BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC BƯU ĐIỆN TRUNG ƯƠNG

SỔ TAY MÔ HÌNH THAM CHIẾU VỀ KẾT NỐI MẠNG CỦA BỘ, NGÀNH, ĐỊA PHƯƠNG VỚI MẠNG TRUYỀN SỐ LIỆU CHUYÊN DÙNG CỦA CÁC CƠ QUAN ĐẢNG, NHÀ NƯỚC

Hà Nội, năm 2020

PHẦN I - MỞ ĐẦU

Để thuận lợi trong tra cứu, áp dụng khi triển khai kết nối mạng bộ, ngành, địa phương vào mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước do Cục Bưu điện Trung ương quản lý. Cục Bưu điện Trung ương xây dựng cuốn sổ tay về kết nối mạng bộ, ngành, địa phương vào mạng truyền số liệu chuyên dùng để triển khai áp dụng trong công việc được đồng bộ, hiệu quả.

Giải thích từ ngữ:

- Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước là hệ thống thông tin quan trọng quốc gia, được sử dụng trong hoạt động truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước. Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước bao gồm mạng TSLCD cấp I và mạng TSLCD cấp II.

- Cổng kết nối là thiết bị mạng, thiết bị bảo mật hoặc thiết bị khác có chức năng tương đương để cung cấp giao diện kết nối giữa hệ thống mạng của cơ quan, tổ chức với các hệ thống mạng bên ngoài.

Từ ngữ viết tắt:

- Mạng TSLCD: Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước.

- CPĐT: Chính phủ điện tử

- TTDL: Trung tâm dữ liệu

- DNVT: Doanh nghiệp viễn thông

- CQNN: Cơ quan Nhà nước

- BNĐP: Bộ, ngành, địa phương

- CBCC: Cán bộ công chức

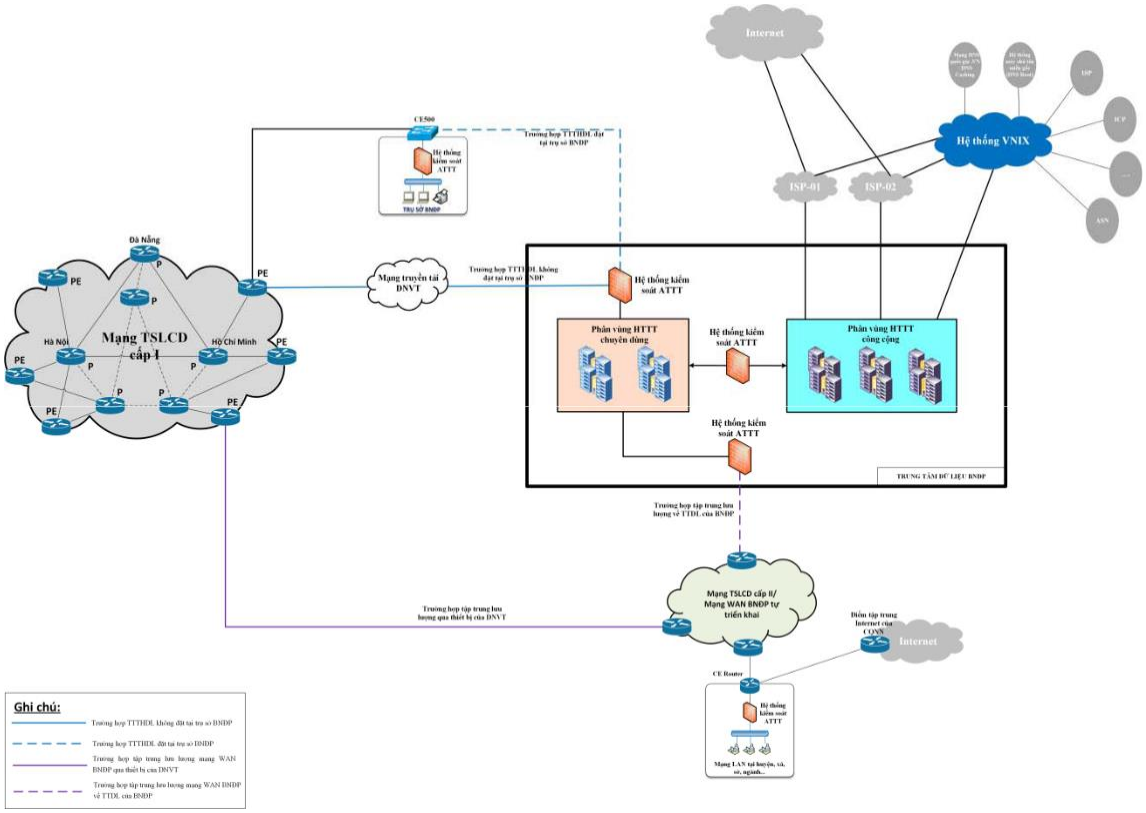
- ATTT: An toàn thông tin

- HTTT: Hệ thống thông tin

- DNS: Hệ thống máy chủ phân giải tên miền sang IP và ngược lại.

PHẦN II - NỘI DUNG

I. MÔ HÌNH TỔNG QUAN MẠNG LAN, WAN, TTDL



Hình 1. Mô hình tổng quan kết nối mạng LAN, WAN, trung tâm dữ liệu

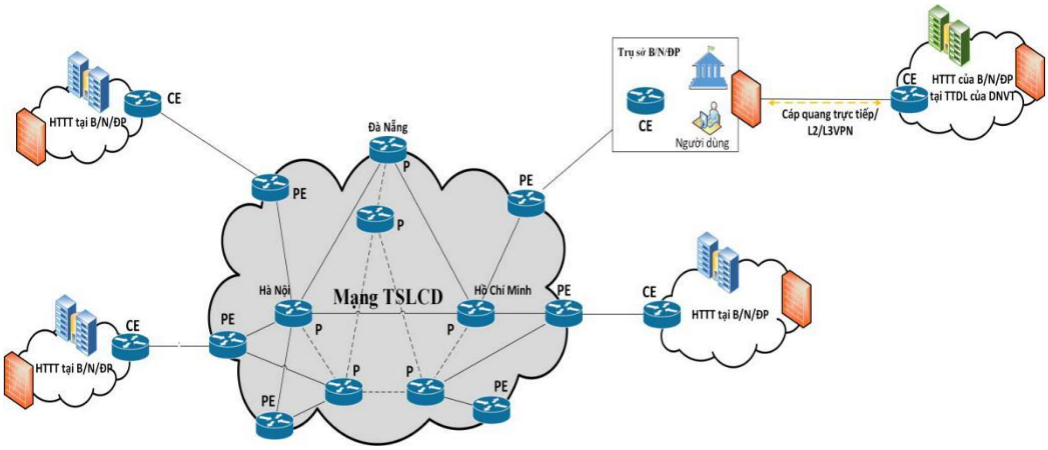
Phân hệ TTDL của BNĐP: kết nối trực tiếp vào mạng TSLCD qua hạ tầng mạng truyền tải của DNVT hoặc kết nối về trụ sở BNĐP và được phân thành 2 phân vùng là HTTT chuyên dùng và HTTT công cộng được đồng bộ về cơ sở dữ liệu thông qua hệ thống kiểm soát ATTT:

***Phân hệ mạng diện rộng (WAN) của BNĐP*:** kết nối tập trung lưu lượng về TTDL của BNĐP hoặc qua thiết bị tập trung của DNVT.

***Phân hệ mạng nội bộ (LAN) của đơn vị trực thuộc BNĐP*:** có 2 kết nối là kết nối mạng TSLCD cấp II và kết nối Internet qua điểm tập trung Internet của CQNN tại DNVT.

