BAN CHẤP HÀNH TRUNG ƯƠNG
VĂN PHÒNG
*
Số 18468-CV/VPTW

V/v hướng dẫn mô hình kết nối mạng và hệ thống trực tuyến

ĐẢNG CỘNG SẢN VIỆT NAM

Hà Nội, ngày 24 tháng 10 năm 2025

Kính gửi: Các tỉnh uỷ, thành uỷ,

Căn cứ Quyết định số 204-QĐ/TW, ngày 29/11/2024 của Ban Bí thư về việc phê duyệt Đề án chuyển đổi số trong các cơ quan đảng; Quyết định số 333-QĐ/TW, ngày 23/6/2025 của Ban Bí thư về ban hành Kiến trúc chuyển đổi số trong các cơ quan đảng, phiên bản 3.0; Báo cáo nghiên cứu khả thi Dự án Chuyển đổi số trong các cơ quan đảng; căn cứ tình hình thực tế, Văn phòng Trung ương Đảng hướng dẫn mô hình kết nối mạng và hệ thống trực tuyến bảo mật cấp tỉnh, các xã *(chi tiết trong Phụ lục kèm theo).*

Trong quá trình thực hiện, nếu có vướng mắc, đề nghị các đồng chí trao đổi với Cục Chuyển đổi số - Cơ yếu, Văn phòng Trung ương Đảng, điện thoại 080.43366.

Nơi nhận:
- Như trên,
- Đồng chí Chánh Văn phòng Trung ương Đảng (để báo cáo),
- Ban Cơ yếu Chính phủ,
- Cục Bưu điện Trung ương,
- Cục Chuyển đổi số - Cơ yếu,
- Lưu Văn phòng Trung ương Đảng.

K/T CHÁNH VĂN PHÒNG
PHÓ CHÁNH VĂN PHÒNG

ĐẢNG CỘNG SẢN VIỆT NAM
VĂN PHÒNG
BAN CHẤP HÀNH TRUNG ƯƠNG

VĂN THƯ VĂN PHÒNG TRUNG ƯƠNG ĐẢNG
24-10-2025
16:48:11 +07:00

Võ Thành Hưng

PHỤ LỤC

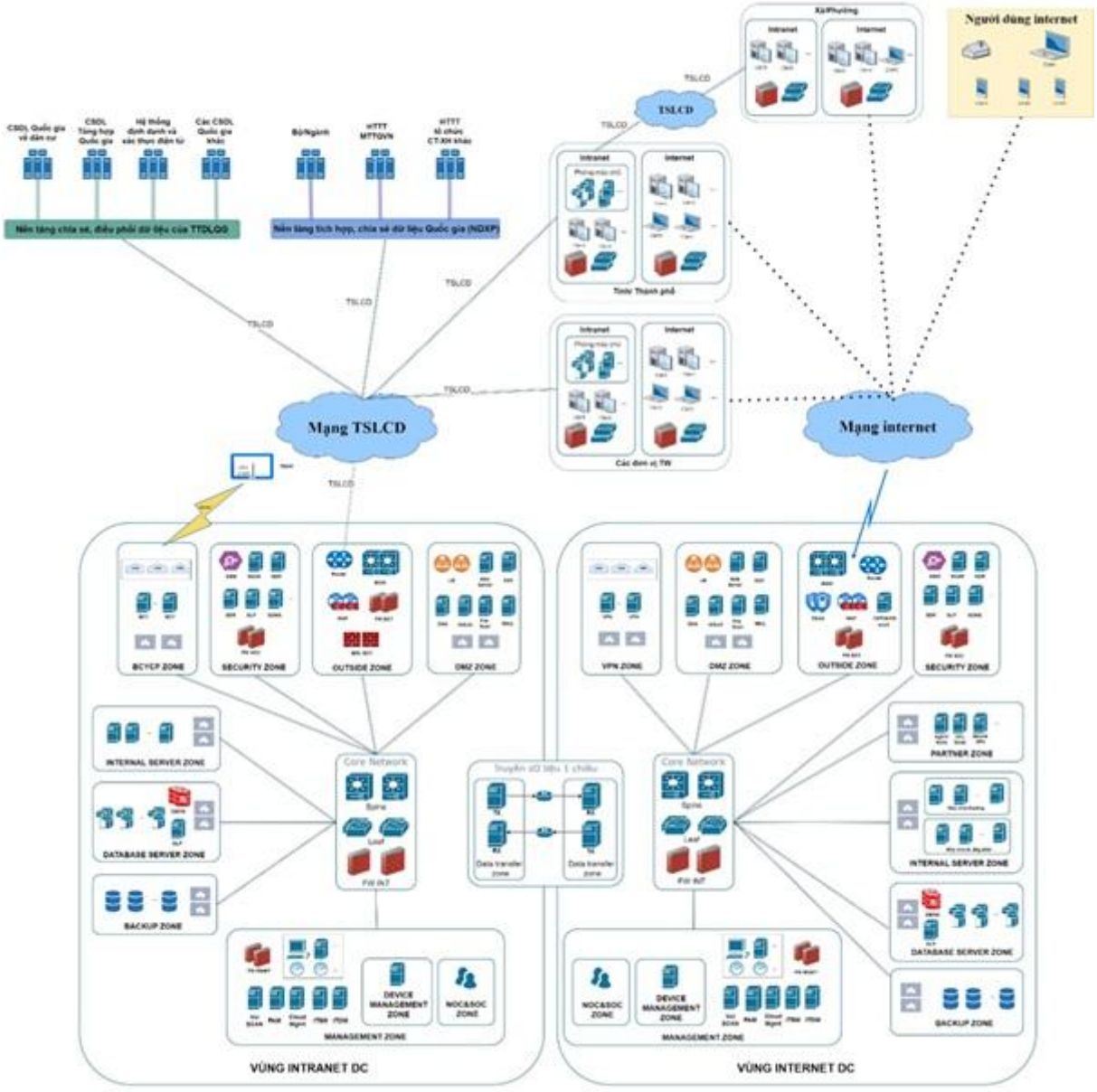
Hướng dẫn mô hình kết nối mạng và hệ thống trực tuyến bảo mật

