập nhật phần mềm về hệ thống phòng thủ bao gồm các giải pháp bảo mật Giải pháp phòng chống mã độc cho điểm cuối (EPS), Giải pháp quản lý mật khẩu/ tài khoản đặc quyền PIM/PAM, Giải pháp xác thực đa yếu tố (MFA).

1.6.4 Phương án tổ chức quản lý, khai thác, sử dụng dự án

1.6.4.1 Phương án tổ chức quản lý thực hiện dự án

Ban QLDA tiến hành thủ tục để mở thầu, lựa chọn nhà thầu.

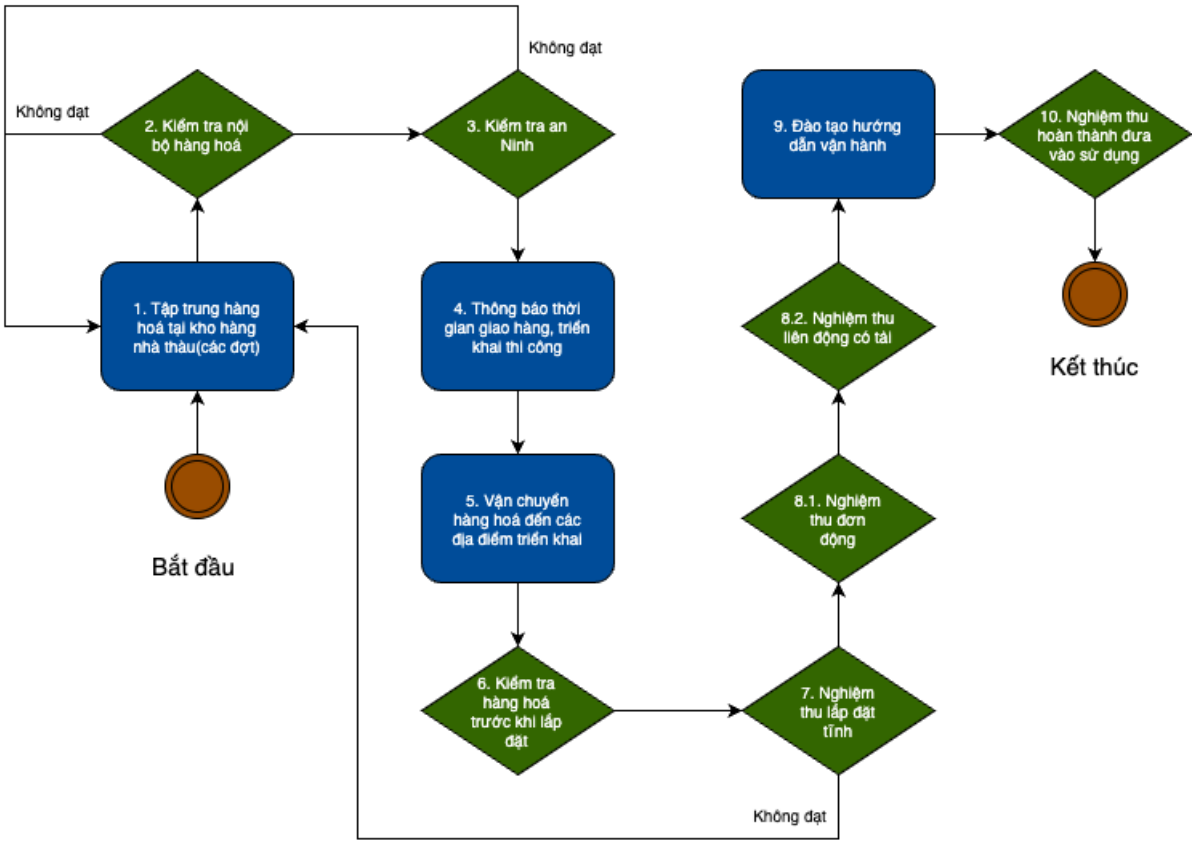
Sau khi hoàn thành lựa chọn Nhà thầu, kí hợp đồng, hợp đồng có hiệu lực, ban QLDA và đơn vị QLVH quản lý việc triển khai của Nhà thầu được lựa chọn.

Nhà thầu phối hợp với đơn vị QLVH để thực hiện việc cài đặt, lắp đặt thiết bị theo đúng số lượng, yêu cầu kỹ thuật theo dự án mua sắm "Giải pháp an toàn, an ninh thông tin cho hệ thống giám sát, điều khiển và tự động hoá tại EVNHANOI" và hợp đồng.

Sau khi hoàn thành việc triển khai, chủ trì ban QLDA, đơn vị QLVH và Nhà thầu tiến hành nghiệm thu tổng thể hệ thống hạ tầng để đưa hệ thống vào sử dụng. Chất lượng hàng hoá phải đảm bảo theo đúng yêu cầu đưa ra trong hợp đồng.

1.6.4.2 Phương án tổ chức triển khai

Trình tự triển khai dự án được mô tả theo sơ đồ sau:



TKTC-BV 30 Phương án tổ chức triển khai

1.6.4.2.1 Tập trung hàng hóa tại kho hàng của Nhà thầu

- Bố trí chuẩn bị địa điểm kho hàng tại Hà Nội với đầy đủ các yêu cầu về điều kiện môi trường, an ninh, bảo vệ.
- Tập trung toàn bộ hàng hóa theo phạm vi cung cấp của hợp đồng và các phụ lục.
- Kiểm tra nội bộ toàn bộ các hàng hóa (hoặc theo đợt bàn giao).

1.6.4.2.2 Kiểm tra nội bộ hàng hóa (vật tư, thiết bị phần cứng, phần mềm)

- Các hàng hóa đều phải được kiểm tra về chủng loại, quy cách, xuất xứ theo hồ sơ chất lượng đã được quy định trong hợp đồng. Kết quả kiểm tra phải được lập thành biên bản, ghi rõ chủng loại, quy cách, số lượng vật tư, thiết bị đưa vào công trường từng đợt, có ký xác nhận của đại diện bộ phận giám sát và đại diện bộ phận triển khai thi công của Nhà thầu. Hai bộ phận ký xác nhận theo mẫu.
- Trường hợp các vật tư, thiết bị công nghệ thông tin, phần mềm không phù hợp với thiết kế chi tiết được duyệt và hợp đồng đã ký, bộ phận giám sát yêu cầu bộ phận triển khai đưa ra khỏi khu vực tập kết hàng hóa;
- Hồ sơ chất lượng vật tư, thiết bị bao gồm:
  - Giấy chứng nhận xuất xứ (CO) của vật tư, thiết bị.
  - Giấy chứng nhận chất lượng (CQ) của vật tư, thiết bị do Hãng / nhà phân phối cấp;
  - Giấy chứng nhận bản quyền phần mềm.

1.6.4.2.3 Kiểm tra an ninh

- Chủ đầu tư/Ban QLDA sẽ có trách nhiệm mời Đơn vị chuyên trách thực hiện kiểm tra an ninh toàn bộ các thiết bị chính trong dự án tại kho tập kết hàng hóa của Nhà thầu.
- Quy trình kiểm tra an ninh sẽ do đơn vị chuyên trách đảm nhiệm với sự phối hợp của Nhà thầu, Đại diện Ban QLDA và sự tham gia của Bộ phận CBSX/Tiếp nhận vận hành hệ thống (nếu có).
- Kết thúc quá trình kiểm tra an ninh sẽ được các Bên ký biên bản xác nhận.

1.6.4.2.4 Thông báo thời điểm tiến hành triển khai thi công tại từng đơn vị, thiết lập kênh truyền/tuyến cáp.

- Nhà thầu căn cứ kế hoạch triển khai, thông báo cho Ban QLDA về thời điểm bắt đầu triển khai, tính từ khi bắt đầu vận chuyển hàng hóa đến địa điểm triển khai cho đến thời điểm nghiệm thu hoàn thành, đưa vào sử dụng từng hệ thống thành phần tại từng địa điểm. Ban QLDA thông báo cho Đơn vị QLVH, Đơn vị tiếp nhận Hệ thống trước khi triển khai tại các đơn vị tối thiểu 15 ngày.
- Ban QLDA thông báo cho Đơn vị phụ trách khai kênh truyền/cấp tuyến cáp thực hiện việc khai báo kênh truyền/ cấp tuyến cáp trước khi triển khai tại các đơn vị 15 ngày. Các bên gồm Nhà thầu, Ban QLDA, Đơn vị cấp kênh sẽ ký xác nhận biên bản thiết lập kênh truyền/tuyến cáp.

1.6.4.2.5 Vận chuyển hàng hóa về địa điểm triển khai

- Căn cứ theo yêu cầu tại từng địa điểm triển khai gồm:
  - Tại địa điểm Số 69 Đinh Tiên Hoàng: Ban QLDA bố trí 01 phòng kho tạm phục vụ công tác lưu kho trong quá trình vận chuyển, lắp đặt và triển khai thiết bị của Nhà thầu. Thời gian lưu kho từ 2-5 ngày/đợt
  - Tại các địa điểm khác: Các đơn vị QLVH Hệ thống IT/SCADA/DCS bố trí 01 phòng kho tạm phục vụ công tác lưu kho trong quá trình vận chuyển, lắp đặt và triển khai thiết bị của Nhà thầu. Thời gian lưu kho 1-3 ngày/đợt.

Bảng phân bổ hàng hoá, thiết bị như sau:

STT	Đơn vị	Địa điểm	Thiết bị phân bổ
1	Trung tâm điều khiển	Số 69 Đinh Tiên Hoàng, Phường Lý Thái Tổ, Quận Hoàn Kiếm, Thành phố Hà Nội, Việt Nam	02 Firewall core, 15 Firewall dự phòng 01 thiết bị USG/Datadiode Hệ thống backup Hệ thống HCI Máy trạm
2	Trạm biến áp không người trực		
3	Trạm biến áp không người trực	E1.1 Đông Anh	01 Firewall
		E1.16 Nội Bài	01 Firewall
		E1.41 Mai lâm	01 Firewall
		E1.42 Sân bay Nội Bài	01 Firewall
		E1.49 Đông Anh 2	01 Firewall
		E1.17 Bắc Thăng Long	01 Firewall
		E1.24 Hải Bối	01 Firewall
		E1.36 Quang Minh	01 Firewall
		E1.8 Yên Phụ	01 Firewall
		E1.9 Nghĩa Đô	01 Firewall
		E1.14 Giám	01 Firewall
		E1.21 Nhật Tân	01 Firewall
		E1.40 Tây Hồ	01 Firewall
		E1.63 Bắc Thành Công	01 Firewall
		E1.7 Sơn Tây	01 Firewall
		E1.28 Phùng Xá	01 Firewall
		E1.44 Sơn Tây 2	01 Firewall
		E1.48 Quốc Oai	01 Firewall
		E10.6 Phúc Thọ	01 Firewall
		E1.53 Ba Vì	01 Firewall
		E1.54 Hòa Lạc	01 Firewall
		E1.20- Thanh Xuân	01 Firewall
		E1.25- Mỹ Đình	01 Firewall
		E1.31 Trôi	01 Firewall
		E1.33 Cầu Diễn	01 Firewall
		E1.37 Bắc An Khánh	01 Firewall
		E1.46 Từ Liêm	01 Firewall
		E1.56 Thị Trấn Phùng	01 Firewall
		E1.12 Trần Hưng Đạo	01 Firewall
		E1.13 Phương Liệt	01 Firewall
		E1.18 Bờ Hồ	01 Firewall
		E1.22 Thanh Nhàn	01 Firewall
		E1.26 Linh Đàm	01 Firewall

STT	Đơn vị	Địa điểm	Thiết bị phân bổ
		E1.52 Thống Nhất	01 Firewall
		E1.57 Minh Khai	01 Firewall
		E1.64 Hồ Yên Sở	01 Firewall
		E1.32 Thường Tín	01 Firewall
		E1.39 Thanh Oai	01 Firewall
		E10.2 Vân Đình	01 Firewall
		E10.4 Tía	01 Firewall
		E1.58 Phú Xuyên	01 Firewall
		E1.62 Ngọc Hồi	01 Firewall
		E1.66 Mỹ Đức	01 Firewall
		E1.2 Gia Lâm	01 Firewall
		E1.15 Sài Đồng	01 Firewall
		E1.38 Gia Lâm 2	01 Firewall
		E1.47 Long Biên	01 Firewall
		E1.59 Sài Đồng 2	01 Firewall
		E1.5 Thượng Đình	01 Firewall
		E1.10 Văn Điển	01 Firewall
		E1.30 Văn Quán	01 Firewall
		E1.43 Mỗ Lao	01 Firewall
		E10.9 Xuân Mai	01 Firewall
		E1.51 Phú Nghĩa	01 Firewall
		E1.61 Dương Nội	01 Firewall
		E1.67 CV Thủ Lệ	01 Firewall
		E1.69 Trâu Quỳ	01 Firewall
		E1.71 Hồng Dương	01 Firewall
		E1.73 CNC 2	01 Firewall
		E1.74 Thạch Thất 2	01 Firewall
		E1.68 Chương Mỹ	01 Firewall
		E1.72 Kim Chung	01 Firewall
		E1.76 Đại Kim	01 Firewall
		E1.77 Lĩnh Nam	01 Firewall

Nhà thầu vận chuyển danh mục hàng hóa theo phân bổ cho từng địa điểm triển khai.

Lưu ý: Đối với hàng hoá là phần mềm thì nhà thầu bàn giao bản quyền điện tử (E-license) vào thư điện tử (email) của cán bộ chuyên trách hoặc nhận bàn giao kèm thiết bị dưới dạng bản cứng giấy/ usb/ đĩa CD v.v…

1.6.4.2.6 Kiểm tra hàng hóa (vật tư, thiết bị phần cứng, phần mềm) trước khi đưa vào lắp đặt

- Các hàng hóa đều phải được kiểm tra về chủng loại, quy cách, xuất xứ theo hồ sơ chất lượng đã được quy định trong hợp đồng trước khi đưa vào lắp đặt. Kết quả kiểm

tra phải được lập thành biên bản, ghi rõ chủng loại, quy cách, số lượng vật tư, thiết bị đưa vào công trường từng đợt, có ký xác nhận của đại diện bộ phận giám sát và đại diện bộ phận triển khai thi công của Nhà thầu, Đại diện Ban QLDA, Đại diện các Bên có liên quan. Các Bên ký biên bản nghiệm thu trước khi lắp đặt theo mẫu quy định.

- Trường hợp các vật tư, thiết bị công nghệ thông tin, phần mềm không phù hợp với thiết kế chi tiết được duyệt và hợp đồng đã ký, yêu cầu đưa ra khỏi khu vực tập kết hàng hóa; Hồ sơ chất lượng vật tư, thiết bị bao gồm:
    - Giấy chứng nhận xuất xứ (CO) của vật tư,thiết bị.
    - Giấy chứng nhận chất lượng (CQ) của vật tư, thiết bị do Hãng / nhà phân phối cấp;
    - Giấy chứng nhận bản quyền phần mềm.

  (Các bộ giấy tờ này theo từng địa điểm sẽ sử dụng bản sao công chứng).