II. MÔ HÌNH KẾT NỐI TRUNG TÂM DỮ LIỆU VÀO MẠNG TSLCD

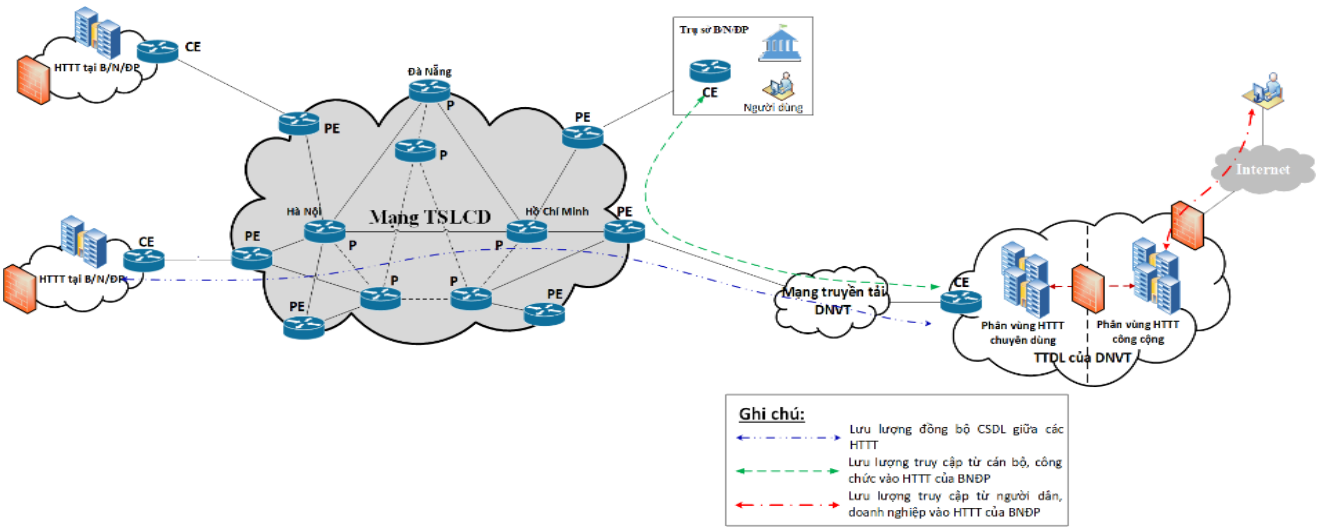
1. MÔ HÌNH SỐ 1: *Kết nối phân vùng TTDL của doanh nghiệp viễn thông với bộ, ngành, địa phương*



Hình 2. Kết nối phân vùng TTDL của DNVT phục vụ BNĐP về trụ sở BNĐP

Mô hình trên được sử dụng trong trường hợp TTDL của DNVT **chưa đủ điều kiện kết nối trực tiếp** vào mạng TSLCD. Để triển khai mô hình này, DNVT cần triển khai kênh kết nối bằng cáp quang trực tiếp, qua thiết lập kênh L2/L3VPN qua hạ tầng mạng của DNVT hoặc kênh IPSec VPN qua Internet từ TTDL của DNVT về trụ sở BNĐP. BNĐP cần đáp ứng các quy định tại Điều 6 Thông tư số 27/2017TT-BTTTT ngày 20/10/2019; Phụ lục 1 Thông tư số 12/2019/TT-BTTTT ngày 5/11/2019 và chịu trách nhiệm các vấn đề liên quan đến an toàn bảo mật khi kết nối vào mạng TSLCD.

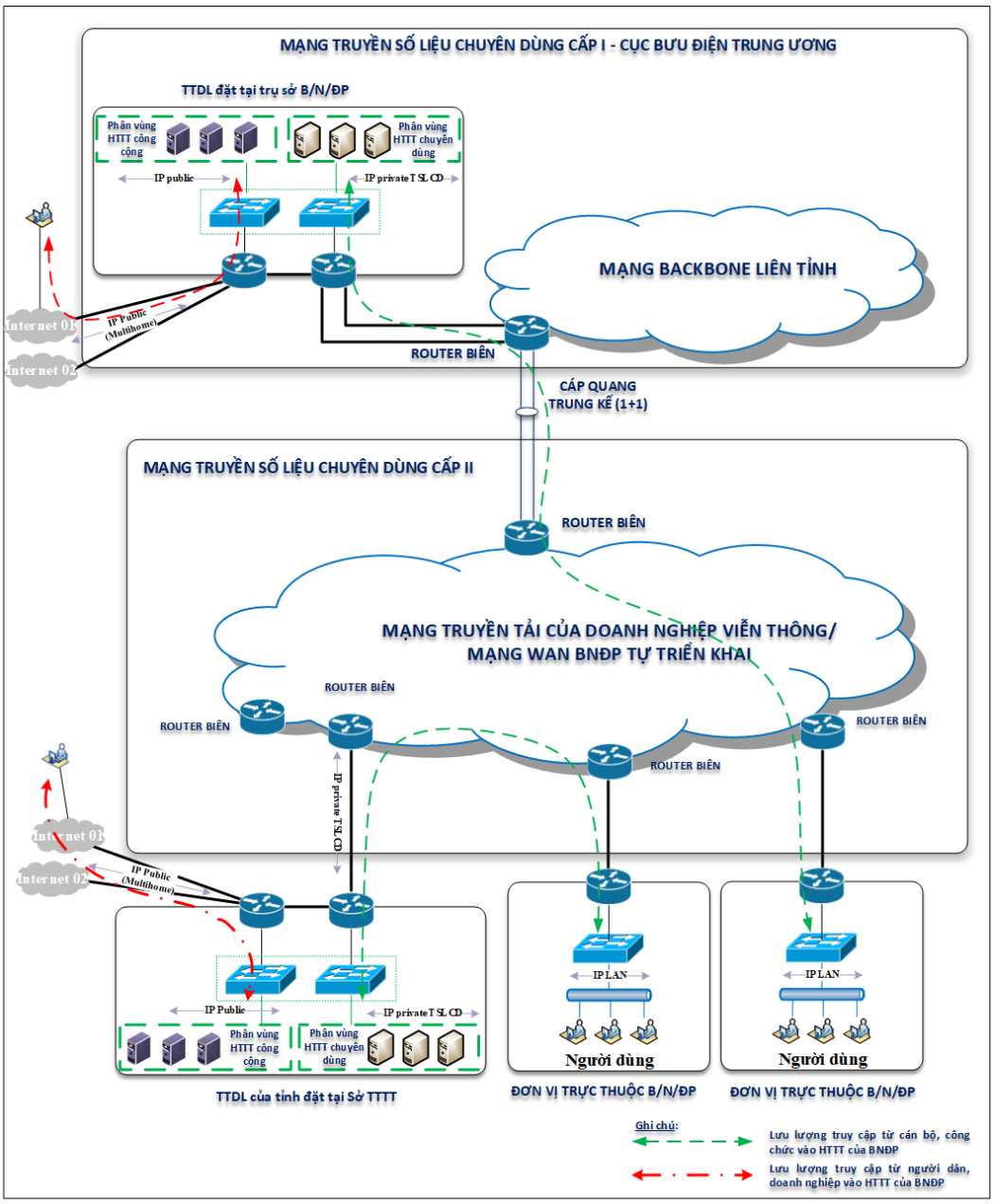
2. MÔ HÌNH SỐ 2*: Kết nối trực tiếp phân vùng TTDL của DNVT phục vụ BNĐP vào mạng TSLCD*



Hình 3. Kết nối trực tiếp phân vùng TTDL của DNVT phục vụ BNĐP vào mạng TSLCD

Mô hình kết nối trên sử dụng trong trường hợp TTDL của DNVT **đủ điều kiện kết nối trực tiếp** vào mạng TSLCD. Để triển khai mô hình này, DNVT cần triển khai kênh kết nối bằng cáp quang trực tiếp vào mạng TSLCD cấp I hoặc qua kết nối trung kế với mạng TSLCD cấp I của Cục BĐTW. Với các yêu cầu cơ bản cần đáp ứng: TTDL của DNVT cần đáp ứng các quy định về TTDL phục vụ BNĐP; DNVT cần phân tách khu vực riêng tại TTDL phục vụ BNĐP với khu vực tại TTDL phục vụ mục đích thương mại cho người dân, tổ chức, doanh nghiệp; Tại khu vực TTDL phục vụ BNĐP: cần phân tách phân vùng HTTT chuyên dùng và phân vùng HTTT công cộng.

3. MÔ HÌNH SỐ 3*: Kết nối TTDL của BNĐP vào mạng TSLCD*



Hình 4. Kết nối TTDL của BNĐP vào mạng TSLCD

Mô hình kết nối trên sử dụng trong trường hợp các BNĐP có TTDL riêng đặt tại trụ sở của BNĐP. Kết nối từ TTDL của BNĐP vào mạng TSLCD sử dụng kênh truyền mạng TSLCD sẵn có của BNĐP. Với các yêu cầu cơ bản cần đáp ứng: BNĐP cần phân tách phân vùng HTTT chuyên dùng và phân vùng HTTT công cộng.