(Kèm theo Công văn số 18468-CV/VPTW, ngày 24/10/2025 của Văn phòng Trung ương Đảng)

---

1. Mô hình kết nối mạng của các cơ quan đảng

1.1. Mô hình tổng quan kết nối mạng của các cơ quan đảng



Hình 1. Mô hình tổng quan kết nối mạng của các cơ quan đảng

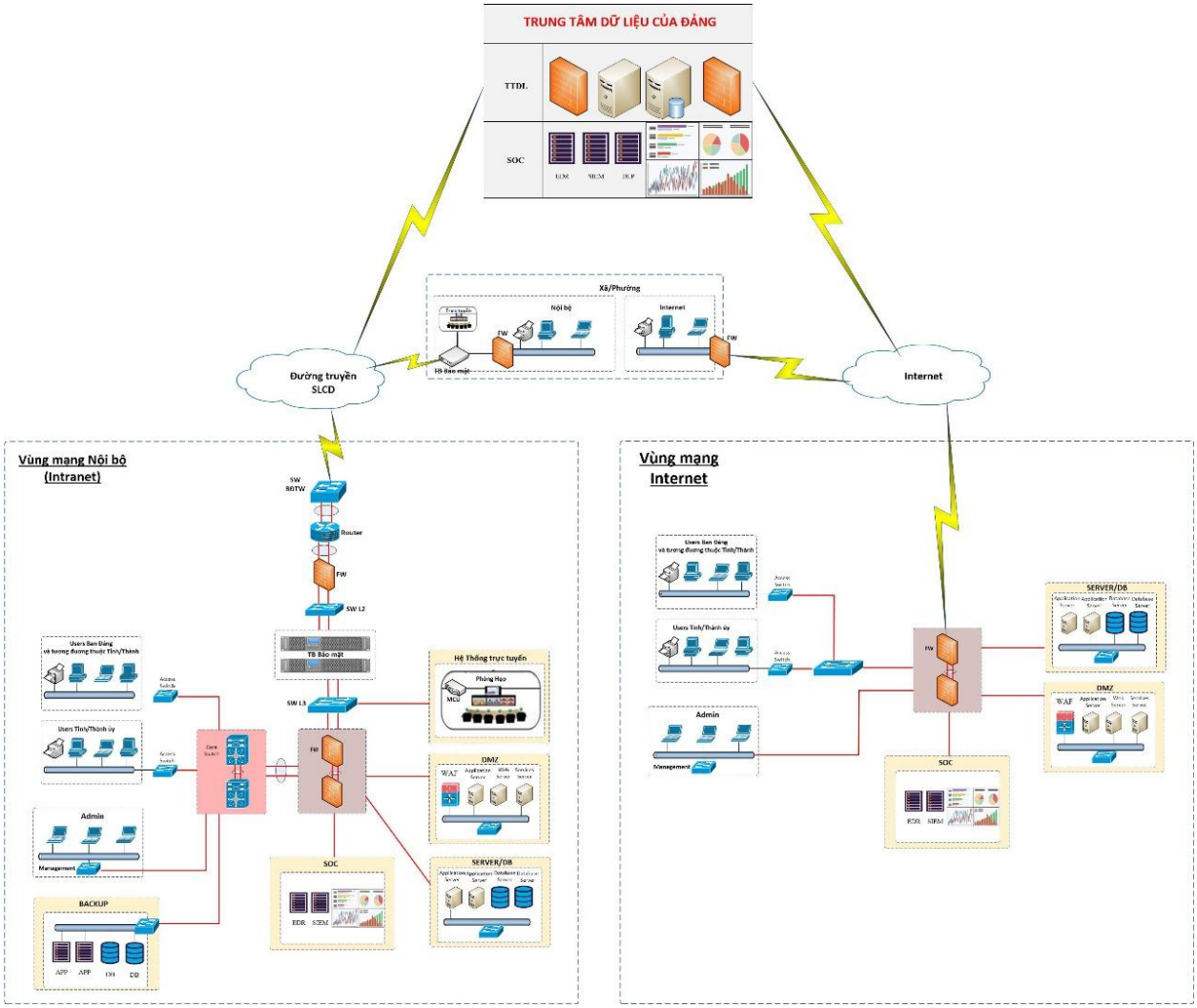
Mạng của các cơ quan đảng gồm 2 vùng: mạng diện rộng (Intranet) và mạng Internet. Mỗi vùng mạng có kết nối các cơ quan từ Trung ương, cấp tỉnh, cấp xã.

Trung tâm dữ liệu của đảng bao gồm Trung tâm dữ liệu chính (DC) và Trung tâm dữ liệu dự phòng (DR). Tại mỗi trung tâm dữ liệu triển khai 02 vùng mạng chính là: Vùng Internet, Vùng Intranet (nội bộ).

- Vùng Internet được thiết kế triển khai các hệ thống CNTT và giải pháp bảo mật cung cấp cho các cán bộ, viên chức có thể khai thác, sử dụng ứng dụng từ ngoài Internet (an toàn).

- Vùng Intranet được thiết kế và triển khai là vùng mạng nội bộ của các cơ quan Đảng và kết nối vào mạng TSLCD của Đảng, đáp ứng cho cán bộ, viên chức có thể khai thác, sử dụng ứng dụng tại trụ sở cơ quan có kết nối mạng nội bộ (TSLCD).