1.6.4.2.7 Nghiệm thu lắp đặt tĩnh

- Nghiệm thu tĩnh là kiểm tra, xác định chất lượng lắp đặt đúng thiết kế và phù hợp với các yêu cầu kỹ thuật lắp đặt để chuẩn bị đưa thiết bị vào chạy thử đơn động.
- Chi tiết hướng dẫn lắp đặt các thiết bị tương ứng theo từng địa điểm được mô tả trong mục dưới. Khi nghiệm thu, cần nghiên cứu các hồ sơ tài liệu sau: Hồ sơ Thiết kế Chi tiết đã được phê duyệt; Hợp đồng, phụ lục hợp đồng đã ký và các hồ sơ tài liệu có liên quan khác.
- Sau khi đã nghiên cứu hồ sơ và thực địa. Nếu thấy thiết bị lắp đặt đúng thiết kế và phù hợp với yêu cầu kỹ thuật quy định trong tài liệu hướng dẫn lắp đặt và các tiêu chuẩn kỹ thuật hiện hành thì các Bên lập và ký biên bản nghiệm thu lắp đặt tĩnh, cho phép tiến hành vận hành thử đơn động.

1.6.4.2.8 Nghiệm thu vận hành/chạy thử đơn động, vận hành/chạy thử liên động có tải

- Quy trình này quy định trình tự các bước thực hiện, quyền và trách nhiệm các chủ thể liên quan trọng công tác Quản lý chất lượng vận hành/chạy thử thực hiện theo hình thức hợp đồng EPC.
- Đối với hệ thống hạ tầng kỹ thuật, thiết bị, phần mềm thương mại, nhà thầu triển khai chủ trì, phối hợp với chủ đầu tư tổ chức vận hành/chạy thử:

Quy trình

Việc vận hành/chạy thử thử do nhà thầu triển khai thực hiện bao gồm các bước chính sau đây:

Bước 1. Lập kế hoạch vận hành/chạy thử

a) Đơn vị thực hiện: Nhà thầu triển khai phối hợp với chủ đầu tư và các bên có liên quan.

b) Các hoạt động chính:

- Phân tích, xác định các công việc để vận hành/chạy thử.
- Phân tích, xác định các nguồn lực huy động để vận hành/chạy thử.
- Xây dựng các biểu mẫu cần thiết trong quá trình vận hành/chạy thử.
- Lập kế hoạch vận hành/chạy thử.

- Kế hoạch vận hành/chạy thử được chủ đầu tư chấp thuận.

Bước 2. Xây dựng kịch bản vận hành/chạy thử

a) Đơn vị thực hiện: Nhà thầu triển khai phối hợp với chủ đầu tư và các bên có liên quan.

b) Các hoạt động chính:

- Nghiên cứu, phân tích các tài liệu đầu vào có liên quan để xác định phạm vi, tình huống, kịch bản vận hành/chạy thử.
- Xây dựng, thiết kế tài liệu về các tình huống, kịch bản vận hành/chạy thử mức đơn động, mức liên động có tải đảm bảo đầy đủ các yêu cầu về chức năng, tính năng kỹ thuật của các thiết bị theo thiết kế chi tiết được phê duyệt.
- Trình chủ đầu tư chấp thuận kịch bản vận hành/chạy thử.

Bước 3. Thiết lập môi trường vận hành/chạy thử

a) Đơn vị thực hiện: Nhà thầu triển khai phối hợp với chủ đầu tư và các bên có liên quan.

b) Các hoạt động chính:

- Chuẩn bị môi trường vận hành/chạy thử và các yêu cầu của nhà thầu triển khai cần chủ đầu tư chuẩn bị để phục vụ vận hành/chạy thử.
- Thiết lập nguồn điện và các điều kiện hạ tầng kỹ thuật khác liên quan; kiểm tra các biện pháp đảm bảo an toàn vận hành/chạy, phòng chống cháy, nổ trong quá trình vận hành/chạy thử.

Bước 4. Thực hiện vận hành/chạy thử

a) Đơn vị thực hiện: Nhà thầu triển khai phối hợp với chủ đầu tư và các bên có liên quan.

b) Các hoạt động chính:

- Kiểm tra, theo dõi, lập và ký xác nhận báo cáo kết quả vận hành/chạy thử.
- Kiểm tra, theo dõi, lập và ký xác nhận biên bản xử lý sự cố, các nội dung thay đổi hoặc các vấn đề phát sinh khác tại hiện trường trong quá trình vận hành/chạy thử (nếu có).
- Kiểm tra, theo dõi, ghi nhận các thay đổi so với thiết kế chi tiết đã được duyệt trong quá trình vận hành/chạy thử (nếu có).
- Theo dõi, giám sát của đơn vị giám sát công tác triển khai trong quá trình nhà thầu triển khai thực hiện vận hành/chạy thử.
- Trong trường hợp vận hành/chạy thử, nếu thiết bị, phần mềm thương mại xảy ra hỏng hóc, lỗi thì các bên liên quan họp thống nhất để điều chỉnh kế hoạch vận hành/chạy thử hoặc ngừng vận hành/chạy thử (nếu cần thiết).

Bước 5. Báo cáo kết quả vận hành/chạy thử

a) Đơn vị thực hiện: Nhà thầu triển khai phối hợp với chủ đầu tư và các bên có liên quan

b) Các hoạt động chính:

- Tổng hợp, lập báo cáo kết quả vận hành/chạy thử.
- Kiểm tra các tài liệu, hồ sơ hoàn thành.
- Các kiến nghị, đề xuất với chủ đầu tư (nếu có).

Nghiệm thu vận hành/chạy thử đơn động

- Nghiệm thu vận hành/chạy thử đơn động không tải là kiểm tra, xác định chất lượng lắp đặt và tình trạng thiết bị trong quá trình chạy thử không tải, phát hiện và loại trừ những sai sót, khiếm khuyết chưa phát hiện trong nghiệm thu tĩnh.
- Trong quá trình chạy thử cần theo dõi sự hoạt động của thiết bị, các thông số về RAM, CPU,...nếu phát hiện các khuyết tật thì dừng thiết bị, tìm nguyên nhân và sửa chữa.
- Thời gian vận hành/chạy thử đơn động không tải thường ghi trong các tài liệu hướng dẫn vận hành/chạy thiết bị. Nếu không có số liệu, đối với các thiết bị đơn giản thời gian chạy thử không tải tối đa là 4 giờ, các thiết bị phức tạp tối đa là 8 giờ liên tục không dừng máy.
- Khi kết thúc vận hành/chạy thử đơn động không tải. Ban nghiệm thu cơ sở lập và ký biên bản nghiệm thu chạy thử đơn động. Một số thiết bị có đặc điểm kết cấu không chạy được chế độ không tải thì sau khi nghiệm thu tĩnh xong thì có thể chuyển sang chạy thử liên động có tải.

Nghiệm thu vận hành/chạy thử liên động có tải

- Nghiệm thu chạy thử liên động có tải để phát hiện và loại trừ các khuyết tật của thiết bị trong quá trình mang tải, điều chỉnh các thông số kỹ thuật cho phù hợp, để chuẩn bị đưa thiết bị vào vận hành/chạy.
- Các mức mang tải và thời gian chạy thử thường quy định trong tài liệu hướng dẫn vận hành/chạy thiết bị. Nếu trong tài liệu trên không quy định, sau khi thiết bị mang tải 72 giờ liên tục không ngừng máy, đảm bảo các thông số kỹ thuật về thiết bị và thông số kỹ thuật vận hành/chạy thì kết thúc chạy thử liên động có tải.
- Khi kết thúc chạy thử liên động có tải. Các Bên lập và ký biên bản nghiệm thu chạy thử liên động có tải.
    - Hệ thống thiết bị ATTT (Firewall, USG, Backup, HCI) cho hệ thống Điều khiển trung tâm tại TTĐK EVNHANOI: 03 ngày.
    - Hệ thống Firewall tại các đơn vị được đầu tư: 24 giờ.

1.6.4.2.9 Đào tạo, hướng dẫn vận hành

- Nhà thầu tổ chức các buổi đào tạo, hướng dẫn vận hành các thiết bị được trang bị và lắp đặt tại từng địa điểm triển khai.
- Nội dung cụ thể của các buổi đào tạo sẽ được đệ trình, lấy ý kiến và phê duyệt trước khi thực hiện.

1.6.4.2.10 Nghiệm thu hoàn thành, đưa vào sử dụng

- Nhà thầu tổ chức nghiệm thu hoàn thành và đưa vào sử dụng các hệ thống thành phần tại từng địa điểm triển khai.

1.6.4.3 Bảng phân chia vai trò, trách nhiệm

TT	Các nội dung chính trong quá trình thực hiện dự án	Nhà thầu	Ban QLDA	Đơn vị QLVH tiếp nhận hệ thống ATTT SCADA/DCS
I	Tổ chức đấu thầu, tiến hành lựa chọn nhà thầu		Thực hiện	
II	Thương thảo, ký hợp đồng	Thực hiện	Thực hiện	
III	Bàn giao hàng hoá			
1	Tập trung hàng hoá tại kho hàng của Nhà thầu	Thực hiện		
2	Kiểm tra an ninh hàng hoá và bàn giao hàng hoá	Thực hiện	Được cung cấp thông tin	Tham gia
IV	Triển khai, đào tạo hướng dẫn sử dụng			
1	Lắp đặt và nghiệm thu lắp đặt tĩnh	Thực hiện	Tham gia	Thực hiện/ phối hợp
2	Cài đặt, cấu hình, tích hợp. Nghiệm thu đơn động, liên động có tải	Thực hiện	Tham gia	Thực hiện/ phối hợp
3	Đào tạo, hướng dẫn vẫn hành	Thực hiện	Được cung cấp thông tin	Tham gia
4	Nghiệm thu hoàn thành, đưa vào sử dụng	Thực hiện	Tham gia	Tham gia

1.6.4.4 Dự kiến tiến độ thực hiện dự án

TT	Các nội dung chính trong quá trình thực hiện dự án	Thời gian dự kiến	Biểu mẫu, hồ sơ tài liệu	Ghi chú
I	Tổ chức đấu thầu, tiến hành lựa chọn nhà thầu			
II	Thương thảo, ký hợp đồng			
III	Bàn giao hàng hoá			
1	Tập trung hàng hoá tại kho hàng của Nhà thầu			
2	Kiểm tra an ninh hàng hoá và bàn giao hàng hoá		Phụ lục 4	

TT	Các nội dung chính trong quá trình thực hiện dự án	Thời gian dự kiến	Biểu mẫu, hồ sơ tài liệu	Ghi chú
IV	Triển khai, đào tạo hướng dẫn sử dụng			
1	Lắp đặt và nghiệm thu lắp đặt tĩnh		Phụ lục 4	
2	Cài đặt, cấu hình, tích hợp. Nghiệm thu đơn động, liên động có tải		Phụ lục 4	
3	Đào tạo, hướng dẫn vẫn hành		Phụ lục 4	
4	Nghiệm thu hoàn thành, đưa vào sử dụng		Phụ lục 4	

1.6.4.5 Tiến độ triển khai chi tiết

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																								GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120	
A.	**Bàn giao hàng hoá**	**5**	**T**	**T+5**																									
	Tập trung hàng hoá, kiểm tra an ninh	**5**																											
	Hoàn thiện biên bản bàn giao	**5**																											
B	**Khảo sát, thiết kế**	**15**	**T+5**	**T+20**																									
	Tiến hành khảo sát trước triển khai	**10**																											
	Lên thiết kế HLD, LLD. Chủ đầu tư Phê duyệt thiết kế	**15**																											

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																									GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120		
C	**Triển khai và nghiệm thu kỹ thuật**	**85**	**T+10**	**T+95**																										
I	**Triển khai tại trung tâm**																													
I.1	**Hạng mục thiết bị HCI**	**15**	**T+10**	**T+25**																										
I.1.1	Lắp đặt máy chủ HCI																													
I.1.2	Đấu nguồn, đi dây, đánh nhãn																													
I.1.3	Cấu hình máy cơ bản chủ HCI (Upgrade Firmware, Raid, idrac)																													

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																										GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120			
I.1.4	Cài đặt ảo hoá Vsphere																														
I.1.5	Cấu hình cơ bản Vsphere (datatstore, vmotion, DRS)																														
I.1.6	Phân chia máy chủ ảo cho các hệ thống SIEM, PAM, MFA																														
I.1.7	Xây dựng tài liệu và thực hiện kiểm thử																														
I.2	**Hạng mục thiết bị Backup**	**30**	**T+10**	**T+40**																											

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																										GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120			
I.2.1	Lắp đặt máy chủ, storage backup																														
I.2.2	Đi nguồn, đi dây, đánh nhãn																														
I.2.3	Cấu hình cơ bản, khởi tạo thiết bị																														
I.2.4	Cài đặt software backup																														
I.2.5	Tích hợp các thành phần backup server và storage, clients																														
I.2.6	Cấu hình backup job, policy																														

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																										GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120			
I.2.7	Xây dựng tài liệu và thực hiện kiểm thử																														
I.3	**Hạng mục cài đặt giải pháp SIEM**	**20**	**T+20**	**T+40**																											
I.3.1	Cấu hình cài đặt các thành phần																														
I.3.2	Cấu hình HA hệ thống																														
I.3.3	Cấu hình cơ bản tham số hệ thống																														
I.3.4	Tích hợp Log Source																														
I.3.5	Cài đặt Application																														

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																									GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120		
I.3.6	Cấu hình thông tin Users																													
I.3.7	Tối ưu Rules																													
I.4	**Hạng mục cài đặt giải pháp Endpoint**	**20**	**T+20**	**T+40**																										
I.4.1	Cấu hình cài đặt các thành phần																													
I.4.2	Cấu hình HA hệ thống																													
I.4.3	Cấu hình cơ bản tham số hệ thống																													
I.4.4	Cấu hình Policies																													

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																									GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120		
I.4.5	Cài đặt Agent, đảm bảo hoạt động trên các thiết bị client																													
I.5	**Hạng mục cài đặt giải pháp PAM**	**30**	**T+20**	**T+50**																										
I.5.1	Cấu hình cài đặt các thành phần																													
I.5.2	Cấu hình HA hệ thống																													
I.5.3	Cấu hình cơ bản tham số hệ thống																													
I.5.4	Cấu hình Platform và Policy																													

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																									GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120		
I.5.5	Cấu hình Dual Control																													
I.5.6	Cấu hình tích hợp AD và MFA																													
I.5.7	Cấu hình User và phân quyền																													
I.5.8	Cấu hình tích hợp và cảnh báo với PTA																													
I.5.9	Cấu hình tích hợp thiết bị																													
I.5.10	Cấu hình tích hợp SIEM																													

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																										GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120			
I.6	**Hạng mục cài đặt giải pháp MFA**	**20**	**T+20**	**T+40**																											
I.6.1	Cấu hình cài đặt các thành phần																														
I.6.2	Cấu hình HA hệ thống																														
I.6.3	Cấu hình cơ bản tham số hệ thống																														
I.6.4	Cấu hình BackEnd Authentication																														
I.6.5	Cấu hình Polices																														
I.6.6	Cấu hình Account																														

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																										GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120			
I.6.7	Cấu hình tích hợp thiết bị																														
I.6.8	Cấu hình tích hợp với hệ thống PAM																														
I.6.9	Cấu hình tích hợp với hệ thống SIEM																														
I.7	**Hạng mục triển khai Firewall**	**25**	**T+10**	**T+35**																											
I.7.1	Lắp đặt Firewall																														
I.7.2	Đấu nguồn, đi dây, đánh nhãn																														
I.7.3	Cấu hình Firewall cơ																														