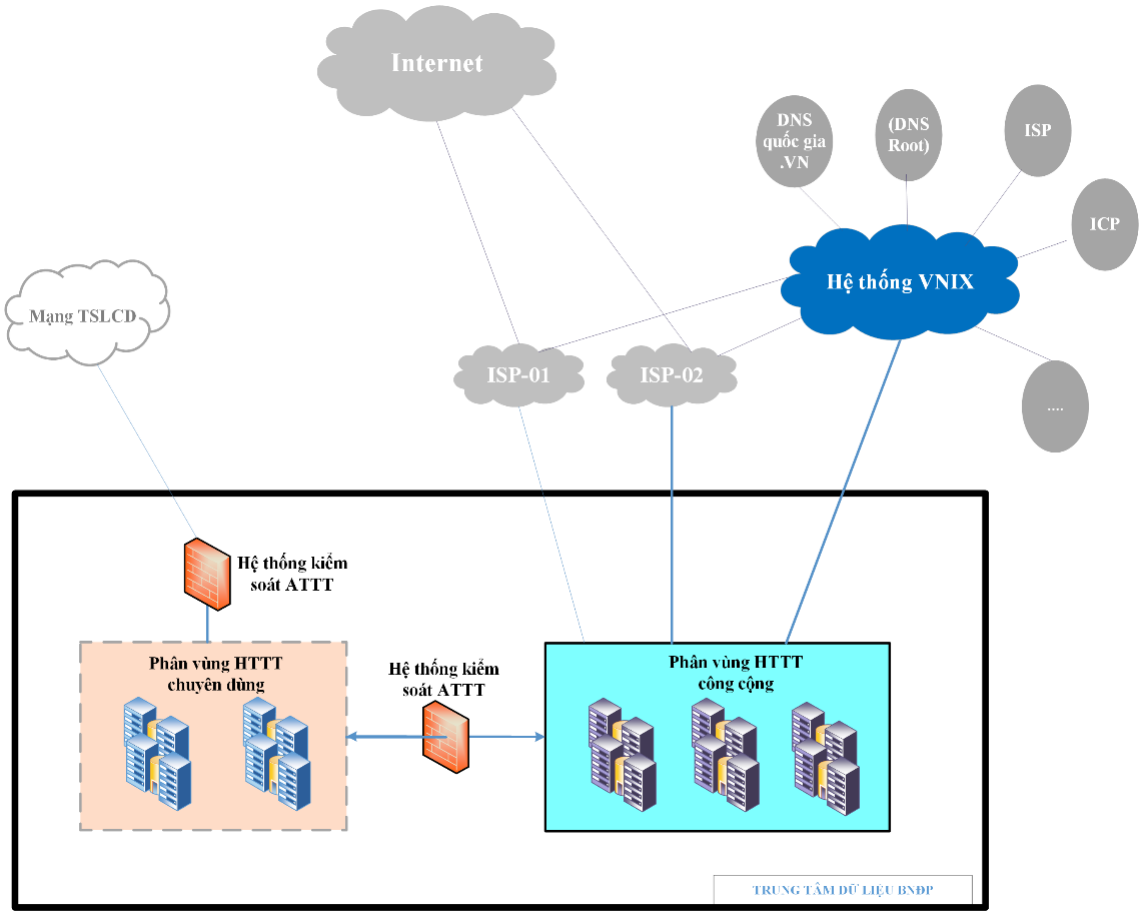
- Đối với phân vùng HTTT chuyên dùng: Kết nối vào mạng TSLCD sử dụng IP private do Cục BĐTW quy hoạch; Phân vùng HTTT chuyên dùng để đồng bộ cơ sở dữ liệu với HTTT của Chính phủ, BNĐP khác và kết nối từ cán bộ, công chức đến HTTT chuyên dùng.

- Đối với phân vùng HTTT công cộng: Phân vùng HTTT công cộng phục vụ người dân, tổ chức, doanh nghiệp truy cập đến HTTT công cộng; Sử dụng AS/IP độc lập do VNNIC cấp, kết nối Internet theo cơ chế multi-home tới một hoặc nhiều ISP, kết nối vào VNIX.

4. MÔ HÌNH SỐ 4*: Mô hình kết nối Internet tại TTDL*

a) Mô hình kết nối Internet của TTDL

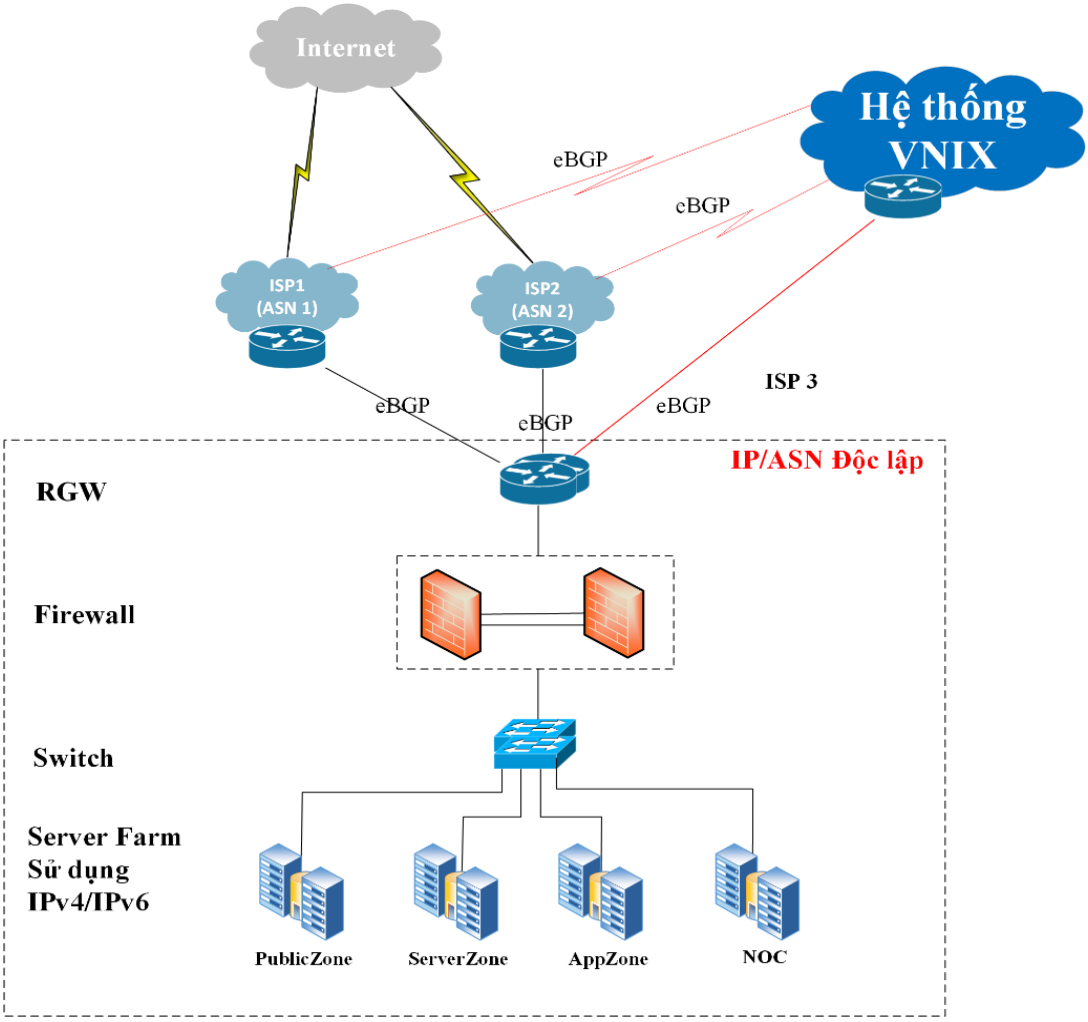
Phân hệ Internet của TTDL quy hoạch cung cấp các dịch vụ chung cho các hoạt động của BNĐP, bao gồm các ứng dụng, cổng thông tin BNĐP, các dịch vụ web khác, cơ sở dữ liệu, các hệ thống thông tin dùng chung như DNS, thư điện tử (email)…



Hình 5. Kết nối Internet tại TTDL

Phân hệ Internet cần được quy hoạch theo kiến trúc của một mạng độc lập, kết nối đa hướng (multi-home), từng bước chuyển đổi IPv6.

b) Giải pháp kết nối đa hướng với ISP và Trạm trung chuyển Internet quốc gia VNIX



Hình 6. Kết nối đa hướng với ISP và VNIX

Hệ thống mạng TTDL kết nối Internet cần được thiết kế theo mô hình phân tầng, bao gồm các khối như sau:

- Tầng định tuyến: khối Router Gateway kết nối định tuyến đa hướng cho toàn bộ hệ thống mạng với các ISP, trạm trung chuyển Internet quốc gia VNIX.

- Tầng an toàn an ninh: khối Firewall/IPS đảm bảo an toàn tổng thể cho hệ thống mạng, bảo vệ hệ thống mạng và các phân vùng quản lý phía trong mạng.

- Tầng chuyển mạch: khối Hệ thống chuyển mạch (Switch) kết nối giữa các tầng, các phân vùng quản lý và các hệ thống thiết bị máy chủ.