1.2. Mô hình kết nối mạng tại cấp tỉnh



Hình 2. Mô hình kết nối mạng cấp tỉnh

Mạng cấp tỉnh gồm 2 vùng là nội bộ (thuộc mạng Intranet của đảng) và Internet.

Vùng mạng nội bộ ở cấp tỉnh bao gồm các các thành phần cụ thể như sau:

- Zone Outside (vùng mạng biên): được thiết lập để cung cấp các kết nối hệ thống ra bên ngoài mạng truyền số liệu chuyên dùng bao gồm thiết bị định tuyến

(router), thiết bị tường lửa (Firewall) ngoài (hiện tại có thể chưa có), Switch L2, thiết bị bảo mật BML để bảo mật đường truyền kết nối từ tỉnh đến Trung ương.

- Zone Core Network (vùng mạng core): bao gồm thiết bị chuyển mạch Switch Core Layer 3 hiệu năng cao nhằm đảm bảo kết nối giữa các phân vùng nội bộ hệ thống với tốc độ cao, không gây trễ hoặc nghẽn mạng, thiết bị tường lửa (Firewall) trong. Switch Core L3 cần có các cổng kết nối tốc độ 10Gbps để bảo đảm kết nối tới tường lửa, máy chủ và thiết cần thiết khác.

- Zone HNTT (vùng hội nghị truyền hình): kết nối các trang thiết bị của hệ thống hội nghị trực tuyến bao gồm hệ thống MCU THHN mật toàn tỉnh và các thiết bị đầu cuối THHN của cấp tỉnh.

- Zone APP (vùng máy chủ ứng dụng): triển khai các máy chủ vật lý, máy chủ ảo hoá cài đặt các dịch vụ các hệ thống hoặc các phần mềm ứng dụng, các hệ thống thông tin phục vụ cho nội bộ trong tỉnh.

- Zone DB (vùng máy chủ cơ sở dữ liệu): triển khai các máy chủ vật lý, máy chủ ảo hoá cài đặt các cơ sở dữ liệu phục vụ cho nội bộ trong tỉnh.

- Zone LAN (Vùng máy trạm): kết nối các máy trạm của người dùng của văn phòng tỉnh uỷ, thành uỷ, các ban xây dựng đảng, đảng uỷ các cơ quan đảng tỉnh, đảng uỷ uỷ ban nhân dân tỉnh, đảng uỷ quân sự tỉnh, đảng uỷ công an tỉnh để khai thác các phần mềm ứng dụng, các ứng dụng nội bộ tại tỉnh uỷ thành uỷ và các ứng dụng dùng chung của đảng ở Trung ương.

Vùng mạng Internet gồm switch, tường lửa, máy trạm, máy chủ, thành phần giám sát, thành phần bảo đảm an toàn, an ninh.

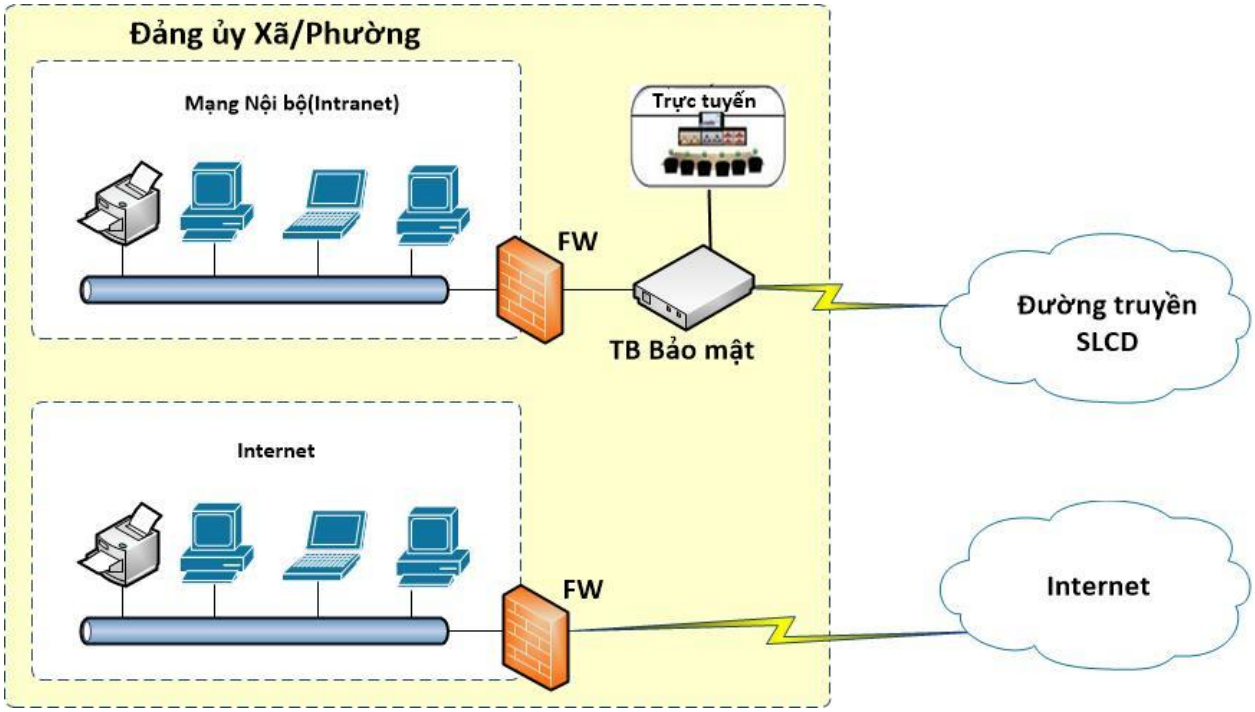
Để đáp ứng yêu cầu đặc thù của tỉnh trong quá trình thực hiện chuyển đổi số, địa phương có thể triển khai xây dựng Trung tâm dữ liệu (tập trung, duy nhất) phục vụ nhiệm vụ riêng, đặc thù của địa phương, bảo đảm tính liên thông, thống nhất và an toàn dữ liệu trên phạm vi toàn quốc, phù hợp với quy định tại Luật Dữ liệu, Nghị định số 165/2025/NĐ-CP và Quy định số 05-QĐ/BCĐTW, ngày 27/8/2025.