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																										GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120			
	bản, cập nhật Firewall																														
I.7.4	Cấu hình mạng LAN, WAN																														
I.7.5	Cấu hình Firewall Rule & Policies																														
I.7.6	Cấu hình chế độ bảo mật																														
I.7.7	Triển khai giải pháp quản lý firewall tập trung																														
I.7.8	Cấu hình tích hợp với hệ thống																														

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																										GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120			
	quản trị Firewall tập trung																														
I.8	**Hạng mục triển khai Data Diode**	**15**	**T+10**	**T+25**																											
I.8.1	Lắp đặt Data Diode																														
I.8.2	Đấu nguồn, đi dây, đánh nhãn																														
I.8.3	Cấu hình Datadiode cơ bản, cập nhật Datadiode																														
I.8.4	Cấu hình tích hợp với các thiết bị mạng																														

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																										GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120			
II	**Triển khai tại các đơn vị**																														
II.1	**Công ty điện lực Hà Nội**	**30**	**T+20**	**T+50**																											
II.1.1	Cài đặt Endpoint Protection																														
II.1.2	Cài đặt Authentication for Windows Logon																														
II.3.3	Cài đặt SIEM Agent																														
II.2	**Công ty lưới điện cao thế**	**10**	**T+20**	**T+30**																											

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																										GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120			
II.2.1	Cài đặt Endpoint Protection																														
II.2.2	Cài đặt Authentication for Windows Logon																														
II.3.3	Cài đặt SIEM Agent																														
II.3	**Tại Trạm biến áp**	**55**	**T+20**	**T+75**																											
II.3.1	Triển khai, lắp đặt Firewall																														
II.3.2	Cài đặt Endpoint Protection																														
II.3.3	Cài đặt Authentication for																														

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																								GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120	
	Windows Logon																												
II.3.4	Cài đặt SIEM Agent																												
III	**Nghiệm thu kỹ thuật**																												
III.1	Nghiệm thu lắp đặt tĩnh	**5**	**T+10**	**T+15**																									
III.2	Lên kịch bản nghiệm thu kỹ thuật và thống nhất với Chủ đầu tư	**10**	**T+70**	**T+80**																									
III.3	Tiến hành nghiệm thu đơn động, nghiệm thu liên động có tải và hoàn tấn các thủ	**20**	**T+80**	**T+100**																									

TT	NỘI DUNG CÔNG VIỆC	THỜI GIAN THỰC HIỆN	NGÀY BẮT ĐẦU	NGÀY KẾT THÚC	NGÀY THỰC HIỆN																									GHI CHÚ
					5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120		
	tục nghiệm thu																													
D	**Đào tạo, hướng dẫn sử dụng**																													
I	Đào tạo, hướng dẫn vận hành	**35**	**T+80**	**T+115**																										
II	Nghiệm thu đào tạo	**5**	**T+115**	**T+120**																										
III	Bàn giao tài liệu	**5**	**T+115**	**T+120**																										

1.6.5 Biện pháp an toàn khi thi công, vận hành

1.6.5.1 Biện pháp đảm bảo an toàn khi thi công

- Thi công đúng theo yêu cầu kỹ thuật, đảm bảo chất lượng công trình;
- Công cụ, dụng cụ dùng để lắp đặt là dụng cụ chuyên dụng, sử dụng đúng chức năng;
- Các thiết bị lắp đặt trong dự án yêu cầu bắt buộc khi thi công phải thực hiện đúng quy trình, bản vẽ thiết kế thi công lắp đặt đã được phê duyệt và tài liệu hướng dẫn của nhà sản xuất;
- Khi thi công trong phòng có thiết bị thông tin khác đang khai thác, đảm bảo tuyệt đối không làm ảnh hưởng, sự cố đến các thiết bị thông tin;
- Trong quá trình thi công đảm bảo không làm ảnh hưởng đến vệ sinh môi trường ở khu vực thi công và nơi công cộng;
- Quy trình đi dây phải đảm bảo đúng kỹ thuật, cẩn thận, chắc chăn ngay ngắn và hợp mỹ quan;
- Trong quá trình thi công cần phối hợp với các đơn vị sử dụng để có biện pháp ngăn chặn chập cháy điện, mất an toàn lao động.

1.6.5.2 Biện pháp an toàn lao động, phòng chống cháy nổ

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

Kiểm tra, giám sát biện pháp chuẩn bị của Bộ phận thi công đảm bảo chấp hành các quy định về an toàn lao động đã ban hành.

Kiểm tra, giám sát biện pháp vận chuyển vật tư, dụng cụ thi công khi đưa lên cao và khi hạ xuống, đảm bảo an toàn tuyệt đối cho người, phương tiện, dụng cụ, vật tư.

Kiểm tra, giám sát biện pháp chuẩn bị của Bộ phận thi công đảm bảo chấp hành các quy định về an toàn điện.

Kiểm tra trang bị dụng cụ bảo hộ cho người tham gia.

Kiểm tra an toàn lao động khi bốc dỡ, vận chuyển vật tư, vật liệu và dụng cụ thi công. Kiểm tra độ bền vững của phương tiện vận chuyển.

Về an toàn phòng, chống cháy nổ: phải đảm bảo tối đa khả năng chống cháy tại các phòng đặt máy chủ, nơi làm việc, tránh các kết nối gây chạm, chập điện có thể phát cháy;

Hệ thống mạng, bảo mật tại trung tâm dữ liệu đòi hỏi nghiêm ngặt về điều kiện hoạt động cũng như an toàn, ổn định trong mọi trường hợp. Để đảm bảo an toàn cho thiết bị và con người làm việc tránh các sự cố do chập cháy gây ra, giải pháp PCCC đề xuất sử dụng hệ thống phòng cháy hiện hữu của các đơn vị.

Yêu cầu thi công gần các vật liệu bắt lửa, phải che chắn và phải có các dụng cụ chữa cháy đi kèm:

- Không để các vật dễ cháy gần cầu chì, bảng điện
- Không dùng dây điện cắm trực tiếp vào ổ điện

- Thường xuyên quan sát phát hiện kịp thời và nguyên nhân gây cháy

Những máy móc thiết bị thi công đều được kiểm tra hoạt động trước khi đưa vào phục vụ thi công thiết bị phải đảm bảo các điều kiện an toàn, chất lượng mới được sử dụng tại công trường. Có nội quy sử dụng máy, cử người có trình độ chuyên môn điều khiển.

1.6.5.3 Biện pháp đảm bảo an toàn thông tin trong quá trình triển khai, vận hành

- Quá trình triển khai đảm bảo không sử dụng các thiết bị điện tử/thông tin như thiết bị lưu trữ di động, máy tính xách tay, điện thoại di động, máy tính bảng, v.v.. không được phép để kết nối vào các hệ thống của Chủ đầu tư.
- Cập nhật bản vá, các phiên bản phần mềm, phiên bản hệ điều hành theo khuyến cáo của nhà sản xuất nhằm hạn chế các lỗ hổng về bảo mật giúp phòng chống việc mất an toàn, an ninh thông tin. Bên cạnh đó là tuân thủ các yeu cầu về bảo mật thông tin của Chủ đầu tư và của Chủ đầu tư trong suốt quá trình triển khai, vận hành hệ thống.
- Nhà thầu cam kết không thực hiện chia sẻ, tiết lộ các tài liệu, thông tin nhạy cảm của Chủ đầu tư và dự án với các cá nhân, tổ chức không liên quan đến dự án.
- Thông tin, dữ liệu hình thành trong quá trình triển khai và bảo hành thuộc sở hữu của Chủ đầu tư. Nhà thầu có trách nhiệm bảo đảm an ninh, an toàn thông tin, chuyển giao đầy đủ cho Chủ đầu tư.

1.6.5.4 Biện pháp đảm bảo an toàn cho quá trình sản xuất, kinh doanh của EVNHANOI trong quá trình triển khai

- Cài đặt, cấu hình hệ thống đảm bảo theo đúng như tài liệu thiết kế đã được phê duyệt và hướng dẫn từ nhà sản xuất.
- Khi đấu nối các thiết bị vào hệ thống thông tin hiện tại, cần chuẩn bị trước điều kiện hạ tầng kết nối trước, sau đó phối hợp với các cán bộ QLVH triển khai trong lúc EVNHANOI dừng hoạt động hoặc tạm thời ngắt hệ thống để đảm bảo không ảnh hưởng đến quá trình sản xuất, kinh doanh của EVNHANOI.
- Quá trình thực hiện cài đặt cấu hình các thiết bị cụ thể như sau:

Trình tự	**Nội dung công việc**	**Đánh giá ảnh hưởng**	**Phương án đảm bảo**
1	Cài đặt hệ thống máy chủ HCI	Không ảnh hưởng	Thực hiện cài đặt và cấu hình theo đúng thiết kế đã được phê duyệt. Triển khai trong thời gian cho phép của EVNHANOI. Có sự giám sát của cán bộ phụ trách.
2	Cài đặt và cấu hình hệ thống tường lửa trung tâm và chuyển đổi hệ thống	Ảnh hưởng đến toàn bộ hệ thống của TTĐK	1. Lắp đặt thiết bị và đấu nối với các Switch core theo đúng thiết kế được phê duyệt.

Trình tự	Nội dung công việc	Đánh giá ảnh hưởng	Phương án đảm bảo
			2. Cấu hình thiết bị Firewall mới theo các phân vùng đã quy hoạch trên Firewall cũ. 3. Shutdown toàn bộ các interface đấu nối với Switch Core 4. Shutdown các interfaces trên Firewall cũ và enable interfaces trên Firewall mới để giảm thiểu tối đa thời gian downtime hệ thống.
3	Cài đặt và cấu hình hệ thống tường lửa tại các Trạm biến áp không người trực	Ảnh hưởng đến kết nối giữa TBA và TTĐK	1. Lắp đặt thiết bị và đấu nối với các Switch tại TBA theo đúng thiết kế được phê duyệt. 2. Cấu hình thiết bị Firewall mới theo các phân vùng đã quy hoạch theo QĐ168 3. Shutdown toàn bộ các interface đấu nối với Switch TBA 4. Cấu hình quy hoạch sẵn các VLAN theo QĐ 168 trên Switch tại TBA 5. Chuyển các máy tại TBA về đúng các VLAN được quy hoạch và enable lại các interfaces trên Firewall
4	Cài đặt agent lên các máy chủ cần backup	Không ảnh hưởng	Thực hiện theo đúng thiết kế đã được phê duyệt. Triển khai trong thời gian cho phép của EVNHANOI. Có sự giám sát của cán bộ phụ trách.
5	Cấu hình backup dữ liệu	Có thể có ảnh hưởng đến tải của máy chủ, tải mạng trong quá trình backup dữ liệu	Chọn thời gian backup vào giờ thấp tải

Trình tự	Nội dung công việc	Đánh giá ảnh hưởng	Phương án đảm bảo
6	Cấu hình tích hợp tài khoản đặc quyền	Không ảnh hưởng	Thực hiện theo đúng thiết kế đã được phê duyệt. Triển khai trong thời gian cho phép của EVNHANOI. Có sự giám sát của cán bộ phụ trách.
7	Cài đặt agent MFA lên các máy trạm	Không ảnh hưởng	Thực hiện theo đúng thiết kế đã được phê duyệt. Triển khai trong thời gian cho phép của EVNHANOI. Có sự giám sát của cán bộ phụ trách.
8	Cài đặt agent thu thập log	Không ảnh hưởng	Thực hiện theo đúng thiết kế đã được phê duyệt. Triển khai trong thời gian cho phép của EVNHANOI. Có sự giám sát của cán bộ phụ trách.
9	Cài đặt Agent EPS lên các máy trạm	Có thể ảnh hưởng đến hoạt động của máy trạm	Thực hiện thử nghiệm trên một vài máy với các hệ điều hành có trong hệ thống của EVNHN, theo dõi hoạt động trước khi tiến hành cài đặt trên toàn bộ các máy trạm còn lại. Cấu hình các chính sách bảo mật có action notify để giám sát trước khi chuyển sang action block.
10	Cài đặt Agent EPS lên các máy chủ ứng dụng	Có thể ảnh hưởng đến hoạt động của máy chủ ứng dụng	Thực hiện kiểm thử trên các máy chủ test có cùng phiên bản hệ điều hành và ứng dụng, theo dõi và đánh giá trước khi cài đặt lên các máy chủ vùng production. Cấu hình các chính sách bảo mật có action notify để giám sát trước khi chuyển sang action block.
11	Cài đặt Agent EPS lên các máy chủ CSDL	Có thể ảnh hưởng đến hoạt	Thực hiện kiểm thử trên các máy chủ test có cùng phiên bản hệ điều hành và CSDL, theo dõi

Trình tự	Nội dung công việc	Đánh giá ảnh hưởng	Phương án đảm bảo
		động của máy chủ CSDL	và đánh giá trước khi cài đặt lên các máy chủ vùng production. Cấu hình các chính sách bảo mật có action notify để giám sát trước khi chuyển sang action block.

1.6.6 Xây dựng quy trình vận hành và đảm bảo ATTT

1.6.6.1 Sự cần thiết của quy trình vận hành và cập nhật

Để vận hành hiệu quả hệ thống An toàn, an ninh thông tin cho hệ thống Điều khiển trung tâm tại ENVHANOI, quy trình là một thành phần không thể thiếu. Các quy trình sẽ giúp cho hệ thống được vận hành hiệu quả, phát huy tối đa vai trò đội ngũ chuyên viên vận hành, cũng như các công nghệ đang được sử dụng.

1.6.6.2 Các quy trình tổng lược

Theo công văn số 2973/BTTTT-CATTT ngày 04/09/2019 về việc hướng dẫn triển khai hoạt động giám sát an toàn thông tin trong cơ quan, tổ chức nhà nước cùng với việc dựa trên nhu cầu cũng như năng lực hiện tại, EVNHANOI sẽ lập kế hoạch xây dựng tối thiểu các quy trình sau để áp dụng cho hệ thống An toàn, an ninh thông tin.