- Tầng máy chủ: khối Server farm là các máy chủ, ứng dụng, thiết bị lưu trữ, sao lưu…

Các phương án để kết nối Internet TTDL như sau:

- Phương án kết nối Internet qua các DNVT (ISP): phân hệ Internet của TTDL kết nối (peering, transit) với một hoặc hoặc nhiều các ISP để trao đổi lưu lượng hoặc transit đi Internet theo nhu cầu.

- Phương án đấu nối VNIX[1]: Hệ thống trạm trung chuyển Internet quốc gia VNIX được quản lý bởi Trung tâm Internet Việt nam (VNNIC), hiện tại được triển khai tại 3 điểm Hà Nội, Đà Nẵng và Tp. Hồ Chí Minh. VNIX cho phép các mạng cơ quan, tổ chức, doanh nghiệp sử dụng số hiệu mạng ASN và địa chỉ IP độc lập do VNNIC cấp phát kết nối đến để trao đổi lưu lượng Internet. Đối với phân hệ Internet của TTDL có thể kết nối VNIX theo 2 mô hình như sau:

+ Kết nối đa phương MLPA để trao đổi lưu lượng Internet trong nước: Với mô hình này khi kết nối với VNIX phân hệ Internet của TTDL chỉ cần thiết lập một kênh kết nối vật lý, cấu hình định tuyến eBGP ngang hàng (peering) với thiết bị quản lý định tuyến (route server) của VNIX là có thể kết nối trao đổi lưu lượng trực tiếp với tất cả các thành viên khác, hiện có 21 thành viên là các ISP, ICP, IDC, mạng của cơ quan nhà nước, chính phủ, mạng DNS quốc gia, DNS ROOT … đang kết nối VNIX.

+ Kết nối song phương BLPA: Trên cơ sở kênh kết nối vật lý tới VNIX, ngoài việc kết nối đa phương MLPA như trên thì BNĐP có thể thỏa thuận kết nối song phương BLPA với các thành viên khác hiện có tại VNIX để trao đổi lưu lượng riêng hoặc transit qua mạng khác. Có thể thoả thuận với các ISP đang kết nối vào VNIX để transit lưu lượng Internet quốc tế ngay tại VNIX thay vì phải thuê thêm kênh vật lý đến ISP.

Có thể kết hợp hai phương án kết nối trên (qua ISP và VNIX) đảm bảo tính sẵn sàng cho hệ thống, tiết kiệm chi phí đường truyền và tăng chất lượng kết nối dịch vụ cho hệ thống phân mạng kết nối Internet cho các tổ chức BNĐP.

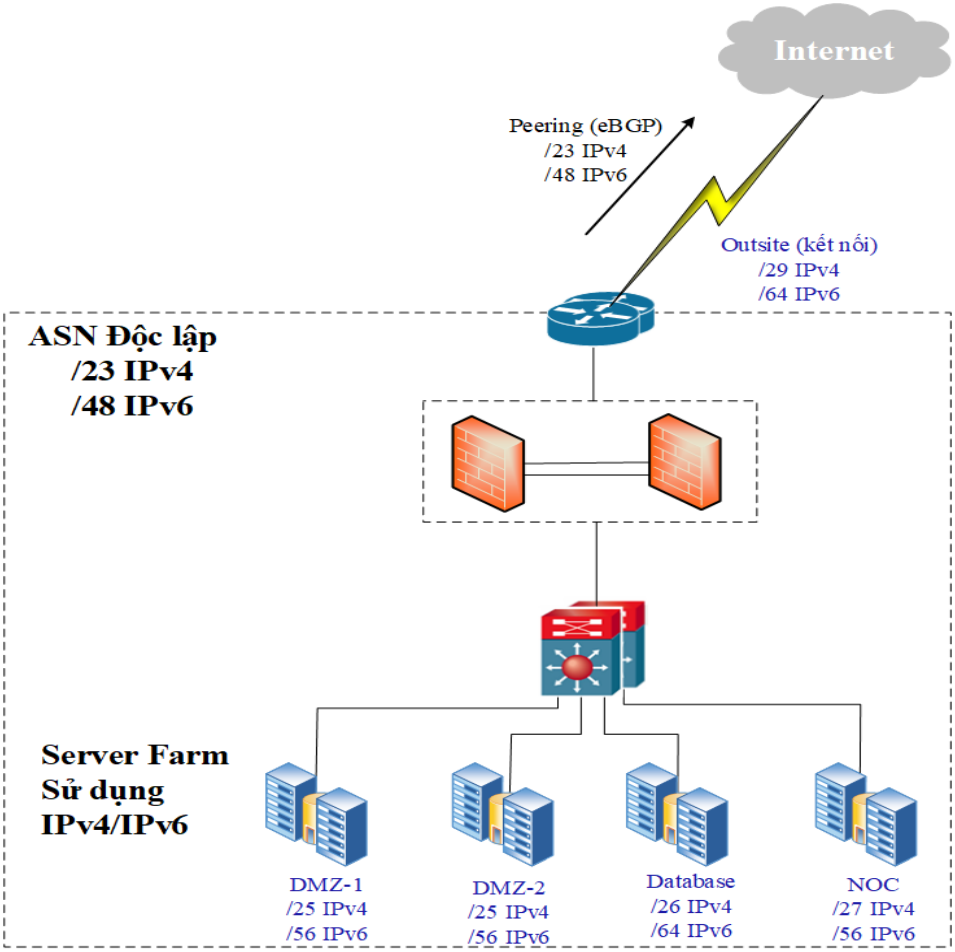
c) Quy hoạch địa chỉ IP (IPv4/IPv6):

Hệ thống mạng BNĐP cần phải phân vùng với mục đích, mức độ an toàn khác nhau để quản lý; và quy hoạch địa chỉ IP cho toàn bộ hạ tầng CNTT đảm bảo hiệu quả, liên tục, tránh bị phân mảnh, đáp ứng nhu cầu sử dụng trong từng khối và đảm bảo khả năng mở rộng trong tương lai mà không cần quy hoạch, thay đổi lại địa chỉ và chính sách định tuyến.

[1] https://vnnic.vn/vnix

Sử dụng địa chỉ IPv4, IPv6 và số hiệu mạng độc lập (ASN) do VNNIC cấp để quy hoạch, phân bổ trong phân hệ Internet của TTDL, không dùng địa chỉ IP private kết hợp với NAT để cung cấp các dịch vụ ra Internet. BNĐP sẽ đăng ký với VNNIC 01 số hiệu mạng, 01 vùng địa chỉ IPv4 (2^16 = 512 địa chỉ) và 01 vùng địa chỉ IPv6 /32 hoặc /48 (tương đương với 2^32 địa chỉ hoặc 2^48 địa chỉ). Từ đó có thể chia thành các vùng địa chỉ nhỏ hơn tuỳ theo nhu cầu, ví dụ như sau (tham khảo trên website của VNNIC[2]):

- Các phân vùng mạng cho các ứng dụng kết nối trực tiếp Internet: DMZ-1, DMZ-2: /25 địa chỉ IPv4 (2^7 = 128 địa chỉ), /56 địa chỉ IPv6
- Các phân vùng CSDL, Middleware: /26 địa chỉ IPv4 (2^6=64 địa chỉ), /64 địa chỉ IPv6.
- Phân vùng NOC/SOC: /27 địa chỉ IPv4, /64 địa chỉ IPv6.
- Phân vùng kết nối bên ngoài tới các ISP: /29 địa chỉ IPv4, /64 địa chỉ IPv6.
- Dự phòng địa chỉ cho các phân vùng có thể phát sinh trong tương lai.