** Để nâng cao tính sẵn sàng của hệ thống, khuyến cáo nên sử dụng:*

+ Tường lửa ngoài và tường lửa trong của hai hãng khác nhau giúp giảm thiểu rủi ro từ một điểm lỗi duy nhất, tận dụng được thế mạnh chuyên biệt của mỗi hãng và tăng cường khả năng phòng thủ đa lớp hiệu quả hơn. Nếu một hãng có lỗ hổng bảo mật, tường lửa còn lại có thể vẫn hoạt động tốt, đảm bảo an toàn cho hệ thống).

+ Các thành hệ thống nên triển khai theo mô hình có tính sẵn sàng cao (HA) cho các thành phần chính (ví dụ như: tường lửa, máy chủ, SAN Storage, SAN Switch, thiết bị mạng…).

1.3. Mô hình kết nối mạng tại cấp xã, phường (gọi chung là cấp xã)



Hình 4. Mô hình mạng diện rộng tại cấp xã

Mô tả sơ đồ và nguyên lý hoạt động:

Mạng tại cấp xã chia thành 2 vùng là nội bộ (kết nối vào mạng Intranet của Đảng) và vùng Internet. Các thiết bị tường lửa Firewall cho phép quản lý, cấu hình từ tỉnh.

Vùng nội bộ có các thành phần chính như sau:

- Zone Outside (vùng mạng biên): được thiết lập để cung cấp các kết nối hệ thống ra bên ngoài mạng truyền số liệu chuyên dùng bao gồm thiết của nhà cung cấp đường truyền, thiết bị bảo mật BML để bảo mật đường truyền kết nối từ xã đến Tỉnh và Trung ương.

- Zone HNTT (vùng hội nghị truyền hình): kết nối các thiết bị đầu cuối THHN của cấp xã.

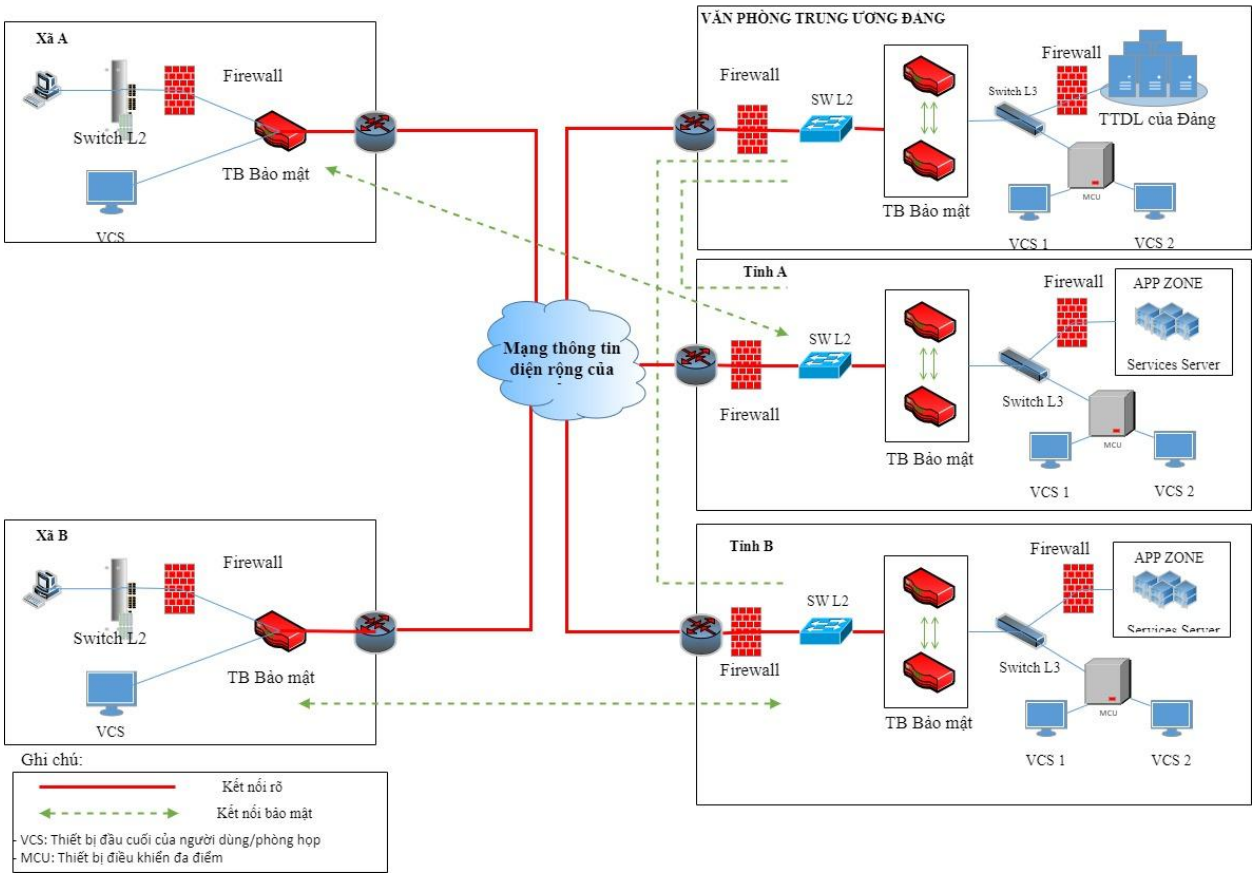
- Zone LAN (Vùng máy trạm): Bao gồm các máy trạm của người dùng xã và thiết bị tường lửa (Firewall) để bảo vệ các máy trạm khi khai thác các ứng dụng nội bộ tỉnh tại Tỉnh/Thành uỷ và các hệ thống thông tin dùng chung của Đảng tại Trung ương.