STT	Quy trình	Nội dung mô tả
1	Quy trình đăng nhập và kiểm soát thao tác người dùng trên hệ thống	- Phân loại các nhóm thiết bị (theo các đơn vị chủ quản hoặc theo các loại ứng dụng...) - Xây dựng quy trình yêu cầu và phê duyệt đăng nhập vào hệ thống - Xây dựng quy trình thực thi và thao tác trên hệ thống
2	Quy trình thu thập dữ liệu phục vụ giám sát an ninh mạng	- Thu thập log End-point - Thu thập log Firewall - Thu thập log PIM/PAM - Thu thập log các thiết bị mạng - Thu thập log các thiết bị bảo mật (EPS) - Tập hợp và lưu trữ tập trung
3	Quy trình giám sát ATTT	Quy trình này sẽ giúp các chuyên viên của EVNHANOI có thể giám sát tình hình ATTT theo thời gian thực
4	Quy trình xử lý sự cố ATTT	Quy trình này sẽ giúp các chuyên viên của EVNHANOI có những chuẩn bị tốt nhất trước, trong, và sau khi sự cố xảy ra như việc leo thang thông tin khi sự cố xảy ra; cơ chế phối hợp với bên thứ ba hay lập kế hoạch xử lý truyền thông; các biện pháp cô lập nhanh hệ thống nhiễm mã độc… từ đó có khả năng phản ứng nhanh và

STT	Quy trình	Nội dung mô tả
		xử lý kịp thời giúp giảm thiểu tối đa thiệt hại khi xảy ra sự cố.
5	Quy trình nâng cấp, cập nhật bản vá cho hệ thống	- Thực hiện cập nhật các bản vá, bản nâng cấp các thành phần hệ thống từ Vendor - Quản trị viên thực hiện đẩy các bản vá, nâng cấp lên NFS server - Quản trị viên thực hiện nâng cấp hệ thống, cập nhật bản vá theo tài liệu hướng dẫn vận hành hệ thống

1.6.6.3 Quy trình đăng nhập và kiểm soát thao tác người dùng trên hệ thống

Mục đích của quy trình:

Trước khi triển khai PAM, người quản trị sử dụng username/password truy cập đến các hệ thống một cách trực tiếp, các phiên truy cập không được giám sát, đồng thời việc đổi mật khẩu định kì cũng không được giám sát, và người quản trị phải nhớ quá nhiều mật khẩu. Việc chia sẻ mật khẩu cũng tiềm ẩn nguy cơ rò rỉ mật khẩu.

Sau khi triển khai PAM, các hệ thống đích sẽ được đưa vào PAM quản lý, các mật khẩu sẽ được đổi tự động định kì theo chính sách đặt ra trước. Người quản trị sẽ không còn truy cập trực tiếp đến thiết bị nữa mà sẽ truy cập vào web PVWA rồi mới truy cập được đến thiết bị đích, các phiên truy cập người quản trị không cần phải nhập username/password mà chỉ cần chọn thiết bị đích và click "Connect", điều này giúp không phải nhớ quá nhiều mật khẩu, tránh việc chia sẻ mật khẩu dẫn đến các nguy cơ rò rỉ mật khẩu.

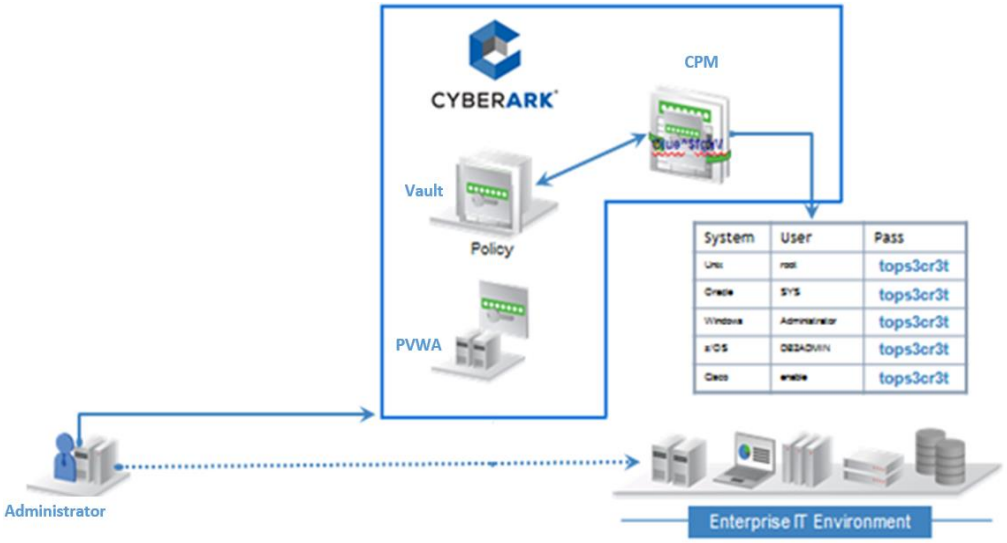
a. *Đối tượng trong quy trình đăng nhập và kiểm soát thao tác người dùng trên hệ thống*

- Quy trình này áp dụng đối với:
  - Đơn vị QLVH: chịu trách nhiệm vận hành hệ thống PAM
  - Cán bộ phê duyệt: người chịu trách nhiệm phê duyệt các yêu cầu đăng nhập từ các cán bộ IT
  - Các cán bộ IT có nhu cầu đăng nhập vào hệ thống OT

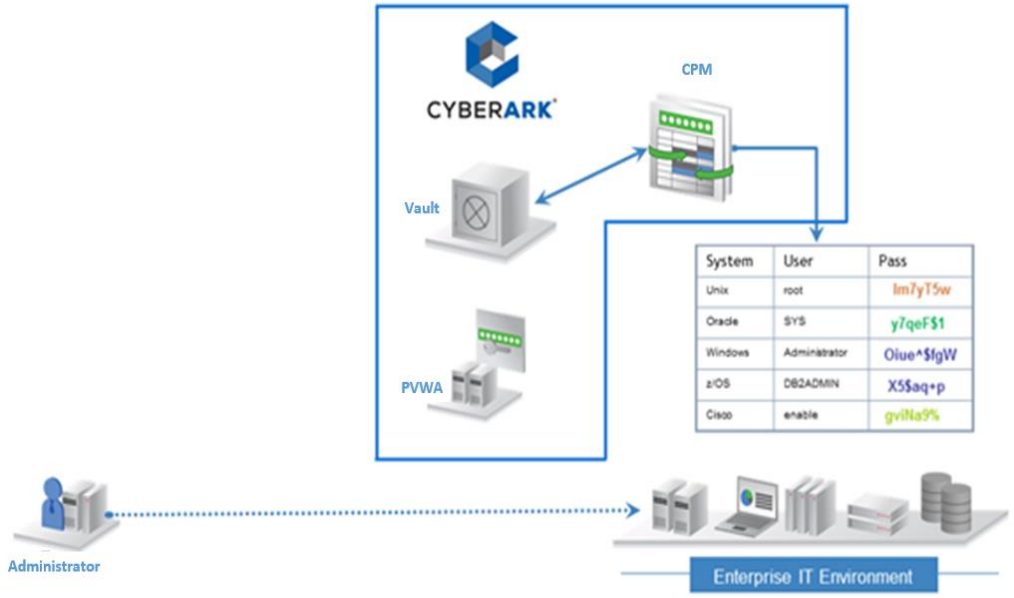
b. *Quy trình đăng nhập và kiểm soát thao tác người dùng trên hệ thống*

Việc cấp tài khoản, đăng nhập vào hệ thống và kiểm soát thao tác người dùng được mô tả theo 5 quy trình sau:

Quy trình 01: Định nghĩa chính sách về mật khẩu cho các thiết bị trong toàn hệ thống

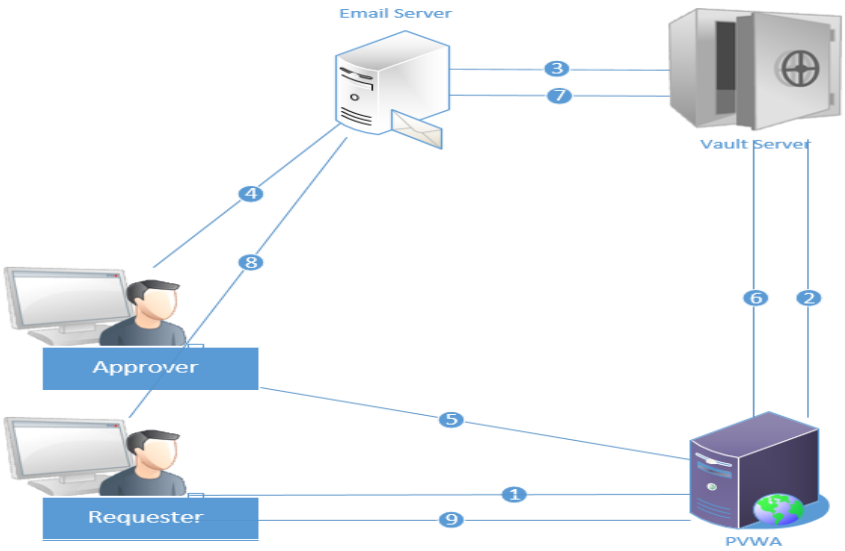


- Đơn vị QLVH đăng nhập vào PVWA để định nghĩa các chính sách về mật khẩu cho các thiết bị trong toàn hệ thống.
- Chính sách về mật khẩu sẽ được lưu tại Vault Server và được đẩy xuống CPM.



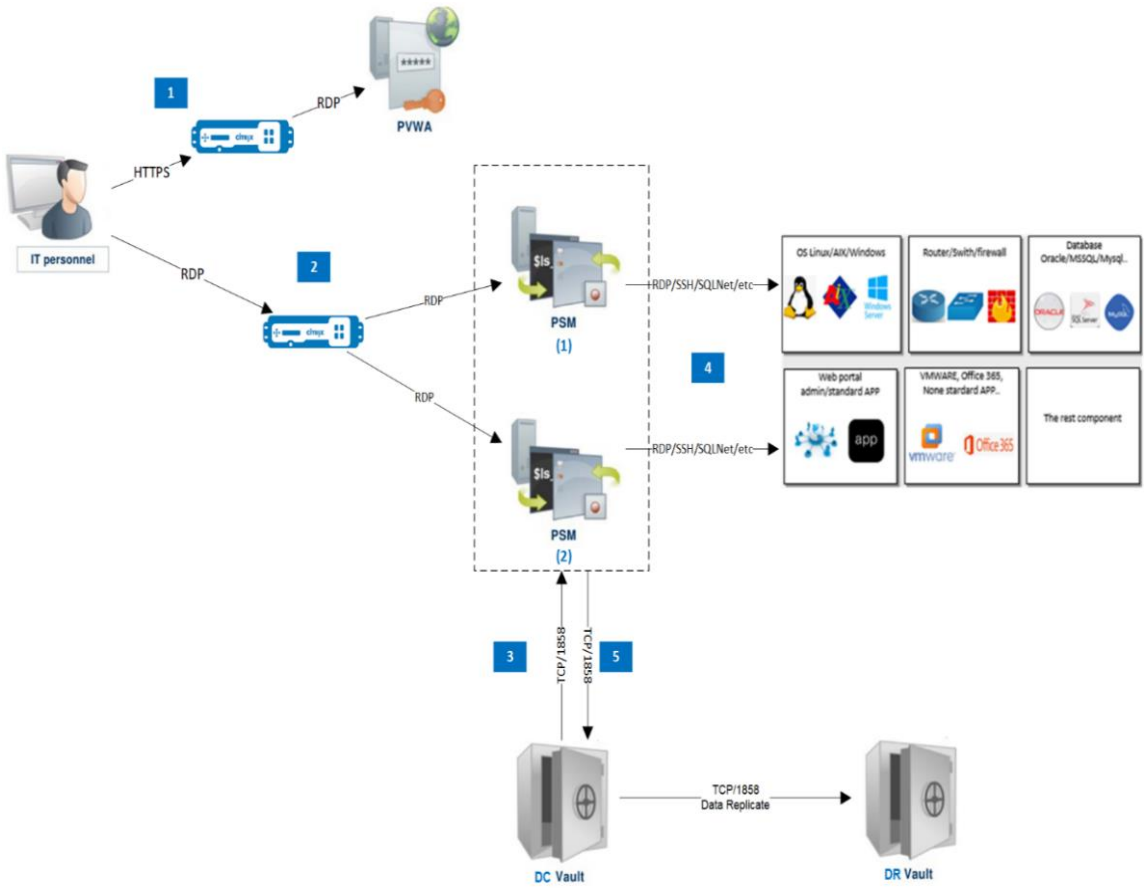
- Khi các thiết bị trong hệ thống công nghệ thông tin được quản lý bởi hệ thống quản lý mật khẩu đặc quyền, Module CPM sẽ sinh ra các mật khẩu mới (dựa trên chính sách về mật khẩu được Administrator định nghĩa) và đẩy các mật khẩu này xuống các thiết bị, đồng thời các mật khẩu này cũng được CPM đẩy về phía Vault Server để lưu lại.

Quy trình 02: Yêu cầu mật khẩu từ nhân viên IT để sử dụng (Dual Control)



- (1). Chuyên viên IT (requester) yêu cầu sử dụng account.
- (2). Thông tin yêu cầu sử dụng account được PVWA gửi đến Vault Server.
- (3). Vault Server sẽ tạo ra một thông báo gửi tới Email Server
- (4). Email Server gửi thông báo tới người phê duyệt (Approver)
- (5). Approver đăng nhập vào PVWA và xác nhận yêu cầu sử dụng account của requester.
- (6). Thông tin về xác nhận này được lưu vào Vault Server
- (7). Vault Server tạo một thông báo về xác nhận này và gửi tới Email Server
- (8). Email Server gửi thông báo tới Requester.
- (9). Requester đăng nhập vào PVWA và sử dụng account.

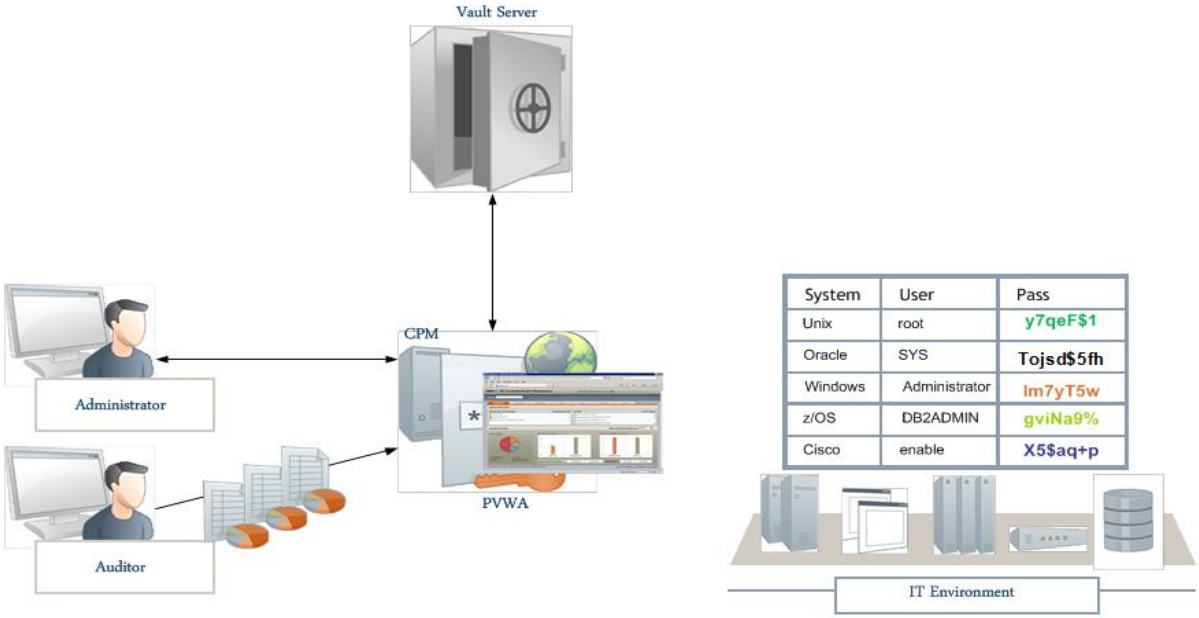
Quy trình 03: Truy cập tới thiết bị đích



- Đây là một ưu điểm giải pháp, giúp tăng tính bảo mật cho toàn hệ thống. Nhân viên IT vẫn có quyền truy cập và thiết bị do họ quản lý nhưng họ không cần phải biết mật khẩu đăng nhập vào thiết bị đó.
- Họ sẽ đăng nhập vào PVWA, PVWA gửi yêu cầu cho PSM. PSM thực hiện quá trình lấy mật khẩu từ Vault server và đăng nhập vào thiết bị.
- Sau đó PSM gửi lại người IT màn hình đã login vào thiết bị tại thời điểm này mọi thao tác của nhân viên IT trên thiết bị đó sẽ được hệ thống xác thực ghi lại dưới dạng video.
- Mô tả qui trình kết nối của user đến hệ thống đích qua hệ thống PIM-:
- Module PSM (Privileged Session Manager) đảm trách nhiệm vụ mở phiên truy cập trong suốt từ người dùng tới các thiết bị đích. Người dùng thay vì truy cập trực tiếp tới thiết bị đích từ máy tính cá nhân của mình, sẽ phải truy cập theo các bước được mô tả như sau:
    - Người dùng đăng nhập vào giao diện Web PVWA để làm việc với hệ thống quản lý tài khoản đặc quyền.
    - Người dùng chọn tài khoản đặc quyền cần sử dụng rồi ấn Connect (kết nối). Trên máy tính của người dùng tự động mở một phiên kết nối remote desktop tới máy chủ PSM.
    - Module PSM giao tiếp trực tiếp với EPV, lấy về thông tin của tài khoản được chọn (bao gồm username, password, IP address, hostname, v.v.).