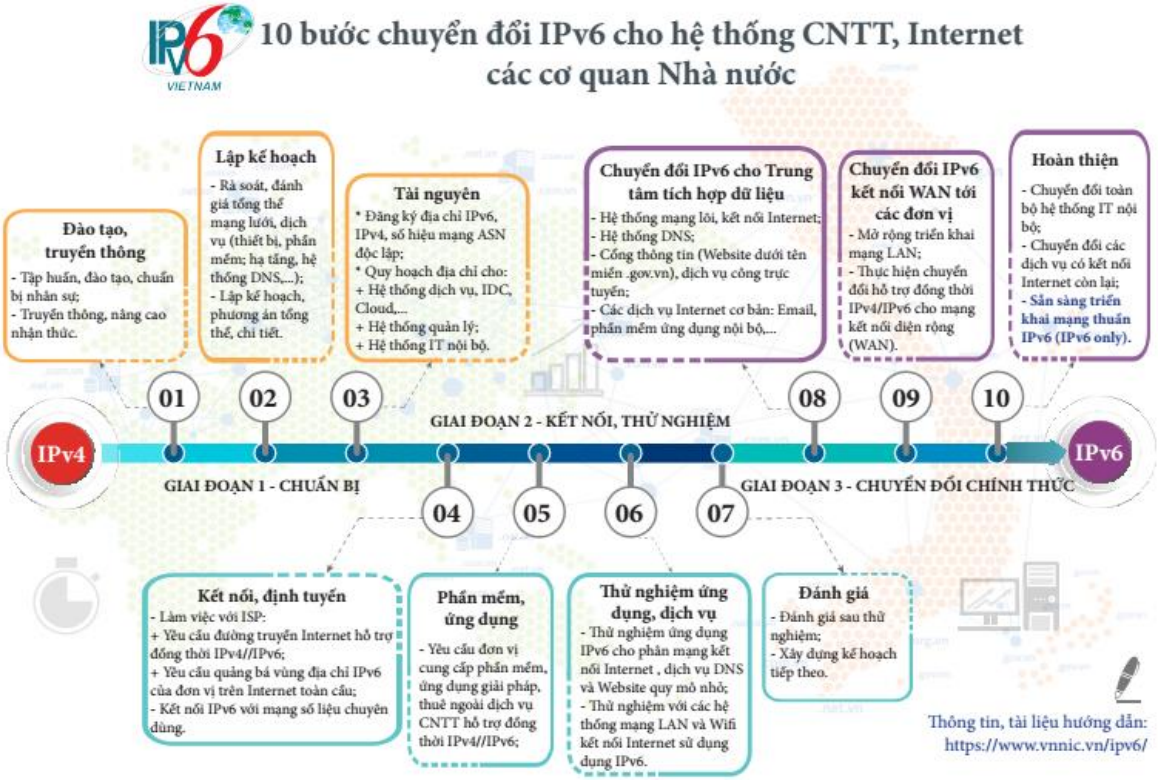


Hình 7. Quy hoạch IPv4/IPv6

[2]https://www.vnnic.vn/sites/default/files/tailieu/VNNIC_TaiLieuHuongDanQuiHoachQuanLySuDungIPv6.pdf

d) Chuyển đổi IPv6:

Địa chỉ IPv4 đã hết, không còn đủ để phát triển mạng Internet, vì vậy cần phải chuyển đổi sang IPv6. Việc triển khai chuyển đổi IPv6 khuyến nghị theo phương án song song IPv4/IPv6 (dual-stack), sau này tiến tới chỉ dùng IPv6 (IPv6 only). Chi tiết tham khảo tại địa chỉ: https://vnnic.vn/ipv6forgov.



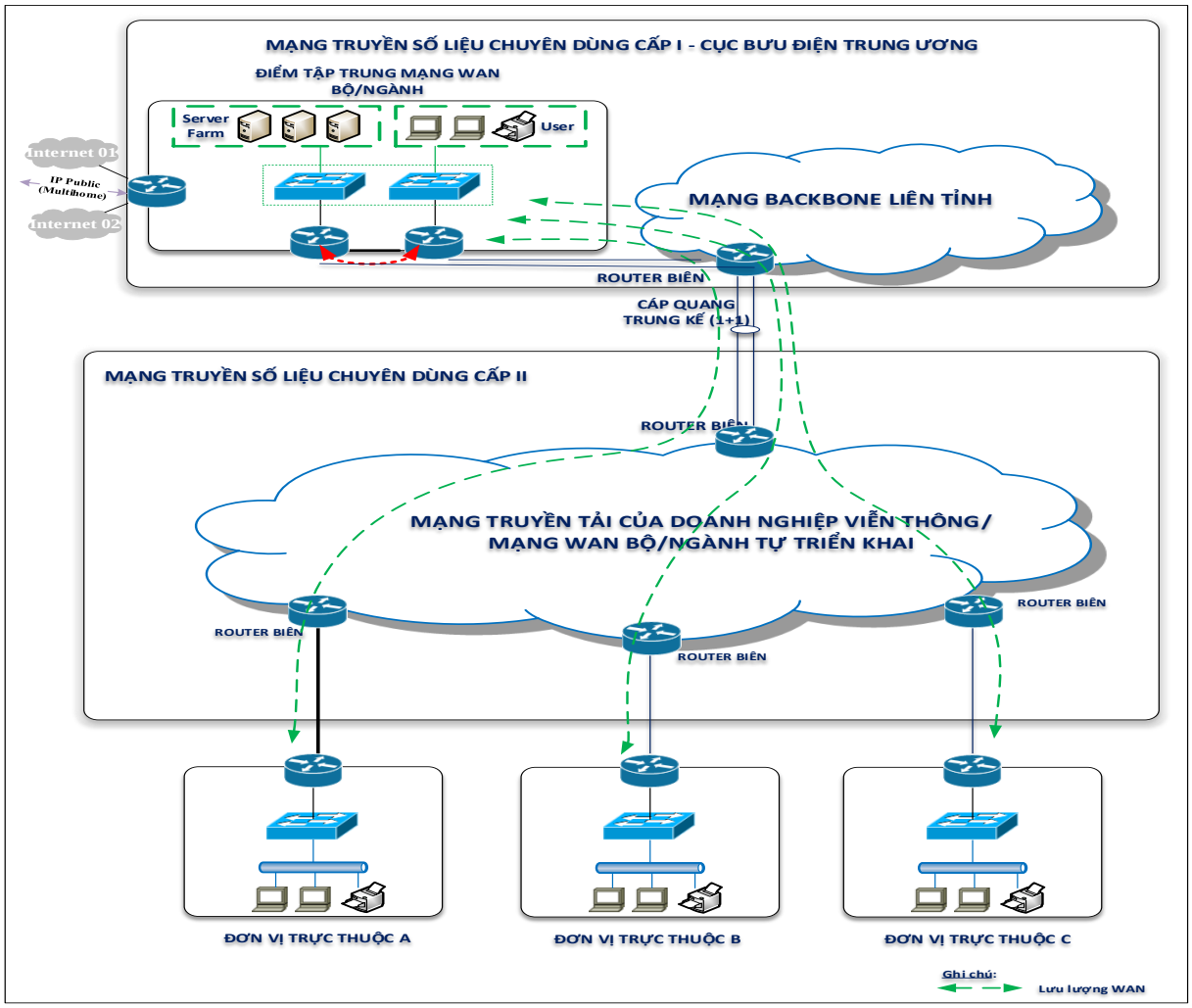
Hình 8. Lộ trình chuyển đổi IPv6 cho các cơ quan Nhà nước

Về cơ bản CQNN thực hiện theo lộ trình chuyển đổi 3 giai đoạn, 10 bước[3] theo khuyến nghị của VNNIC.

[3] https://www.vnnic.vn/sites/default/files/tailieu/brochureIPv6-coquannhanuoc-final.pdf