Vùng Internet gồm có các thành phần: các thiết bị đầu cuối (máy trạm, máy in, máy quét, máy tính bảng, codec …), thiết bị chuyển mạch, tường lửa (Khuyến cáo sử dụng tính năng tường lửa trên thiết bị của nhà cung cấp dịch vụ đường truyền).

2. Hệ thống trực tuyến bảo mật

Hệ thống trực tuyến bảo mật là hệ thống trực tuyến triển khai trong mạng Intranet của các cơ quan đảng, có tích hợp giải pháp bảo mật của Ban Cơ yếu Chính phủ. Hệ thống này có phạm vi kết nối các điểm cầu bảo mật toàn quốc sử dụng đường truyền số liệu chuyên dùng và giải pháp bảo mật cơ yếu.

2.1. Mô hình, giải pháp kết nối



2.2. Mô tả giải pháp

Về Hạ tầng truyền dẫn: Sử dụng hạ tầng mạng thông tin diện rộng của Đảng (mạng Intranet của các cơ quan đảng có giải pháp bảo mật cơ yếu) trên đường truyền số liệu chuyên dùng của các cơ quan đảng, nhà nước.

Tại Văn phòng Trung ương Đảng: Triển khai thiết bị bảo mật kênh truyền BML5000, hoạt động chế độ dự phòng nóng 1: 1, để bảo mật kênh truyền giữa điểm cầu chính (đặt tại Văn phòng Trung ương Đảng) với các điểm cầu thành phần.

Tại cấp tỉnh: Triển khai thiết bị bảo mật kênh truyền BML5000, hoạt động chế độ dự phòng nóng 1: 1, để bảo mật kênh truyền giữa hệ thống trực tuyến của tỉnh (MCU, Codec, thiết bị liên quan) với bên ngoài.

Trong mô hình đầy đủ, cấp tỉnh cần bổ sung Firewall ngoài và Switch có cổng tối thiểu 4x10GB để kết nối BML với Firewall ngoài. Trong trường hợp chưa có

Firewall ngoài sẽ đấu trực tiếp Router vào BML.

Tại cấp Xã: Triển khai thiết bị bảo mật kênh truyền BML100/BML10, để bảo mật kênh truyền giữa điểm cầu cấp xã với bên ngoài.

Mô hình được thiết kế bao gồm 2 cấp, cụ thể:

- Hệ thống MCU Trung ương đặt tại Trung ương do cán bộ kỹ thuật tại Trung ương quản lý, vận hành. Hệ thống MCU nội bộ địa phương đặt tại văn phòng tỉnh uỷ do cán bộ kỹ thuật của tại địa phương quản lý, vận hành.

- Hệ thống MCU và thiết bị đầu cuối truyền hình hội nghị cần đảm bảo các yêu cầu kỹ thuật chung, thống nhất để đảm bảo đồng bộ trong điều khiển và kết nối; hỗ trợ giao thức kết nối SIP hoặc H.323 để kết nối các thiết bị phần cứng; khuyến nghị hỗ trợ kết nối qua WebRTC cho các điểm cầu sử dụng máy tính qua trình duyệt; hỗ trợ chia sẻ nội dung qua các chuẩn chung H.239 (cho H.323) hoặc BFCP (cho SIP); hỗ trợ mã hoá giải mã hình ảnh H.264, H.264 AVC, H.264 SVC; mã hoá mã hoá và giải mã âm thanh G.711, G.719, G.722; khuyến nghị hỗ trợ chuẩn mã hoá Opus, chuẩn mã hoá VP8/VP9 cho các thiết bị kết nối qua trình duyệt. Hệ thống hỗ trợ quản lý các layout, chế độ hiển thị hình ảnh đáp ứng cho các yêu cầu phiên họp qua thiết bị cứng.

MCU cần bao gồm licence số điểm kết nối, số phiên đồng thời đủ cho kết nối nội bộ tỉnh.

Thiết bị đầu cuối trực tuyến Codec sử dụng loại thiết bị chuyên dụng (thiết bị cứng) hoặc phần mềm cài đặt trên máy tính.

Bảo đảm an ninh, an toàn hệ thống: Việc bảo đảm an ninh, an toàn hệ thống do đơn vị chủ quản hệ thống và các cơ quan, đơn vị có liên quan chịu trách nhiệm triển khai, đảm bảo. Tất cả các thiết bị hoạt động trong hệ thống phải được kiểm định, đánh giá an ninh, an toàn trước khi đưa vào sử dụng, kết nối trong hệ thống Hội nghị trực tuyến bảo mật.