- Trên phiên kết nối của người dùng ở bước 2, module PSM mở phiên kết nối nối tiếp tới các thiết bị đích, sử dụng thông tin tài khoản có được ở bước 3.
- Khi người dùng kết thúc phiên làm việc của mình, PSM tải các file video/text ghi lại phiên làm việc của người dùng lên EPV để lưu trữ tập trung.

Quy trình 04: Thống kê, báo cáo



- Giải pháp cung cấp các chức năng báo cáo, thông kê đầy đủ.
- Đơn vị QLVH đăng nhập vào PVWA thực hiện tạo thông kê về số lượng thiết bị được quản lý mật khẩu, báo cáo về các hoạt động của IT.

1.6.6.4 Quy trình thu thập dữ liệu phục vụ giám sát an ninh mạng

Mục đích của quy trình: Hướng dẫn cách thức thực hiện phối hợp thu thập dữ liệu phục vụ cho việc giám sát an ninh mạng. Các cán bộ QLVH quản lý các hệ thống có thể đề xuất yêu cầu giám sát ATTT cho hệ thống mình quản lý, tuy nhiên cần phải tiến hành việc thu thập dữ liệu log cho SIEM trước.

a. Đối tượng trong quy trình thu thập dữ liệu

- Quy trình này áp dụng với:
  - Cán bộ QLVH quản lý hệ thống SIEM
  - Cán bộ QLVH quản lý hệ thống thiết bị bảo mật
  - Cán bộ QLVH quản lý hệ thống máy chủ
  - Cán bộ QLVH quản lý hệ thống ứng dụng
  - Người phê duyệt: chịu trách nhiệm phê duyệt cho phép cấu hình thu thập log và giám sát hệ thống.

b. Quy trình thu thập dữ liệu

Bước 1: Gửi yêu cầu giám sát

Các cán bộ QLVH hệ thống thiết bị bảo mật/ máy chủ/ ứng dụng muốn giám sát ATTT hệ thống do mình làm chủ quản thì gửi yêu cầu giám sát về cán bộ phê duyệt (người phê duyệt). Sau khi được cán bộ phê duyệt chấp nhận thì tiến hành sang bước 2.

Bước 2: Kiểm tra rà soát hệ thống

Cán bộ QLVH rà soát, kiểm tra toàn bộ hệ thống OT hiện tại bao gồm các thiết bị bảo mật, các máy chủ, các ứng dụng để kiểm tra khả năng cài đặt Agent lấy log, kiểm tra cấu hình mạng để đảm bảo kết nối từ các thiết bị/máy chủ/ứng dụng tới hệ thống SIEM hiện tại. Sau bước này cán bộ QLVH SIEM có thể xem thiết bị/máy chủ/ứng dụng có đủ điều kiện để lấy log, phục vụ giám sát ATTT không.

Bước 3: Gửi yêu cầu và hướng dẫn thu thập log

Cán bộ QLVH gửi yêu cầu cấu hình sang cho các cán bộ QLVH quản lý các hệ thống liên quan kèm theo hướng dẫn/ các yêu cầu cấu hình.

Bước 4: Cấu hình thu thập log

Cán bộ QLVH quản lý các hệ thống tiến hành cấu hình log theo yêu cầu và gửi phản hồi lại cho cán bộ QLVH SIEM.

Bước 5: Kiểm tra và xác nhận

Cán bộ QLVH SIEM kiểm tra trên phần mềm SIEM để đảm bảo hệ thống đã thu thập đúng và đủ lượng log theo yêu cầu. Cán bộ QLVH SIEM xác nhận lại cán bộ QLVH hệ thống máy chủ/ứng dụng/ thiết bị bảo mật rằng hệ thống đã được thu thập log và sẽ được giám sát ATTT theo thời gian thực.

1.6.6.5 Quy trình giám sát an ninh mạng

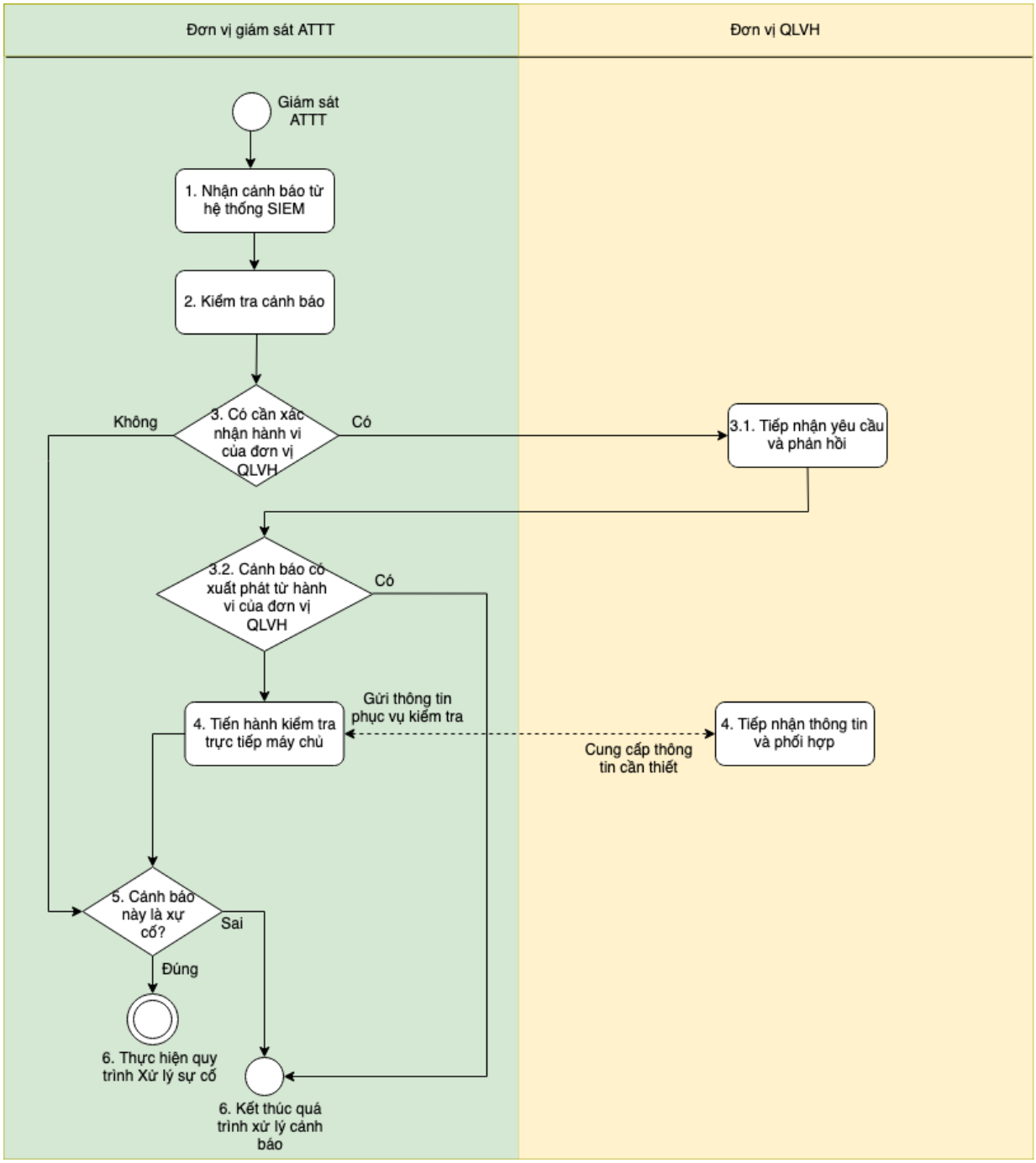
Mục đích của quy trình: Hướng dẫn cách thức thực hiện việc phối hợp giám An toàn thông tin cho hệ thống hệ thống giám sát, điều khiển và tự động hóa của EVNHANOI

a. Đối tượng trong quy trình giám sát an ninh mạng

- Quy trình này áp dụng đối với:
    - Đơn vị phụ trách ATTT tại EVNHANOI – các cán bộ chuyên trách mảng giám sát ATTT (đơn vị giám sát ATTT);
    - Đơn vị QLVH
- Vai trò của đơn vị giám sát ATTT:
    - Giám sát màn hình cảnh báo, tiếp nhận các cảnh báo từ hệ thống giám sát và kiểm tra xác minh trên hệ thống SIEM.
    - Chủ động liên lạc, thảo luận với đơn vị QLVH để xác minh các hành động liên quan đến cảnh báo.
    - Kiểm tra, phân tích dấu hiệu xâm nhập trên các máy chủ khi có nghi ngờ.
- Vai trò của đơn vị QLVH:
    - Cung cấp đầu mối phối hợp với đơn vị phụ trách ATTT trong quá trình giám sát và xử lý sự cố an ninh mạng.
    - Phản hồi các yêu cầu của đơn vị phụ trách ATTT.
    - Đánh giá tác động và tiến hành khắc phục, xử lý sự cố theo khuyến nghị của đơn vị phụ trách ATTT.

b. Quy trình giám sát an ninh mạng

Quy trình phối hợp giám sát ATTT giữa đơn vị giám sát ATTT và đơn vị QLVH sẽ được thể hiện bằng lưu đồ dưới đây:



TKTC-BV 31 Quy trình giám sát an ninh mạng

Giải thích lưu đồ:

Nội dung	**Mô tả**
Giám sát ATTT	Đội giám sát ATTT sẽ thực hiện giám sát màn hình cảnh báo trên phần mềm SIEM
1. Nhận cảnh báo từ hệ thống SIEM	Đội giám sát ATTT sẽ tiếp nhận và xử lý các thông tin khi xuất hiện cảnh báo từ hệ thống SIEM nhằm phục vụ cho các bước phân tích sau này.

Nội dung	Mô tả
2. Kiểm tra cảnh báo	Đội giám sát ATTT sẽ tiến hành kiểm tra các thông tin liên quan đến cảnh báo trên hệ thống SIEM nhằm xác định và sâu chuỗi hành vi khác (nếu có) từ đó kết luận các hành vi này là cảnh báo giả hay không. Nếu cần đơn vị QLVH xác nhận lại các hành vi này thì đơn vị giám sát gửi yêu cầu xác nhận hành vi**.** Nếu không cần đơn vị QLVH xác nhận lại, đơn vị giám sát ATTT tiến hành xác định nếu hành vi này là cảnh báo giả thì tiến hành đóng cảnh báo. Nếu là hành vi sự cố thì **Chuyển quy trình** thực hiện theo Quy trình xử lý sự cố.
3. Đơn vị giám sát ATTT gửi yêu cầu xác nhận hành vi	Trong trường hợp nghi ngờ các hành vi có thể do quản trị hệ thống của đơn vị QLVH thực hiện, đơn vị giám sát ATTT sẽ gửi yêu cầu xác nhận lại hành vi liên quan đến cảnh báo cho đơn vị QLVH trên kênh liên lạc đã được thống nhất giữa hai bên.
3.1. Đơn vị QLVH tiếp nhận và gửi lại thông tin xác nhận	Đơn vị QLVH tiếp nhận thông tin yêu cầu xác nhận, xử lý thông tin và gửi lại kết quả cho đơn vị giám sát ATTT trên kênh liên lạc riêng.
3.2 Đơn vị giám sát ATTT tiếp nhận thông tin phản hồi	Đơn vị giám sát ATTT tiếp nhận thông tin phải hồi từ đơn vị QLVH về các hành vi liên quan đến cảnh báo và dựa vào đó xác định: Nếu đơn vị QLVH xác nhận hành vi này do quản trị, vận hành thực hiện thì thực hiện đóng cảnh báo. Nếu đơn vị QLVH xác nhận hành vi này không phải do đơn vị QLVH thực thiện thì, đơn vị giám sát ATTT sẽ tiến hành kiểm tra trực tiếp trên máy chủ đang có nghi ngờ.
4. Đơn vị giám sát ATTT tiến hành kiểm tra trực tiếp trên máy chủ	- Đơn vị giám sát ATTT sẽ gửi yêu cầu cung cấp thông tin để thực hiện điều tra trực tiếp trên máy chủ (kết nối, tài khoản đăng nhập,…) cho đơn vị QLVH trên kênh liên lạc đã được thống nhất giữa hai bên; - Đơn vị QLVH tiếp nhận thông tin yêu cầu và gửi lại thông tin (kết nối, tài khoản đăng nhập,…) trên kênh liên lạc riêng.
5. Kiểm tra, đánh giá cảnh báo	- Sau khi nhận được thông tin truy cập vào máy chủ, đơn vị giám sát ATTT sẽ tiến hành thu thập thông tin và điều tra trực tiếp trên máy chủ đó. Sau khi kết thúc điều tra trực tiếp, đơn vị giám sát ATTT sẽ đưa ra đánh giá sơ bộ để xác định các hành vi liên quan đến cảnh báo có phải là sự cố không. Nếu hành vi đó là sự cố thì tiến hành chuyển sang quy trình xử lý sự cố;

Nội dung	Mô tả
	Nếu xác định hành vi đó là cảnh báo giả thì đóng cảnh báo.
6. Thực hiện theo Quy trình xử lý sự cố	Nếu hành vi liên quan đến cảnh báo là sự cố thì đơn vị giám sát ATTT tiến hành chuyển sang quy trình xử lý sự cố.
Đóng cảnh báo	Nếu hành vi liên quan đến cảnh báo là cảnh báo giả thì đơn vị giám sát ATTT thực hiện đóng cảnh báo trên hệ thống giám sát.