III. MÔ HÌNH KẾT NỐI MẠNG WAN CỦA BỘ, NGÀNH VÀO MẠNG TSLCD

MÔ HÌNH SỐ 5*: Kết nối mạng WAN của Bộ, ngành vào mạng TSLCD*

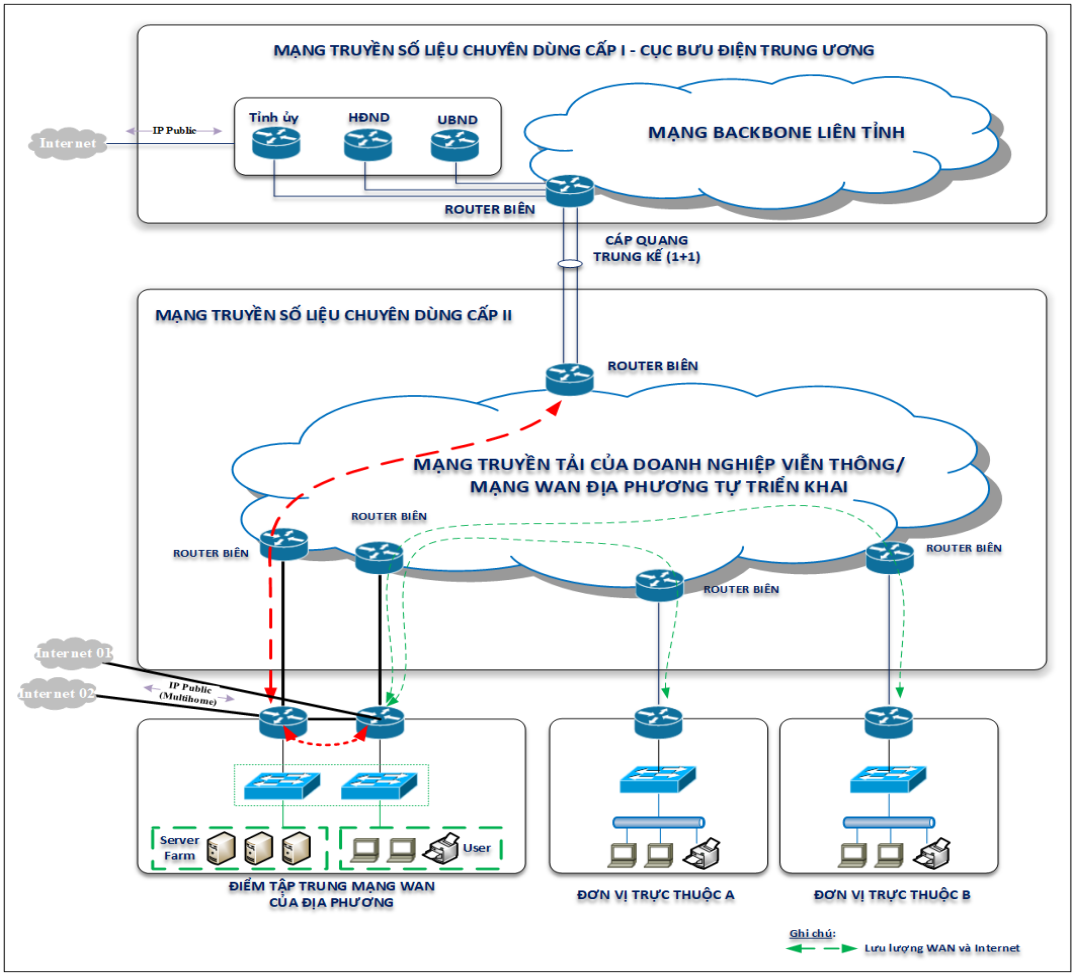


Hình 9. Mô hình kết nối mạng WAN của Bộ, ngành vào mạng TSLCD

Mô hình kết nối trên là mô hình kết nối trực tiếp các đơn vị trực thuộc bộ, ngành lên điểm tập trung mạng WAN của bộ, ngành (thông thường là trụ sở chính hoặc TTDL của bộ, ngành). Với các yêu cầu cơ bản cần đáp ứng: Trên hạ tầng mạng TSLCD cấp II (trong trường hợp bộ, ngành và các đơn vị trực thuộc có kết nối mạng TSLCD cấp II) hoặc hạ tầng mạng WAN của bộ, ngành (trong trường hợp bộ, ngành tự triển khai hạ tầng mạng WAN riêng): tạo kết nối điểm – đa điểm từ các đơn vị trực thuộc về điểm tập trung mạng WAN của bộ, ngành; Tại điểm tập trung mạng WAN của bộ, ngành: thực hiện chuyển tiếp lưu lượng từ các đơn vị trực thuộc đến các ứng dụng tại TTDL của bộ, ngành.

IV. MÔ HÌNH KẾT NỐI MẠNG WAN CỦA ĐỊA PHƯƠNG VÀO MẠNG TSLCD

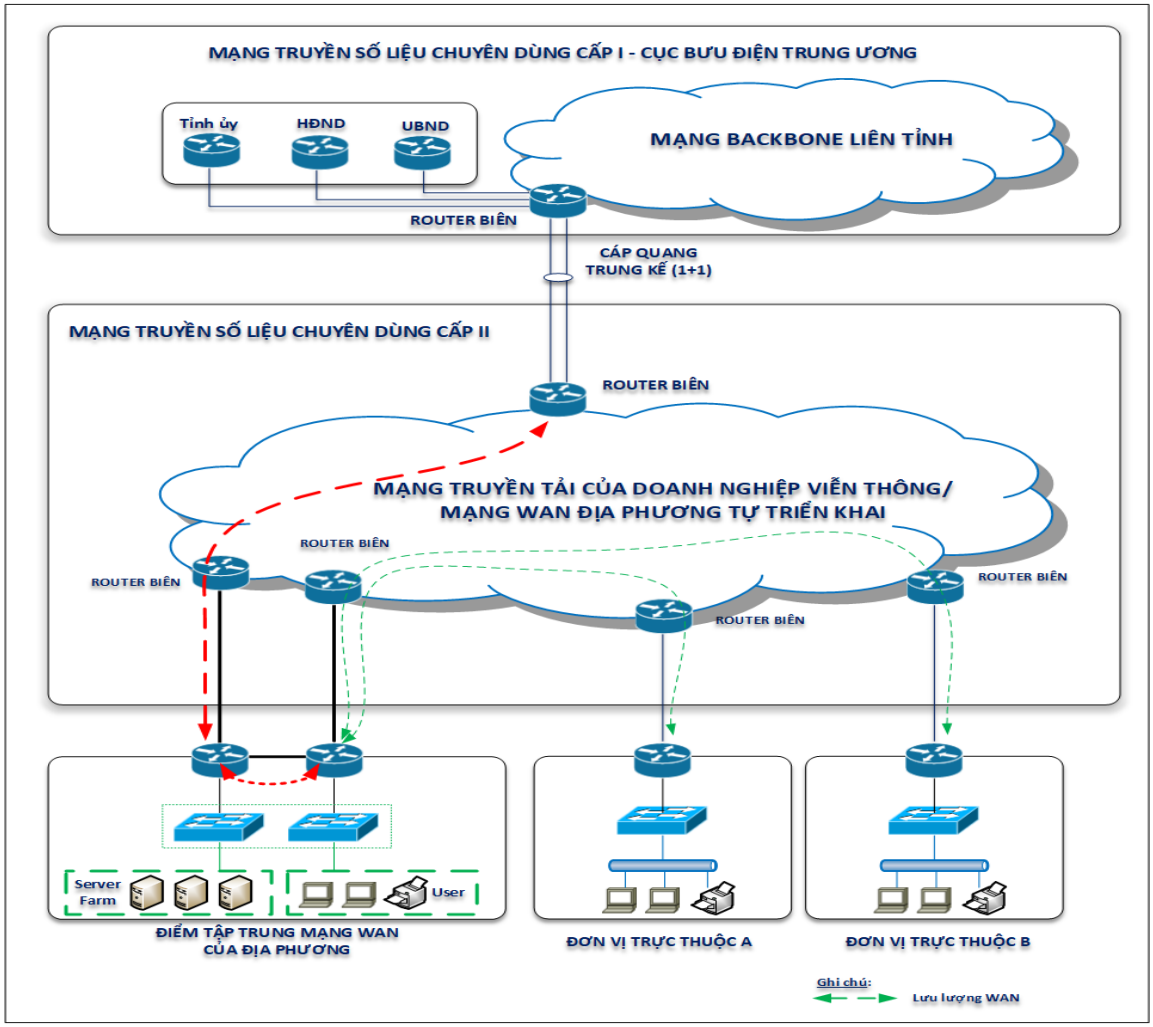
MÔ HÌNH SỐ 6: ***Mô hình tập trung lưu lượng WAN và Internet về điểm quản lý tập trung của địa phương***



Hình 10. Mô hình tập trung lưu lượng WAN và Internet về điểm quản lý tập trung của địa phương

Mô hình trên sử dụng trong trường hợp các địa phương có nhu cầu triển khai Internet tập trung cho các đơn vị trực thuộc. Với các yêu cầu cơ bản cần đáp ứng: Trên hạ tầng mạng TSLCD cấp II *(trong trường hợp địa phương và các đơn vị trực thuộc có kết nối mạng TSLCD cấp II)* hoặc hạ tầng mạng WAN của địa phương *(trong trường hợp địa phương tự triển khai hạ tầng mạng WAN riêng)*: tạo kết nối điểm – đa điểm từ các đơn vị trực thuộc về điểm tập trung mạng WAN của địa phương; Tại điểm tập trung mạng WAN của địa phương thực hiện: Chuyển tiếp lưu lượng từ các đơn vị trực thuộc đến các ứng dụng tại TTDL của địa phương. Chuyển tiếp lưu lượng kết nối Internet của các đơn vị trực thuộc qua kênh kết nối Internet tại điểm tập trung.