3. Mô tả thông số, cấu hình thiết bị cấp tỉnh và cấp xã

TT	Tên thiết bị	Mô tả, cấu hình	Ghi chú
I	**Cấp tỉnh/thành uỷ**		
	Các thiết bị, hạ tầng		
1	Thiết bị định tuyến (Router)	- Thông lượng IPv4 Forwarding (1400Bytes): lên đến 10Gbps - Số lượng route IPv4: ≥ 1M - Số lượng route IPv6: ≥ 600000 - Giao diện: ≥ 2 x 1/10GE (kèm transceiver), 4 x 1GE - Tính năng: Layer 3 - Nguồn: 2 x AC dự phòng - Bảo hành: ≥ 3 năm	Định tuyến kết nối mạng cấp 1 và mạng cấp 2. Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu thực tế.
2	Thiết bị tường lửa vùng ngoài	- Thông lượng Firewall: ≥ 29 Gbps, đo với gói tin Enterprise traffic profile hoặc Appmix - Thông lượng Threat Prevention: ≥ 14 Gbps, khi bật các tính năng Application Control/App-ID, Anti-Malware/Antivirus, IPS, Antispyware, file blocking, SandBlast/WildFire/Sandboxing - Giao diện: 4 x 10GE (kèm transceiver), 4 x 1GE; - Tính năng: Có sẵn tính năng IPS, Application Control, Antivirus, URL Filtering hoặc tương đương, hiệu lực ≥ 3 năm - Độ sẵn sàng cao (High Availability - HA): Active/Active hoặc Active/Passive - Nguồn: 2 x AC dự phòng - Bản quyền thời gian sử dụng, bảo hành: ≥ 3 năm.	Định tuyến và bảo vệ các phân vùng mạng kết nối ngoài. Bản quyền vĩnh viễn, khi không mua bản quyền cập nhật mới, thiết bị vẫn hoạt động bình thường, đầy đủ tính năng nhưng với cơ sở dữ liệu đã được cập nhật lần cuối trước khi hết hạn bản quyền. Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu thực tế.
3	Thiết bị tường lửa vùng lõi	- Thông lượng Firewall: ≥ 35 Gbps, đo với gói tin Enterprise traffic profile hoặc Appmix - Thông lượng Threat Prevention: ≥ 20 Gbps, khi bật các tính năng Application Control/App-ID, Anti-Malware/Antivirus, IPS, Antispyware, file blocking, SandBlast/WildFire/Sandboxing - Giao diện: 4 x 10GE (kèm transceiver), 4 x 1GE; - Tính năng: Có sẵn tính năng IPS hoặc tương đương, hiệu lực ≥ 3 năm - Độ sẵn sàng cao (High Availability - HA): Active/Active hoặc Active/Passive-	Định tuyến và bảo vệ các phân vùng mạng kết nối trong hệ thống tỉnh/thành uỷ. Bản quyền vĩnh viễn, khi không mua bản quyền cập nhật mới, thiết bị vẫn hoạt động bình thường, đầy đủ tính năng nhưng với cơ sở dữ liệu cũ. Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu thực tế.

		Nguồn: 2 x AC dự phòng - Bản quyền thời gian sử dụng, bảo hành: ≥ 3 năm.	
4	Thiết bị chuyển mạch lõi (Core Switch)	- Số port: ≥ 24 hoặc 48 x 10 GbE SFP/SFP+ kèm transceiver - Switching capacity: ≥ 480 Gbps - Forwarding capacity: ≥ 240 Mpps - Tính năng: Layer 2, Layer 3, Ipv6 - Tính năng Stacking hoặc MC-LAG hoặc vPC hoặc tương đương kèm 01 cáp DAC hoặc cáp bắt cặp Switch chuyên dụng. - Nguồn: 2 nguồn AC dự phòng - Bảo hành: ≥ 3 năm	Kết nối các thiết bị đầu cuối. Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu thực tế
5	Thiết bị chuyển mạch nhánh (Switch access)	- Số port: ≥ 24 hoặc 48 x 10/100/1000 Mbps RJ-45; 4 x 1/10 GbE SFP/SFP+ kèm transceiver - Switching capacity: ≥ 128 Gbps - Forwarding capacity: ≥ 95 Mpps - Tính năng: Layer 2 - Nguồn: AC - Bảo hành: ≥ 3 năm	Kết nối các thiết bị đầu cuối. Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu thực tế
6	Máy chủ vật lý cho ảo hoá	- CPU: ≥ 02 x Intel hoặc AMD thế hệ mới nhất - RAM: ≥ 512 GB - SSD: ≥ 03 x 480GB (OS) - HDD hoặc SSD: ≥ 02 x 1TB (dữ liệu) - Giao diện: ≥ 2 x 10GE (kèm transceiver), 2 x 1GE; 2 x 16/32G Fibre Channel - Phần mềm OS bản quyền - Nguồn: 2 nguồn AC dự phòng - Bảo hành: ≥ 3 năm	Số lượng máy chủ tuỳ theo nhu cầu cài đặt ứng dụng và đảm bảo dự phòng tối thiểu N+1 (N thiết bị chạy chính có 01 thiết bị dự phòng). Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu thực tế.
7	Máy chủ số hoá tài liệu	- CPU: ≥ 01 x Intel hoặc AMD thế hệ mới nhất - RAM: ≥ 512 GB - SSD: ≥ 03 x 480GB (OS) - SSD2: ≥ 02 x 1.92 TB (dữ liệu) - Card GPU: Tối thiểu 24GB RAM (cho các máy bóc tách dữ liệu OCR) - Giao diện: ≥ 2 x 10GE (kèm transceiver), 2 x 1GE; 2 x 16/32G Fibre Channel - Phần mềm OS bản quyền - Nguồn: 2 nguồn AC dự phòng - Bảo hành: ≥ 3 năm	Số lượng máy chủ tuỳ theo nhu cầu cài đặt ứng dụng và đảm bảo dự phòng tối thiểu N+1 (N thiết bị chạy chính có 01 thiết bị dự phòng). Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu thực tế.
8	Hệ thống lưu trữ dữ liệu San Storage	1. Thiết bị lưu trữ: - Dual Controller Active-Active - Ổ đĩa cứng >= loại ổ SAS 10K 2.5inch hoặc ổ SSD (dung lượng theo nhu cầu sử dụng). Hỗ trợ Raid tối thiểu: 0,1,5	Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu thực tế