1.6.6.6 Quy trình xử lý sự cố an ninh mạng

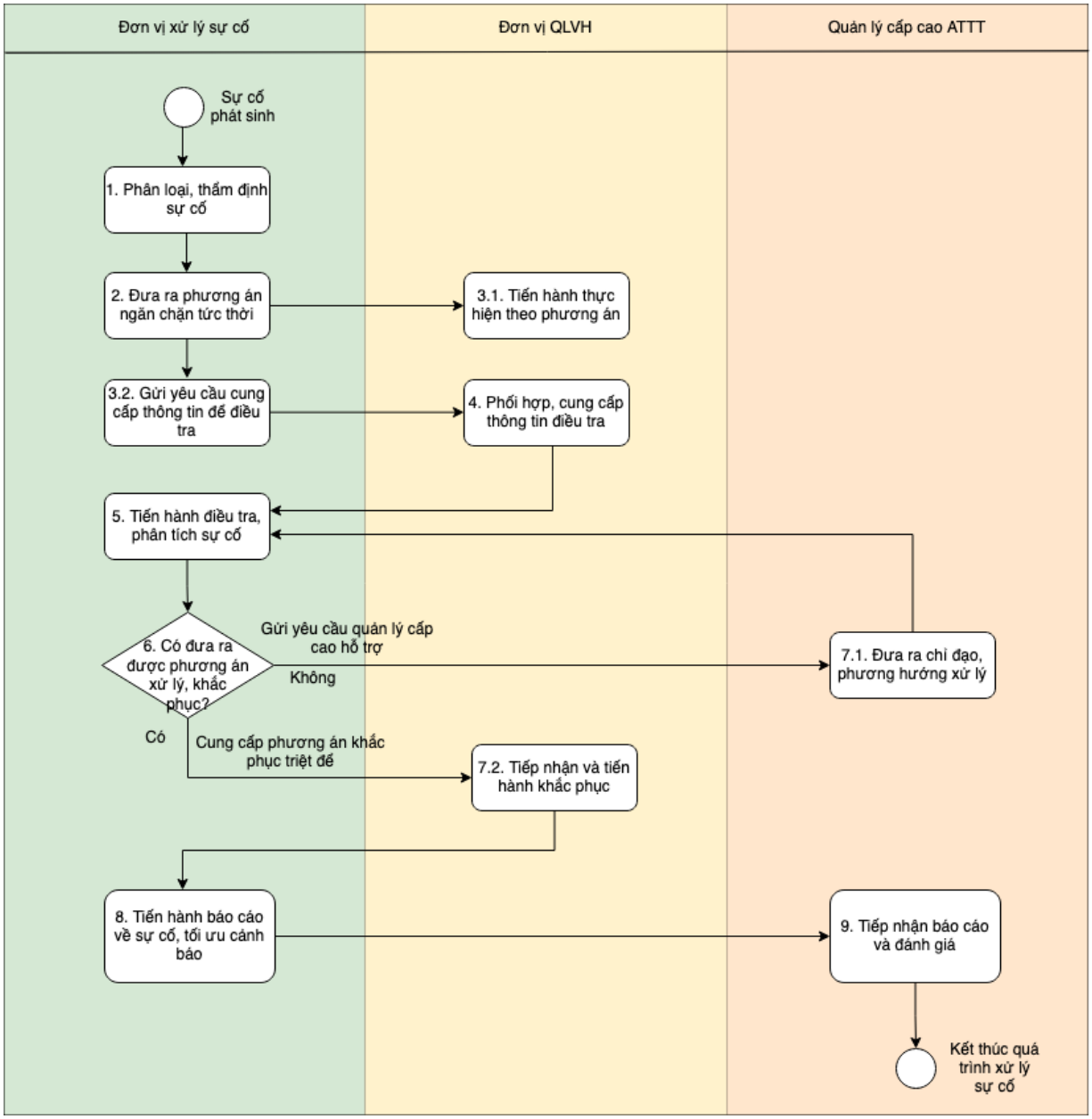
Mục đích của quy trình: Hướng dẫn cách thức thực hiện việc tiếp nhận thông tin, điều tra, xử lý và khắc phục sự cố an toàn thông tin.

a. Đối tượng trong quy trình xử lý sự cố an ninh mạng

- Quy trình này áp dụng đối với:
    - Đơn vị phụ trách ATTT tại EVNHANOI – các cán bộ chuyên trách mảng xử lý sự cố ATTT (đơn vị xử lý sự cố ATTT);
    - Đơn vị QLVH
- Vai trò của đơn vị giám sát ATTT:
    - Giám sát màn hình cảnh báo, tiếp nhận các cảnh báo từ hệ thống giám sát và kiểm tra xác minh trên hệ thống SIEM.
    - Chủ động liên lạc, thảo luận với đơn vị QLVH để xác minh các hành động liên quan đến cảnh báo.
    - Kiểm tra, phân tích dấu hiệu xâm nhập trên các máy chủ khi có nghi ngờ.
- Vai trò của đơn vị QLVH:
    - Cung cấp đầu mối phối hợp với đơn vị phụ trách ATTT trong quá trình giám sát và xử lý sự cố an ninh mạng.
    - Phản hồi các yêu cầu của đơn vị phụ trách ATTT.
    - Đánh giá tác động và tiến hành khắc phục, xử lý sự cố theo khuyến nghị của đơn vị phụ trách ATTT.

b. Quy trình xử lý sự cố an ninh mạng

Quy trình phối hợp xử lý sự cố ATTT giữa đơn vị giám sát ATTT và đơn vị QLVH sẽ được thể hiện bằng lưu đồ dưới đây:



TKTC-BV 32 Quy trình xử lý sự cố an ninh mạng

Giải thích lưu đồ:

B0. Đội ngũ xử lý sự cố ATTT sẽ thực hiện tiếp nhận thông tin sự cố và tiến hành ứng phó, xử lý sự cố theo quy trình.

B1. Sau khi nhận thông tin sự cố, đội ngũ xử lý sự cố sẽ tiến hành phân loại và thẩm định sự cố. Việc phân loại và thẩm định sự nhằm mục đích xác định mức độ nghiêm trọng của sự cố và thẩm định loại sự cố.

Mức độ nghiêm trọng của sự cố được xác định theo các tiêu chí như sau:

Số lượng máy chủ/máy tính bị ảnh hưởng	Khả năng truy cập	Biện pháp phòng thủ	Mức độ ảnh hưởng	Lộ lọt dữ liệu
Mức độ 1: Nhỏ (1 máy)	Người dùng không có quyền truy cập đến các thông tin đặc quyền, các truy cập được giám sát chặt chẽ	Các biện pháp bảo vệ và phát hiện hoạt động hiệu quả	Dữ liệu hoặc hệ thống quan trọng sẽ không bị ảnh hưởng	Không có khả năng lộ lọt dữ liệu
Mức độ 2: Trung Bình (<10 máy)	Người dùng không có quyền truy cập đến các thông tin đặc quyền, nhưng các truy cập không được giám sát chặt chẽ	Các biện pháp bảo vệ hoạt động hiệu quả, các biện pháp phát hiện không hiệu quả	Dữ liệu hoặc hệ thống quan trọng có thể bị ảnh hưởng	Có khả năng lộ lọt dữ liệu
Mức độ 3: Lớn (từ 10 đến 20 máy)	Người dùng có quyền truy cập đến các thông tin đặc quyền, các truy cập được giám sát	Các biện pháp bảo vệ hoạt động không hiệu quả, các biện pháp phát hiện có hiệu quả	Dữ liệu hoặc hệ thống quan trọng sẽ bị ảnh hưởng	Có khả năng cao lộ lọt dữ liệu
Mức độ 4: Rất lớn (>20 máy)	Người dùng có quyền truy cập đến các thông tin đặc quyền, các truy cập không được giám sát	Các biện pháp bảo vệ và phát hiện hoạt động không hiệu quả	Dữ liệu hoặc hệ thống quan trọng đã bị ảnh hưởng	Dữ liệu đã bị lộ lọt và đang tiếp tục

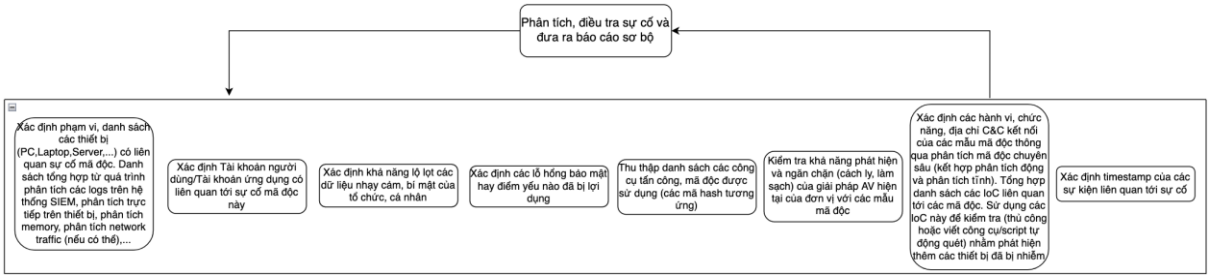
Mỗi tiêu chí sẽ có 4 mức điểm đánh giá từ 1 đến 4, đội ngũ xử lý sự cố ATTT sẽ dựa vào sự cố và tính điểm trên từng tiêu chí. Tổng điểm của các tiêu chí sẽ quyết định mức độ nguy hiểm của sự cố như sau:

Mức độ ưu tiên	Mức độ nguy hiểm	Điểm
P1	Nghiêm trọng	16-20
P2	Cao	11-15
P3	Trung bình	7-10

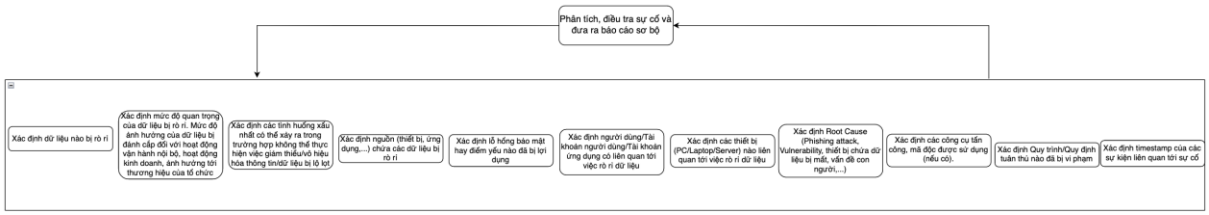
Mức độ ưu tiên	Mức độ nguy hiểm	Điểm
P4	Thấp	1-6

Thẩm định loại sự cố theo hướng dẫn cho từng loại sự cố như sau:

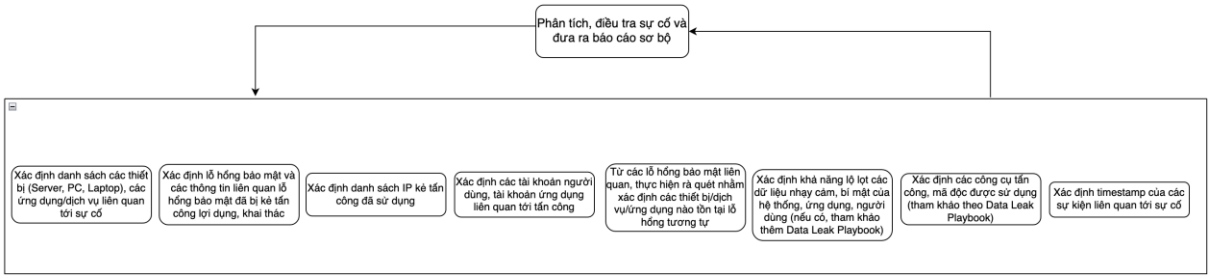
- ***Sự cố mã độc***



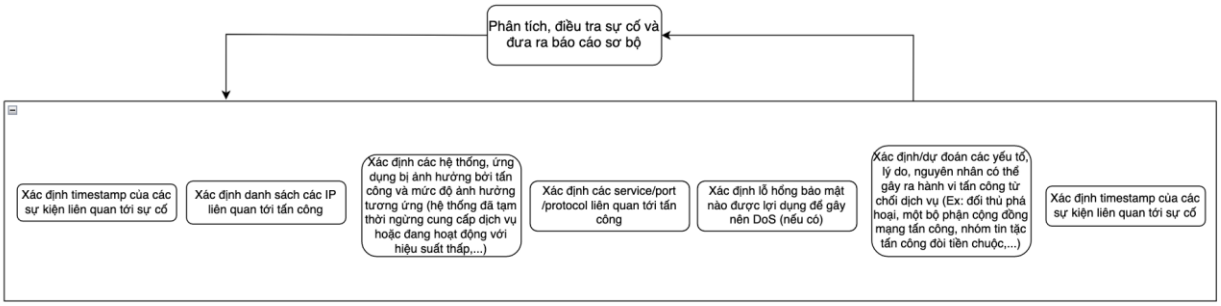
- ***Sự cố lộ lọt dữ liệu***



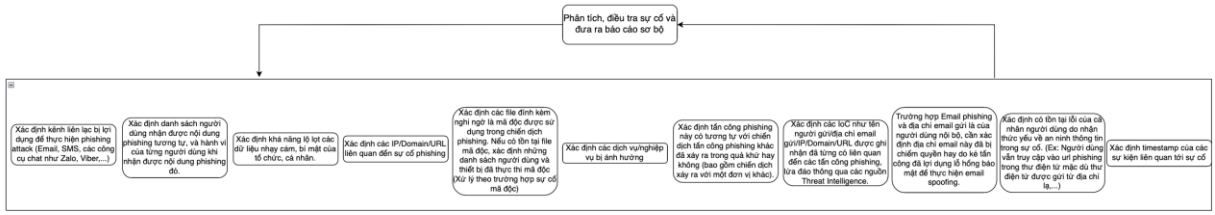
- ***Sự cố khai thác lỗ hổng bảo mật***



- ***Sự cố tấn công từ chối dịch vụ***



- ***Sự cố lừa đảo***



B2. Đội ngũ xử lý sự cố ATTT đưa ra biện pháp chấm dứt tấn công như tạm dừng hoặc cô lập hệ thống tránh tình trạng lây lan sang hệ thống khác. Sau đó đội ngũ xử lý sự cố

ATTT tiến hành gửi hướng dẫn cho đội ngũ Quản lý vận hành để tiến hành thực hiện theo hướng dẫn.

B3. Tiến hành khắc phục theo hướng dẫn và điều tra chuyên sâu

B3.1. Đội ngũ Quản lý vận hành đánh giá biện pháp xử lý sự cố tạm thời và thực hiện theo hướng dẫn của đội ngũ ATTT.

B3.2. Cùng với hướng dẫn xử lý sự cố tạm thời thì đội ngũ ATTT cũng gửi kèm yêu cầu cung cấp thông tin chi tiết để phục vụ quá trình điều tra chuyên sâu.

B4. Đơn vị Quản lý vận hành sau khi tiếp nhận yêu cầu cung cấp thông tin sẽ tiến hành lấy thông tin và cung cấp lại cho đội ngũ ATTT hoặc cung cấp tài khoản truy cập để đội ngũ ATTT truy cập trực tiếp vào hệ thống.

B5. Đội ngũ xử lý sự cố ATTT tiến hành điều tra, phân tích sự cố chi tiết trên hệ thống SIEM hoặc vào trực tiếp máy chủ để xác định các máy chủ bị nhiễm mã độc, phân tích mã độc để đưa ra phương án xử lý.