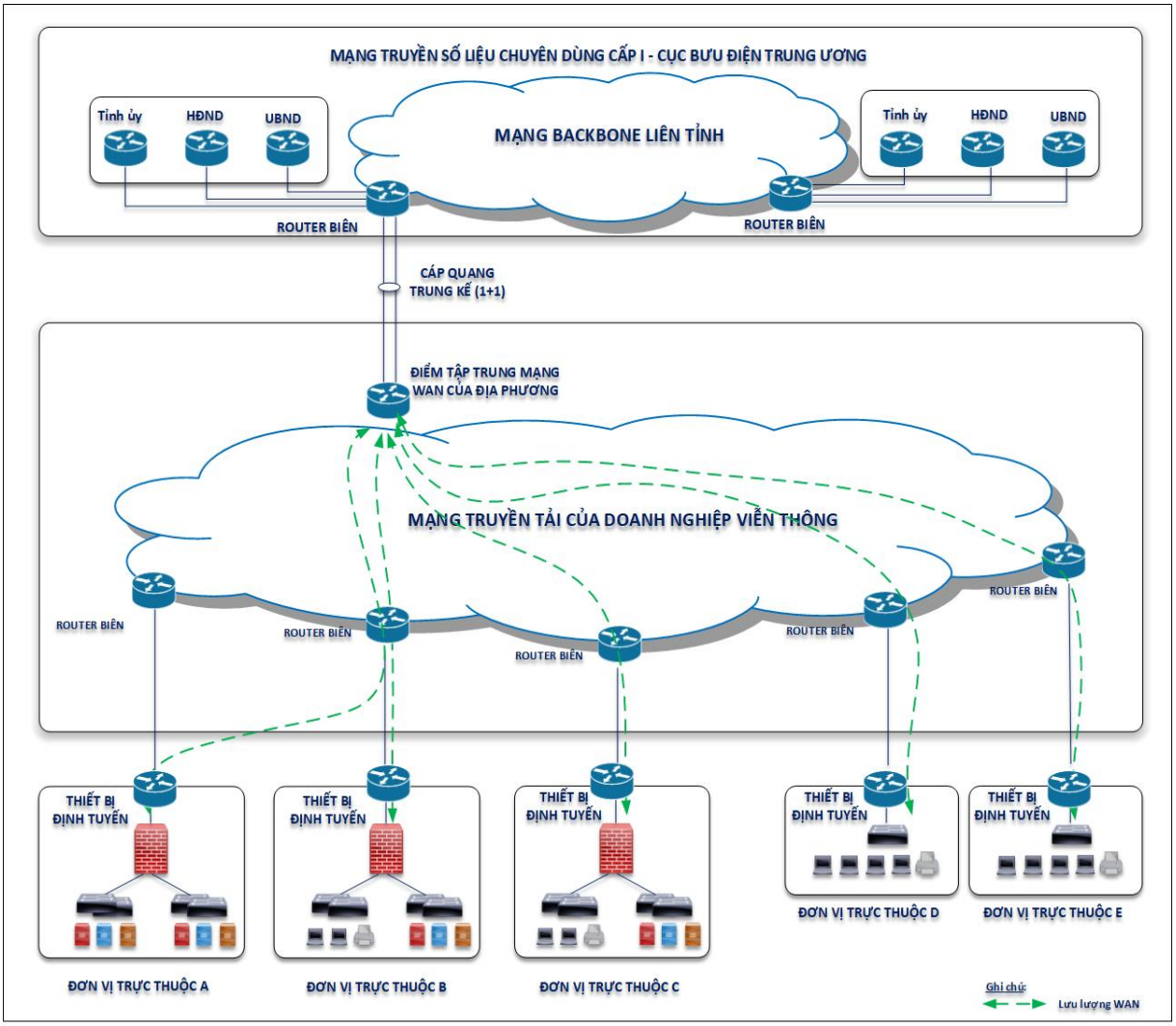
MÔ HÌNH SỐ 7: ***Mô hình chỉ tập trung lưu lượng WAN về điểm quản lý tập trung của địa phương***



Hình 11. Mô hình chỉ tập trung lưu lượng WAN về điểm quản lý tập trung của địa phương

Mô hình trên sử dụng trong trường hợp các địa phương không có nhu cầu triển khai Internet tập trung cho các đơn vị trực thuộc. Với các yêu cầu cơ bản cần đáp ứng: Trên hạ tầng mạng TSLCD cấp II (trong trường hợp địa phương và các đơn vị trực thuộc có kết nối mạng TSLCD cấp II) hoặc hạ tầng mạng WAN của địa phương (trong trường hợp địa phương tự triển khai hạ tầng mạng WAN riêng): tạo kết nối điểm – đa điểm từ các đơn vị trực thuộc về điểm tập trung mạng WAN của địa phương; Tại điểm tập trung mạng WAN của địa phương thực hiện chuyển tiếp lưu lượng từ các đơn vị trực thuộc đến các ứng dụng tại TTDL của địa phương; Đối với lưu lượng Internet: thực hiện rẽ nhánh trực tiếp tại cổng kết nối của các đơn vị trực thuộc.

MÔ HÌNH SỐ 8: ***Mô hình tập trung lưu lượng WAN về điểm quản lý tập trung của DNVT***

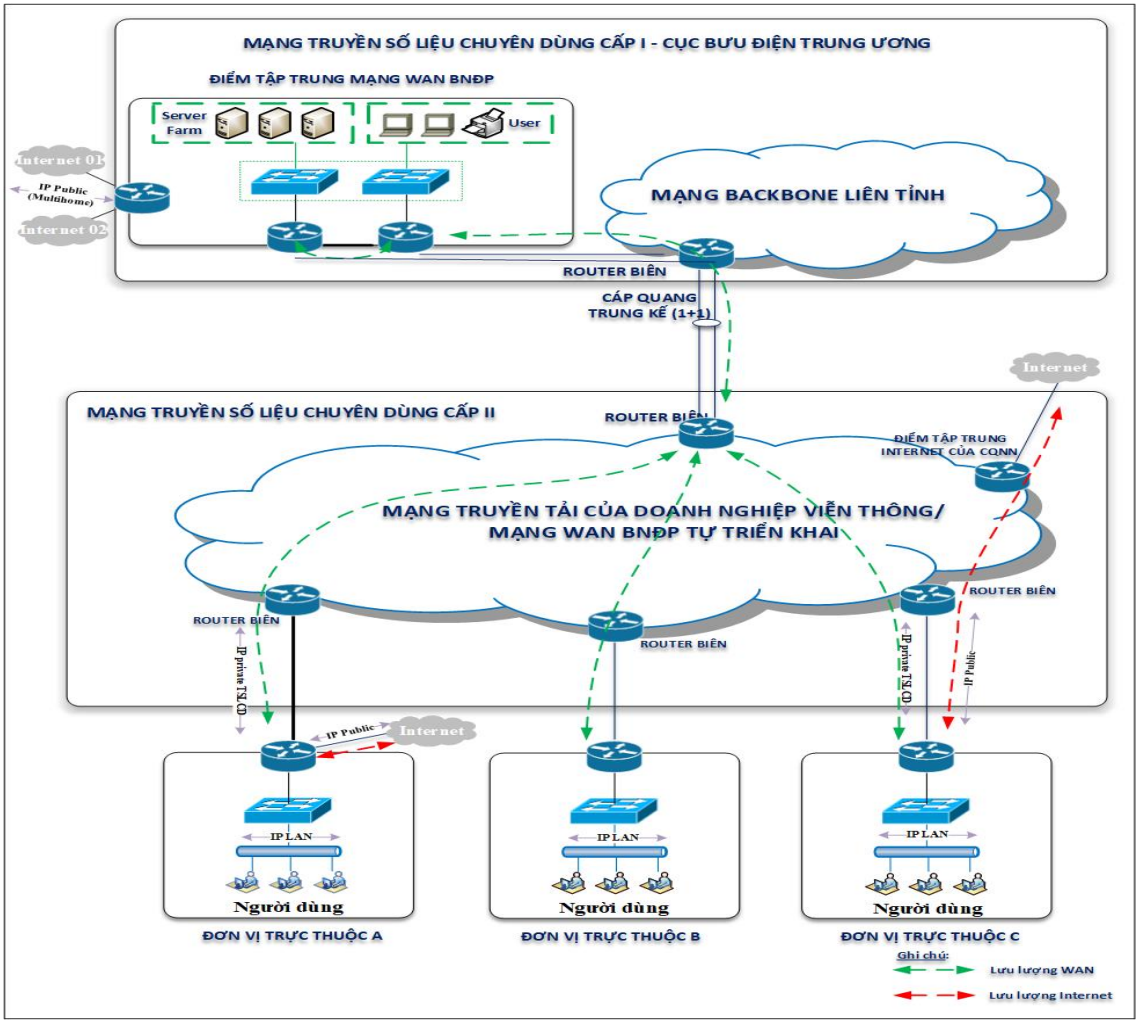


Hình 12. Tập trung lưu lượng về điểm quản lý tập trung của DNVT

Mô hình trên sử dụng trong trường hợp các địa phương không có đủ trang thiết bị để thiết lập điểm tập trung mạng WAN của địa phương. Với các yêu cầu cơ bản cần đáp ứng: Trên hạ tầng mạng TSLCD cấp II: tạo kết nối điểm – đa điểm từ các đơn vị trực thuộc về điểm tập trung mạng WAN của địa phương tại DNVT; Tại điểm tập trung mạng WAN của địa phương tại DNVT thực hiện chuyển tiếp lưu lượng từ các đơn vị trực thuộc đến các ứng dụng tại TTDL của địa phương; Đối với lưu lượng Internet: thực hiện rẽ nhánh trực tiếp tại cổng kết nối của các đơn vị trực thuộc.