		Cổng giao tiếp: FC SFP (Tốc độ tối thiểu 16Gb) - Nguồn: 2 nguồn AC dự phòng 2. Thiết bị chuyển mạch SAN: Tối thiểu 2 bộ (HA), số lượng port >= 8 cổng (theo nhu cầu thực tế). - Nguồn: 2 nguồn AC dự phòng 3. Thiết bị NAS: Lưu trữ, sao lưu dữ liệu. Dung lượng lưu trữ theo nhu cầu sử dụng. 4. Thiết bị sao lưu Tape Trang bị khi cần sao lưu dữ liệu lớn có nhiều bản sao lưu theo nguyên tắc 3-2-1. * Bảo hành: 3 năm. * Hệ thống lưu trữ, sao lưu bảo đảm phòng, chống ransomware.	
9	Máy tính	- Bộ xử lý >= Intel Core i5, thế hệ 12 - Bộ nhớ: >= 8GB DDR4 - Ổ cứng >= SSD 250GB - Màn hình máy tính để bàn >= 19" - Hệ điều hành (có bản quyền): Windows 10 trở lên hoặc tương đương - Phần mềm cài đặt (có bản quyền): MS Office 2016 hoặc tương đương; Bộ gõ tiếng Việt Unikey; Trình duyệt Chrome; Phần mềm diệt virus.	Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu thực tế
10	Máy in	- In laser đen trắng - 2 mặt tự động - Tương thích hệ điều hành Windows	Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu thực tế
11	Máy quét tài liệu số hoá	- Tính năng quét hai mặt, quét nhiều trang - Khay ADF tối thiểu 40 - Tốc độ quét tối thiểu 30ppm (2 mặt) - Khổ giấy A4 - Tương thích hệ điều hành Windows	Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu thực tế
	Hệ thống bảo đảm ATTT và phần mềm		
12	Hệ thống giám sát SOC	- Trung tâm giám sát SOC tại tỉnh, thành đáp ứng tiêu chí về giải pháp, dịch vụ theo Quyết định 1356/QĐ-BTTTT ban hành ngày 07/7/2022. - Trung tâm giám sát SOC gồm các giải pháp cơ bản: SIEM, IPS, AV, EDR.	Chia sẻ log của các giải pháp cho hệ thống giám sát trung ương
13	Phần mềm AV, EDR, Chống Ransomware	- Phần mềm diệt virus tập trung - EDR (Endpoint Detection and Response): giải pháp bảo mật mạng liên tục giám sát, ghi lại và phân tích hoạt động trên các thiết bị đầu cuối (endpoint) để phát hiện các mối đe doạ và tự động phản ứng. - Giải pháp chống Ransomware	- Intranet: AV, EDR trong mạng nội dùng chung từ Trung ương tới địa phương. - Internet: EDR dùng chung từ Trung ương tới địa phương. AV địa phương tự trang bị.

14	Phần mềm ảo hoá	Phần mềm ảo hoá máy chủ (bản thương mại hoặc mã nguồn mở) đáp ứng: - Số lượng máy chủ hoặc CPU hoặc Core. - Chủng loại: Vĩnh viễn (perpetual) thời gian hỗ trợ kỹ thuật 03 năm, hoặc Có thời hạn (subscription). Ưu tiên lựa chọn loại "Vĩnh viễn"	Đáp ứng cho nhu cầu máy chủ vật lý cho ảo hoá
	Hệ thống trực tuyến		
15	MCU	- Bảo đảm các yêu cầu kỹ thuật chung, thống nhất, đồng bộ trong điều khiển và kết nối; hỗ trợ giao thức kết nối SIP hoặc H.323 để kết nối các thiết bị phần cứng; khuyến nghị hỗ trợ kết nối qua WebRTC cho các điểm cầu sử dụng máy tính qua trình duyệt; hỗ trợ chia sẻ nội dung qua các chuẩn chung H.239 (cho H.323) hoặc BFCP (cho SIP); hỗ trợ mã hoá giải mã hình ảnh H.264, H.264 AVC, H.264 SVC; mã hoá mã hoá và giải mã âm thanh G.711, G.719, G.722; khuyến nghị hỗ trợ chuẩn mã hoá Opus, chuẩn mã hoá VP8/VP9 cho các thiết bị kết nối qua trình duyệt. Hệ thống hỗ trợ quản lý các layout, chế độ hiển thị hình ảnh đáp ứng cho các yêu cầu phiên họp qua thiết bị cứng; - MCU cần bao gồm licence đủ cho số điểm kết nối, tối thiểu 2 phiên họp đồng thời.	
16	Phòng họp trực tuyến	- Codec sử dụng loại thiết bị chuyên dụng (thiết bị cứng) hoặc phần mềm cài đặt trên máy tính. - Bảo đảm các yêu cầu kỹ thuật chung, thống nhất, đồng bộ trong điều khiển và kết nối; hỗ trợ giao thức kết nối SIP hoặc H.323 để kết nối các thiết bị phần cứng; khuyến nghị hỗ trợ kết nối qua WebRTC cho các điểm cầu sử dụng máy tính qua trình duyệt; hỗ trợ chia sẻ nội dung qua các chuẩn chung H.239 (cho H.323) hoặc BFCP (cho SIP); hỗ trợ mã hoá giải mã hình ảnh H.264, H.264 AVC, H.264 SVC; mã hoá mã hoá và giải mã âm thanh G.711, G.719, G.722; khuyến nghị hỗ trợ chuẩn mã hoá Opus, chuẩn mã hoá VP8/VP9 cho các thiết bị kết nối qua trình duyệt. Hệ thống hỗ trợ quản lý các layout, chế độ hiển thị hình ảnh đáp ứng cho các yêu cầu phiên họp qua thiết bị cứng. - Màn hình, thiết bị âm thanh.	