B6. Sau khi điều tra thì đội ngũ xử lý sự cố ATTT sẽ đưa ra phương án xử lý, khắc phục triệt để sự cố và gửi sang cho đội Quản lý vận hành để tiến hành xử lý. Trong trường hợp đội ngũ xử lý sự cố ATTT không đưa ra được phương án xử lý sự cố triệt để thì cần đưa vấn đề lên Quản lý cấp cao hoặc lãnh đạo chịu trách nhiệm về ATTT để xin ý kiến chỉ đạo và hỗ trợ.

B7. Tiến hành xử lý sự cố triệt để

B7.1. Khi đội xử lý sự cố ATTT chưa đưa ra được phương án khắc phục triệt để thì Quản lý cấp cao về ATTT của đơn vị sẽ tiến hành xem xét, đưa ra ý kiến chỉ đạo, cử thêm các đội ngũ khác trong đơn vị hoặc các nhà thầu độc lập tham gia hỗ trợ xử lý.

B7.2. Khi có phương án xử lý sự cố triệt để thì đội ngũ Quản lý vận hành sẽ tiếp nhận, đánh giá và tiến hành xử lý theo hướng dẫn để đảm bảo sự cố được xử lý triệt để.

B8. Đội ngũ xử lý sự cố ATTT sẽ viết báo cáo lại thông tin về sự cố và gửi lên Quản lý cấp cao và cập nhật tối ưu cảnh báo trên hệ thống SIEM (nếu có).

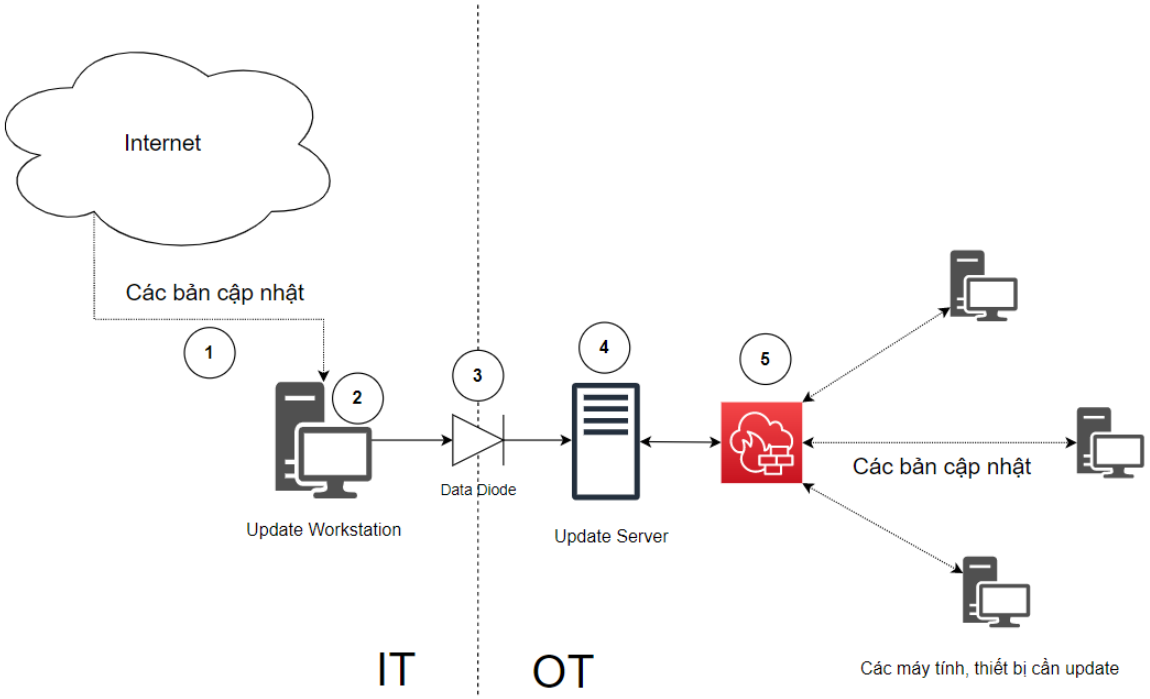
B9. Quản lý cấp cao về ATTT sẽ tiếp nhận báo cáo về sự cố và đưa ra chỉ thị đóng sự cố.

1.6.6.7 Quy trình nâng cấp, cập nhật bản vá cho hệ thống

Mục đích của quy trình: Hướng dẫn cho các cán bộ chủ quản các hệ thống, thiết bị định kỳ kiểm tra và cập nhật bản vá chính hãng để đảm bảo hoạt động và an toàn về mặt bảo mật.

Hiện tại hệ thống đang sử dụng 02 thiết bị Data diode, sau khi trang bị giải pháp Data diode mới phục vụ cho hệ thống GIS và OMS thì chúng tôi đề xuất sử dụng 02 thiết bị này phục vụ cho hệ thống cập nhật bản vá, firmware như dưới. 01 thiết bị dùng cho hệ thống cập nhật bản vá như bên dưới và 01 thiết bị Data Diode dùng làm dự phòng nguội cho thiết bị còn lại.

Mô hình kết nối cho hệ thống cập nhật bản vá:



TKTC-BV 33 Mô hình kết nối cập nhật bản vá

a. Đối tượng trong quy trình xử lý sự cố an ninh mạng

- Quy trình này áp dụng đối với:
  - Cán bộ QLVH: chủ quản các hệ thống máy chủ, thiết bị bảo mật

b. Quy trình nâng cấp, cập nhật bản vá cho hệ thống

Bước 1: Cán bộ QLVH đăng nhập vào hệ thống/ thiết bị để kiểm tra phiên bản của phần mềm/ Firmware của thiết bị hiện tại. Cán bộ QLVH vào website hỗ trợ của phần mềm/ thiết bị đó để tìm bản cập nhật mới nhất cũng như các hướng dẫn cài đặt kèm theo.

Khuyến nghị công việc này cần thực hiện định kỳ 01 tháng 01 lần.

Bước 2: Cán bộ QLVH tải các bản cập nhật từ trang chính thức của các nhà cung cấp (vendor), kèm theo giá trị hash của các file cập nhật về máy trạm dùng riêng phục vụ cập nhật.

Chú ý: Máy trạm cập nhật chỉ sử dụng phục vụ cập nhật, tuyệt đối không sử dụng vào việc khác. Máy chỉ kết nối vào Internet khi cần tải bản cập nhật, và chỉ kết nối vào trang web phát hành bản cập nhật của hãng để tải về. Bản thân máy trạm phải được cập nhật đầy đủ và trang bị phần mềm chống virus, mã độc mới nhất. Khi không có nhu cầu tải bản cập nhật, máy trạm này phải được ngắt khỏi Internet (đường mô tả kết nối từ Internet vào máy trạm cập nhật thể hiện dạng nét đứt để mô tả kết nối này là tạm thời).

Bước 3: Tại máy trạm cập nhật, tiến hành kiểm tra giá trị hash (sử dụng công cụ miễn phí, ví dụ Hash Generator của SecurityExploded) để bảo đảm bản download không bị thay đổi so với bản gốc. Sau đó kiểm tra file download bằng các trình diệt virus, mã độc để giảm thiểu rủi ro.

Bước 4: Chuyển file chứa bản cập nhật qua data diode (sử dụng giao thức FTP mà data diode hỗ trợ) vào máy chủ dùng riêng phục vụ cập nhật trong mạng nội bộ.

Bước 5: Cán bộ QLVH thử nghiệm việc cập nhật bản vá trên môi trường Test và kiểm tra, đánh giá hoạt động của hệ thống. Môi trường Test có thể là hệ thống Clone từ các máy chủ đang hoạt động hoặc khôi phục 01 bản backup từ hệ thống Backup tập trung. Việc cấu hình cần tuân thủ theo hướng dẫn của hãng cung cấp.
Bước 6. Cán bộ QLVH tiến hành cập nhật bản vá trên môi trường thực sau khi việc đánh giá trên môi trường Test hoàn tất.

1.6.7 Xây dựng đội ngũ vận hành đảm bảo ATTT

1.6.7.1 Đội ngũ giám sát và xử lý sự cố ATTT

Căn cứ theo quyết định 1356/QĐ-BTTTT ngày 07/07/2022 về việc Ban hành Tiêu chí đánh giá giải pháp, dịch vụ Trung tâm giám sát điều hành an toàn, an ninh mạng (SOC), đội ngũ giám sát và xử lý sự cố ATTT tối thiểu cần như sau:

a. Về số lượng

- Tier 1: có tối thiểu 06 người trong đó 02 người/ca (Đảm bảo giám sát ATTT 24/7);
- Tier 2: tối thiểu 03 người;
- Tier 3: tối thiểu 02 người;
- SOC Manager: 01 người.

b. Về chất lượng

- Tier :1 Tốt nghiệp ĐH chuyên ngành CNTT/ATTT hoặc chuyên ngành gần với CNTT theo quy định; Có kinh nghiệm ít nhất 1 năm trở lên; Có 1 trong các chứng chỉ CEH, S+, CSA, CND hoặc tương đương;
- Tier 2: Tốt nghiệp ĐH chuyên ngành CNTT/ATTT hoặc chuyên ngành gần với CNTT theo quy định; Có kinh nghiệm ít nhất 3 năm trở lên; Có 1 trong các chứng chỉ: ECIH, CHFI, OCSP hoặc tương đương;
- Tier 3: Có kinh nghiệm ít nhất 5 năm trở lên; Có 1 trong các chứng chỉ: CHFI, CTIA, OCSP, CHFI, OSCE, GSEC hoặc tương đương
- SOC Manager: Có kinh nghiệm ít nhất 5 năm trở lên; Có 1 trong các chứng chỉ: CISA, CISSP, CISM, CCISO hoặc tương đương.

c. Đề xuất đối với EVNHANOI

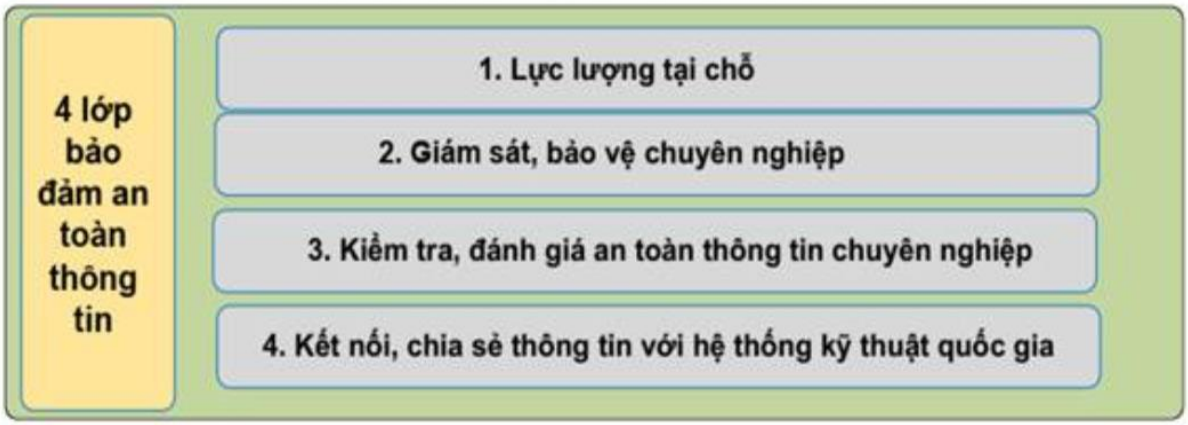
Theo quy định của Bộ TTTT cần tối thiểu 12 người để đảm bảo ATTT cho tổ chức. Tuy nhiên thực tế hiện nay số lượng và chất lượng nhân sự đảm bảo ATTT của EVNHANOI chưa đáp ứng yêu cầu nên ta có 02 phương án sau:

- Phương án 1: EVNHANOI cần tuyển dụng bổ sung thêm kỹ sư, đào tạo các kỹ sư về chuyên môn. Đối với phương án này thì EVNHANOI có thể tiết kiệm được chi phí thuê dịch vụ, tuy nhiên việc tuyển dụng, đào tạo một đội ngũ đảm bảo ATTT không phải là một việc dễ dàng, cần thời gian thông thường từ 06 tháng tới 02 năm để gây dựng đội ngũ. Mặt khác, về chuyên môn thì đội ngũ nội bộ thông thường chỉ tự chủ giải quyết được khoảng 60-80% các sự cố liên quan đến ATTT. Các tổ chức lớn ở Việt Nam như các Ngân hàng, tổ chức tài chính hiện

nay vẫn song song việc duy trì 01 đội ngũ đảm bảo ATTT nội bộ và thuê thêm tối thiểu 01 đơn vị chuyên nghiệp để đảm bảo công tác chuyên môn.

- Phương án 2: EVNHANOI cần thuê các đơn vị cung cấp dịch vụ giám sát, đảm bảo ATTT chuyên nghiệp từ các đơn vị cung cấp uy tín trên thị trường. Việc thuê dịch vụ chuyên nghiệp về ATTT cũng được Bộ TTTT khuyến nghị, với mô hình bảo vệ ATTT 04 lớp. Trong đó lớp 02 là. Thuê đơn vị giám sát, bảo vệ ATTT chuyên nghiệp.

(theo Công văn số 1552/BTTTT-THH ban hành ngày Ngày 26/4/2022)



1.6.7.2 Đội ngũ vận hành các giải pháp ATTT

Vận hành thiết bị phần cứng

Đối với hệ thống phần cứng bao gồm: hệ thống HCI, hệ thống backup, hệ thống Firewall thì cần tối thiểu 01 chuyên viên quản trị với kỹ năng sau:

- Quản trị hệ thống ảo hóa máy chủ và lưu trữ: với chứng chỉ về vSphere, vSAN hoặc tương đương: VMware Certified Professional (VCP) - Data Center Virtualization
- Quản trị hệ thống mạng, firewall: với chứng chỉ Cisco Certified Network Associate (CCNA) hoặc tương đương.

Vận hành hệ thống An ninh, an toàn thông tin

Đối với hệ thống bảo mật bao gồm: hệ thống SIEM, hệ thống PIM/PAM, hệ thống EPS, hệ thống MFA thì cần tối thiểu 01 chuyên viên quản trị với kỹ năng sau:

- Có kỹ năng và hiểu biết về các hệ thống SIEM, PIM, EPS, MFA

II. Giới thiệu về gói thầu:

- Tên gói thầu: Gói thầu 5: Tư vấn giám sát.
- Nguồn vốn: Khấu hao cơ bản.
- Loại hợp đồng: Trọn gói.
- Thời gian thực hiện hợp đồng: 180 ngày

II.1 Phạm vi công việc :

- Giám sát nhà thầu thực hiện Gói thầu 4: Cung cấp thiết bị phần cứng, phần mềm, cài đặt và triển khai giải pháp đảm bảo an toàn, an ninh thông tin cho hệ thống

giám sát, điều khiển và tự động hóa tại EVNHANOI. (180 ngày); Nhà thầu TVGS phải phối hợp chặt chẽ với các nhà thầu thực hiện các gói thầu trên, tổ chức lập kế hoạch chi tiết và bố trí nhân lực giám sát đầy đủ cho từng vị trí cụ thể của dự án, nhằm nâng cao chất lượng và hiệu quả công tác giám sát, thi công.

II.2. Trách nhiệm của nhà thầu tư vấn giám sát gồm các nội dung cụ thể như sau:

II.2.1. Giám sát chất lượng thi công xây dựng công trình:

a. Kiểm tra các điều kiện khởi công công trình xây dựng: Công trình xây dựng chỉ được khởi công khi đáp ứng được các điều kiện theo điều 107 – Luật xây dựng

b. Kiểm tra sự phù hợp năng lực của nhà thầu thi công xây dựng công trình với hồ sơ dự thầu và hợp đồng xây dựng, bao gồm:

+ Kiểm tra về nhân lực, thiết bị thi công của nhà thầu thi công xây dựng công trình đưa vào công trường;

+ Kiểm tra hệ thống quản lý chất lượng của nhà thầu thi công xây dựng công trình;

+ Kiểm tra giấy phép sử dụng các máy móc, thiết bị, vật tư có yêu cầu an toàn phục vụ thi công xây dựng công trình.

c. Kiểm tra và giám sát chất lượng vật tư, vật liệu và thiết bị lắp đặt vào công trình do nhà thầu thi công xây dựng công trình, nhà thầu cung cấp VTTB đã được chủ đầu tư nghiệm thu phê duyệt

d. Kiểm tra và giám sát trong quá trình thi công xây dựng công trình, bao gồm:

+ Kiểm tra biện pháp thi công của nhà thầu thi công xây dựng công trình;

+ Kiểm tra và giám sát thường xuyên có hệ thống quá trình nhà thầu thi công xây dựng công trình triển khai các công việc tại hiện trường. Kết quả kiểm tra đều phải ghi nhật ký giám sát của chủ đầu tư hoặc biên bản kiểm tra theo quy định;

+ Nghiệm thu công trình xây dựng theo quy định của pháp luật về quản lý chất lượng công trình xây dựng Nghị định số 06/2021/NĐ-CP ngày 26/01/2021 của Chính Phủ về quản lý chất lượng công trình xây dựng;

+ Tập hợp, kiểm tra tài liệu phục vụ nghiệm thu công việc xây dựng, bộ phận công trình, giai đoạn thi công xây dựng, nghiệm thu thiết bị, nghiệm thu hoàn thành từng hạng mục công trình xây dựng, xác nhận bản vẽ hoàn công và hoàn thành công trình xây dựng;

+ Phát hiện sai sót, bất hợp lý về thiết kế để đề nghị Bên A điều chỉnh hoặc yêu cầu nhà thầu thiết kế điều chỉnh và tổ chức kiểm định lại chất lượng bộ phận công trình, hạng mục công trình và công trình xây dựng khi có nghi ngờ về chất lượng;

+ Phối hợp với Bên A và các bên liên quan giải quyết những vướng mắc, phát

sinh trong thi công xây dựng công trình. Nhà thầu đảm bảo giám sát thi công Gói thầu 5 : Tư vấn giám sát công trình: Giải pháp an toàn, an ninh thông tin cho hệ thống giám sát, điều khiển và tự động hóa tại EVNHANOI

đúng thiết kế, đúng quy chuẩn, tiêu chuẩn xây dựng được áp dụng, bảo đảm công trình đạt chất lượng cao, khối lượng đầyđủ và chính xác, đúng tiến độ đã được duyệt, đảm bảo an toàn, vệ sinh môi trường và phòng chống cháy, nổ.

II.2.2. Phạm vi công việc của Nhà thầu được thể hiện nhưng không giới hạn và bao gồm các công việc cụ thể sau:

a) Giai đoạn chuẩn bị thi công xây dựng:

- Lập hệ thống quản lý chất lượng phù hợp với yêu cầu của dự án;
- Kiểm tra, báo cáo Bên A về các điều kiện khởi công công trình;
- Kiểm tra và báo cáo bên A về năng lực của các nhà thầu so với hợp đồng đã ký kết;
- Kiểm tra và báo cáo bên A về tính phù hợp với các yêu cầu của dự án và hợp đồng đã ký đối với các loại vật tư, thiết bị của các nhà thầu chuẩn bị đưa vào sử dụng cho công trình;
- Kiểm tra và báo cáo bên A về điều kiện, biện pháp đảm bảo an toàn lao động, vệ sinh môi trường và phòng chống cháy, nổ trong quá trình thi công xây dựng công trình.

b) Giai đoạn thực hiện thi công xây dựng:

- Đánh giá, kiểm soát các quy trình, kế hoạch, biện pháp thi công, biện pháp bảo đảm chất lượng, hệ thống quản lý chất lượng của nhà thầu, đồng thời kiến nghị thay thế hoặc hiệu chỉnh các biện pháp do nhà thầu đưa ra (nếu cần thiết).
- Đôn đốc các nhà thầu thực hiện hệ thống quản lý chất lượng của dự án và các quy định của Nhà nước;
- Kiểm tra tính phù hợp của các thiết bị thi công và nhân lực của nhà thầu so với hợp đồng đã ký kết với bên A như: Kiểm tra tính hợp lệ của các thiết bị, máy móc thi công do nhà thầu trình trước khi đưa vào thi công như: phải được kiểm định của cơ quan có thẩm quyền (đối với các máy móc, thiết bị yêu cầu phải kiểm định); Kiểm tra bố trí nhân lực của nhà thầu để thi công công trình như: chứng chỉ hành nghề của lực lượng công nhân kỹ thuật, việc bố trí cán bộ kỹ thuật, chỉ huy công trường.
- Kiểm tra, giám sát và chấp thuận biện pháp tổ chức thi công, biện pháp thi công của từng công việc do nhà thầu trình so với yêu cầu của dự án và hợp đồng đã ký kết, cụ thể: trước khi triển khai thi công các công việc trọng yếu, Bên B phải yêu cầu nhà thầu trình biện pháp thi công, biện pháp tổ chức thi công để xem xét và chấp thuận; Trường hợp biện pháp thi công, biện pháp tổ chức thi công của Nhà

thầu chưa phù hợp thì bên B phải yêu cầu nhà thầu chỉnh sửa cho phù hợp hoặc đề xuất các biện pháp khác thay thế để làm cơ sở cho nhà thầu thi công; Giám sát việc thực hiện các biện pháp thi công và biện pháp tổ chức thi công của nhà thầu so với các biện pháp đã được phê duyệt.
- Kiểm tra chứng chỉ, chất lượng vật liệu, cấu kiện, sản phẩm xây dựng và kết quả thí nghiệm tại các phòng thí nghiệm hợp chuẩn đã được nêu trong hợp đồng hoặc được bên A chấp thuận do nhà thầu trình trước khi được vào sử dụng cho công trình, cụ thể: Chỉ được cho phép sử dụng vào công trình các loại vật liệu, cấu kiện, sản phẩm xây dựng đảm bảo chất lượng và phù hợp với yêu cầu của dự án, hợp đồng đã ký kết với bên A; Các loại vật liệu, cấu kiện, sản phẩm xây dựng đưa vào công trình phải có xuất xứ rõ ràng, chứng chỉ của nhà sản xuất và phải được thí nghiệm tại các phòng thí nghiệm hợp chuẩn phù hợp với hợp đồng đã ký; Duy trì thường xuyên và liên tục việc giám sát và các biện pháp kiểm soát chất lượng các loại vật liệu, cấu kiện, sản phẩm xây dựng đưa vào công trình.
- Kiểm tra chứng chỉ, chất lượng thiết bị công trình và thiết bị công nghệ của nơi sản xuất thiết bị, kết quả kiểm định chất lượng của các tổ chức có đủ điều kiện năng lực thực hiện theo quy định của pháp luật do các nhà thầu trình; nghiệm thu theo các yêu cầu của thiết kế và các quy chuẩn, tiêu chuẩn, quy phạm hiện hành trước khi cho phép lắp đặt;
- Giám sát quá trình thi công xây dựng công trình của nhà thầu nhằm tuân thủ đúng thiết kế và các quy định hiện hành của pháp luật;
- Kiểm tra, nghiệm thu các công tác thi công xây dựng công trình theo đúng yêu cầu của thiết kế và đúng các quy định của pháp luật hiện hành;
- Đôn đốc việc lập, kiểm tra và xác nhận các bản vẽ hoàn công theo đúng quy định của pháp luật hiện hành;
- Đôn đốc việc lập, kiểm tra và xác nhận hồ sơ thanh toán, quyết toán theo hợp đồng đã ký kết;
- Quản lý, kiểm tra và tập hợp các hồ sơ tài liệu của dự án bàn giao cho bên A sau khi hoàn thành tất cả các công việc;
- Khi phát hiện thiết bị thi công, việc bố trí nhân lực, các vật liệu, thiết bị công trình và thiết bị công nghệ không phù hợp với hợp đồng đã ký, thì Bên B có quyền: Yêu cầu nhà thầu thực hiện đúng hợp đồng đã ký kết với bên A và với các quy định hiện hành của pháp luật; Lập biên bản và yêu cầu nhà thầu ngừng thực hiện công việc cho đến khi nhà thầu thực hiện đúng các quy định của hợp đồng đã ký kết, trường hợp nhà thầu không tuân thủ thì Bên B báo cáo để bên A xử lý vi phạm hợp đồng đối với các nhà thầu; Từ chối nghiệm thu các công tác xây lắp, các giai đoạn xây lắp, việc chạy thử khi không đảm bảo yêu cầu theo hợp đồng

đã ký kết với bên A. Việc từ chối nghiệm thu các công việc của Bên B phải được thể hiện bằng văn bản gửi cho bên A và nhà thầu trong đó nêu rõ lý do từ chối nghiệm thu.
- Đề xuất các biện pháp để xử lý các khiếm khuyết phát hiện trong quá trình thi công xây dựng và chạy thử;
- Kiểm tra, rà soát lại thiết kế để kịp thời báo cáo bên A các mâu thuẫn, các bất hợp lý trong thiết kế nếu có.
- Giám sát tiến độ thi công công trình.- Giám sát công tác an toàn lao động, vệ sinh môi trường.
- Xác nhận bản vẽ hoàn công; khối lượng thi công hoàn thành của nhà thầu. Tổ chức nghiệm thu công trình xây dựng theo quy định I

I.3. Dự kiến thời gian bắt đầu thực hiện: Quý IV/2025.

Trong trường hợp Nhà thầu trúng thầu, thời gian bắt đầu thực hiện công việc giám sát tại công trường cho đến khi kết thúc dự án.

III. Báo cáo và thời gian thực hiện:

* Báo cáo:

- Báo cáo tiến độ thi công hàng ngày: Nhà thầu TVGS có trách nhiệm báo cáo hàng ngày về tiến độ, khối lượng công việc, diễn biến công việc tại hiện trường bằng email (trong báo cáo có kèm theo các hình ảnh công trình) gửi đến Ban Quản lý dự án lưới điện Hà Nội.
- Báo cáo tiến độ thi công hàng tuần: Nhà thầu TVGS có trách nhiệm báo cáo hàng tuần (thứ năm) về tiến độ, khối lượng công việc, diễn biến công việc tại hiện trường bằng bản cứng và email (trong báo cáo có kèm theo các hình ảnh công trình) gửi đến Ban Quản lý dự án lưới điện Hà Nội. Trong trường hợp cần thiết mật độ báo cáo có thể tăng số lần trong tuần khi có yêu cầu của chủ đầu tư.
- Cứ 03 tháng một lần (tháng đầu tiên của quý), Nhà thầu phải báo cáo, đánh giá chất lượng và tiến độ về toàn bộ chất lượng và khối lượng công việc đã thực hiện của công trình, bằng bản cứng và email (trong báo cáo có kèm theo các hình ảnh công trình) gửi đến gửi đến Ban Quản lý dự án lưới điện Hà Nội.
- Vào thứ 6 hàng tuần trước 15h00 nhà thầu phải gửi báo cáo giám sát cho chủ đầu tư (bằng bản cứng có đóng dấu người đại diện nhà thầu, và kèm theo gửi bản mềm qua đường zalo/mail).
- 15 ngày sau khi hoàn thành mỗi giai đoạn công trình nhà thầu nộp báo cáo đánh giá kết quả giám sát giai đoạn đó (có kèm theo hình ảnh gửi kèm)
- 15 ngày sau khi công trình hoàn thành nhà thầu nộp báo cáo đánh giá kết quả công tác giám sát.

- Ngay sau khi phát hiện những yếu tố thay đổi hoặc phát sinh trong quá trình thi công công trình, Nhà thầu phải gửi báo cáo cho chủ đầu tư. Các báo cáo này phải thể hiện rõ nguyên nhân của việc phát sinh, phát sinh do ai (theo thiết kế, theo yêu cầu của Chủ đầu tư hay do sai sót của nhà thầu thi công).

* Tiến độ thực hiện: 180 ngày

IV. Kinh nghiệm và nhân sự của nhà thầu:

Yêu cầu về nhân sự: Chi tiết theo bảng tiêu chuẩn đánh giá phần nhân sự.

V. Vai trò trách nhiệm:

Ban quản lý dự án lưới điện được Tổng công ty Điện lực TP Hà Nội giao nhiệm vụ và chịu trách nhiệm đối với việc thực hiện dự án, cụ thể như sau:

1. Ban quản lý dự án lưới điện Hà Nội:

- Phối hợp chặt chẽ với Nhà thầu trong quá trình thực hiện hợp đồng.
- Cung cấp tài liệu liên quan của dự án hiện có cho nhà thầu (phần thuyết minh và các bản vẽ thiết kế của công trình) cho nhà thầu.
- Cử cán bộ hỗ trợ của bên mời thầu và những tài liệu có liên quan đến nhiệm vụ của tư vấn, tạo điều kiện thuận lợi cho nhà thầu tư vấn trong quá trình thực hiện hợp đồng.

2. Nhà thầu tư vấn giám sát:

- Giám sát chặt chẽ đảm bảo đơn vị thi công thực hiện đúng các cam kết trong Hồ sơ dự thầu, biện pháp tổ chức thi công được duyệt, các yêu cầu kỹ thuật theo quy định an toàn điện, quy phạm ngành điện, tuân thủ theo đúng quy định của pháp luật về quản lý chất lượng công trình xây dựng .
- Tham gia nghiệm thu công trình xây dựng cùng chủ đầu tư theo quy định của pháp luật về quản lý chất lượng công trình xây dựng.
- Mua bảo hiểm trách nhiệm nghề nghiệp và cung cấp cho chủ đầu tư hồ sơ bảo hiểm sau 10 ngày kể từ khi ký hợp đồng.
- Có trách nhiệm tạo điều kiện thuận lợi cho Nhà thầu thi công xây dựng và lắp đặt VTTB đúng tiến độ, đảm bảo chất lượng;
- Phải chịu trách nhiệm trước Chủ đầu tư và pháp luật nếu phát hiện thấy thiếu trách nhiệm, thiếu khách quan hoặc cố tình làm sai trong khi thực hiện nhiệm vụ;
- Có trách nhiệm bồi thường thiệt hại khi làm sai lệch kết quả giám sát đối với khối lượng thi công không đúng thiết kế, không tuân theo tiêu chuẩn áp dụng, quy chuẩn kỹ thuật, nhưng người giám sát không báo cáo với Chủ đầu tư hoặc người có thẩm quyền xử lý và hành vi vi phạm khác do mình gây ra trong quá trình thi công xây lắp.
- Giữ bí mật thông tin liên quan đến dịch vụ tư vấn mà hợp đồng hoặc pháp luật có quy định