II	**Cấp xã/phường và tương đương**		
	Các thiết bị, hạ tầng		
1	Thiết bị tường lửa (Firewall)	1.1. Firewall: - Thông lượng Firewall: ≥ 1.4 Gbps, đo với gói tin Enterprise traffic profile hoặc Appmix - Thông lượng Threat Prevention: ≥ 0.8 Gbps, khi bật các tính năng Application Control/App-ID, Anti-Malware/Antivirus, IPS, SandBlast/WildFire/Sandboxing - Giao diện: 8 x 1GE (bao gồm 01 cổng mgt); - Tính năng: Có sẵn tính năng IPS, Application Control, Antivirus, URL Filtering hoặc tương đương, hiệu lực ≥ 3 năm - Nguồn: AC - Bản quyền thời gian sử dụng, bảo hành: ≥ 3 năm. 1.2. Phần mềm quản trị tường lửa: Bản quyền phần mềm quản trị hệ thống tường lửa cấp xã được cài đặt tại trung tâm dữ liệu tỉnh để quản trị, vận hành hệ thống tường lửa cấp xã. - Bản quyền thời gian sử dụng, bảo hành: ≥ 3 năm.	Định tuyến và bảo vệ các phân vùng mạng của đơn vị. Bản quyền vĩnh viễn, khi không mua bản quyền cập nhật mới, thiết bị vẫn hoạt động bình thường, đầy đủ tính năng nhưng với cơ sở dữ liệu cũ. Cho phép quản lý, cấu hình từ cấp tỉnh. Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu thực tế.
2	Thiết bị chuyển mạch nhánh (Switch access)	- Số port: ≥ 24 hoặc 48 x 10/100/1000 Mbps RJ-45; 4 x 1/10 GbE SFP/SFP+ (số lượng transceiver chỉ mua khi có nhu cầu thực tế)- Switching capacity: ≥ 128 Gbps - Forwarding capacity: ≥ 95 Mpps - Tính năng: Layer 2 - Nguồn: AC - Bảo hành: ≥ 3 năm	Thiết bị chuyển mạch, kết nối với tường lửa, các thiết bị mạng khác và các thiết bị đầu cuối. Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu thực tế.
3	Máy tính	- Bộ xử lý >= Intel Core i5, thế hệ 12 - Bộ nhớ: >= 8GB DDR4 - Ổ cứng >= SSD 250GB - Màn hình máy tính để bàn >= 19" - Hệ điều hành (có bản quyền): Windows 10 trở lên hoặc tương đương - Phần mềm cài đặt (có bản quyền): MS Office 2016 hoặc tương đương; Bộ gõ tiếng Việt Unikey; Trình duyệt Chrome; Phần mềm diệt virus.	Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu thực tế.
4	Máy in	- In laser đen trắng - 2 mặt tự động - Tương thích hệ điều hành Windows	Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu thực tế.
5	Máy quét tài liệu số hoá	- Tính năng quét hai mặt, quét nhiều trang	Cấu hình và hiệu năng có thể thay đổi để đáp ứng yêu cầu

		- Khay ADF tối thiểu 40 - Tốc độ quét tối thiểu 30ppm (2 mặt) - Khổ giấy A4 - Tương thích hệ điều hành Windows	thực tế.
	Hệ thống bảo đảm ATTT và phần mềm		
6	Thành phần đảm bảo ATTT tại máy trạm	- Giải pháp phòng, chống mã độc AV - Giải pháp phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối EDR	Giám sát tập trung tại Tỉnh hoặc Trung ương, cho phép lấy log từ hệ thống giám sát cấp trên.
7	Phần mềm AV, EDR, Chống Ransomware	- Phần mềm diệt virus tập trung - EDR (Endpoint Detection and Response): giải pháp bảo mật mạng liên tục giám sát, ghi lại và phân tích hoạt động trên các thiết bị đầu cuối (endpoint) để phát hiện các mối đe doạ và tự động phản ứng. - Giải pháp chống Ransomware	- Intranet: AV, EDR trong mạng nội dùng chung từ Trung ương tới địa phương. - Internet: EDR dùng chung từ Trung ương tới địa phương. AV địa phương tự trang bị.
	Hệ thống trực tuyến		
8	Phòng họp trực tuyến	- Codec sử dụng loại thiết bị chuyên dụng (thiết bị cứng) hoặc phần mềm cài đặt trên máy tính. - Bảo đảm các yêu cầu kỹ thuật chung, thống nhất, đồng bộ trong điều khiển và kết nối; hỗ trợ giao thức kết nối SIP hoặc H.323 để kết nối các thiết bị phần cứng; khuyến nghị hỗ trợ kết nối qua WebRTC cho các điểm cầu sử dụng máy tính qua trình duyệt; hỗ trợ chia sẻ nội dung qua các chuẩn chung H.239 (cho H.323) hoặc BFCP (cho SIP); hỗ trợ mã hoá giải mã hình ảnh H.264, H.264 AVC, H.264 SVC; mã hoá mã hoá và giải mã âm thanh G.711, G.719, G.722; khuyến nghị hỗ trợ chuẩn mã hoá Opus, chuẩn mã hoá VP8/VP9 cho các thiết bị kết nối qua trình duyệt. Hệ thống hỗ trợ quản lý các layout, chế độ hiển thị hình ảnh đáp ứng cho các yêu cầu phiên họp qua thiết bị cứng. - Màn hình, thiết bị âm thanh.	

**** Lưu ý:***

- Các thiết bị phải có chứng nhận xuất xứ (CO), chứng nhận chất lượng (CQ) và các chứng nhận liên quan khác theo quy định.

- Các máy trạm được cài các phần mềm bản quyền (Windows, Office), các phần mềm bảo đảm an toàn thông tin (AV, EDR) và các phần mềm liên quan, cần thiết.

- Số lượng thiết bị tuỳ thuộc nhu cầu sử dụng cụ thể của từng cơ quan, đơn vị.

- Thiết bị, hệ thống phải tuân thủ các tiêu chuẩn kỹ thuật, các yêu cầu về điện, điều hoà, phòng ốc, an toàn, bảo mật theo quy định của pháp luật và của Đảng.