V. MÔ HÌNH KẾT NỐI MẠNG LAN CỦA ĐƠN VỊ TRỰC THUỘC BNĐP VÀO MẠNG TSLCD

MÔ HÌNH SỐ 9: ***Kết nối mạng LAN của đơn vị trực thuộc BNĐP vào mạng TSLCD:***



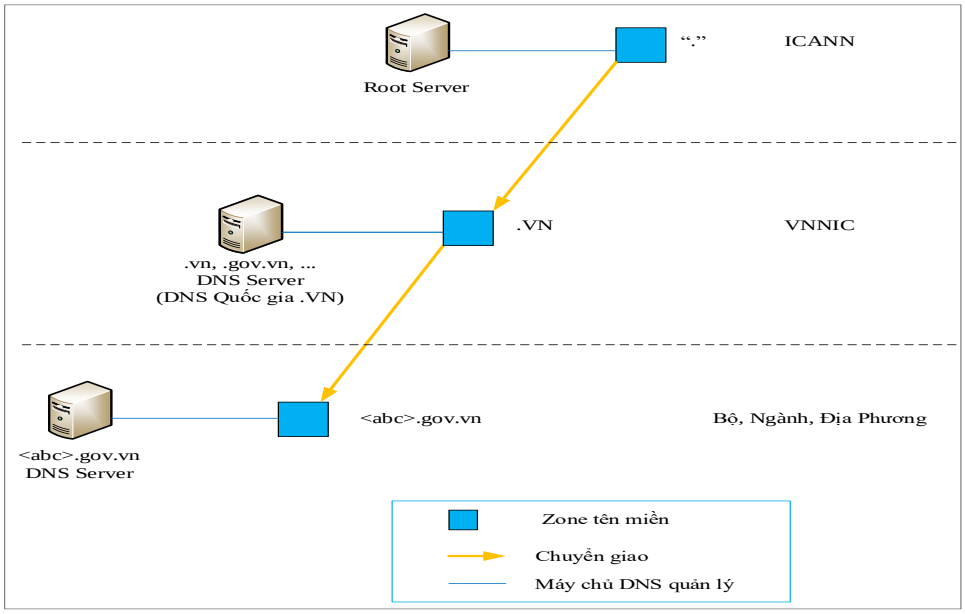
Hình 13. Kết nối mạng LAN của đơn vị trực thuộc BNĐP vào mạng TSLCD:

Mô hình trên sử dụng trong trường hợp các đơn vị không có HTTT (thường là các điểm quận/huyện, xã/phường). Với các yêu cầu cơ bản cần đáp ứng: Tại cổng kết nối của đơn vị: thực hiện tách riêng phân hệ kết nối Internet (IP Public do VNNIC quy hoạch) và phân hệ kết nối mạng TSLCD (IP private do Cục BĐTW quy hoạch). Cổng kết nối tại đơn vị cần đáp ứng các yêu cầu tại Phụ lục 1 Thông tư 12/2019/TT-BTTTT; Tại phân hệ LAN: 1 máy tính sử dụng đồng thời 2 kết nối Internet và TSLCD (IP do đơn vị sử dụng quy hoạch); Trên hạ tầng mạng của DNVT cung cấp kết nối Internet cho đơn vị: cần triển khai điểm tập trung Internet cho các CQNN để quản lý tập trung lưu lượng Internet của các CQNN tại địa phương.

VI. MÔ HÌNH HỆ THỐNG DNS

MÔ HÌNH SỐ 10: ***Hệ thống DNS quản lý tên miền <abc>.gov.vn của BNĐP***

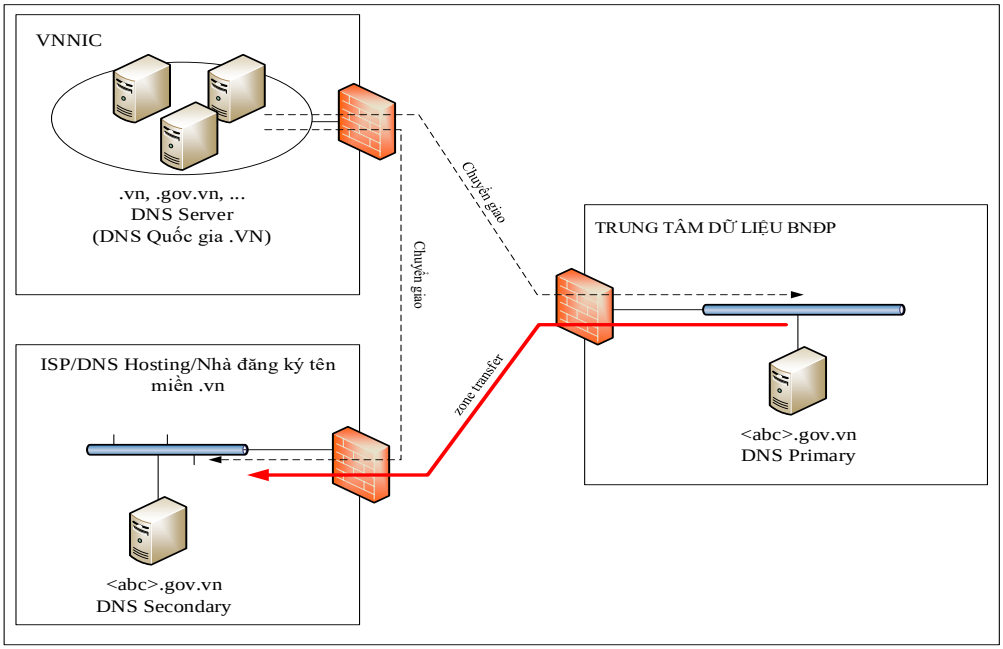
a) Phân cấp tên miền và máy chủ quản lý tên miền:



Hình 14. Hệ thống DNS quản lý tên miền <abc>.gov.vn của BNĐP

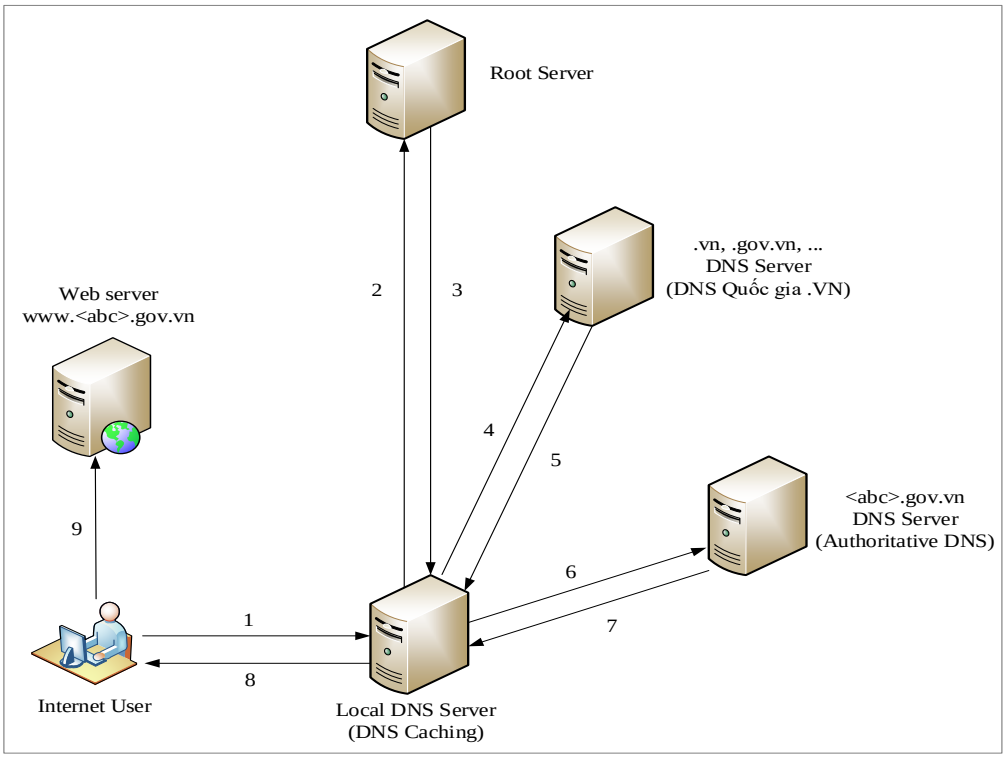
b) Mô hình khuyến nghị:

Khuyến nghị mô hình tổng thể về DNS quản lý tên miền <abc.gov.vn> theo hình vẽ như sau:



Hình 15. Mô hình tổng thể DNS quản lý tên miền <abc.gov.vn>

BNĐP sẽ có tối thiểu 02 máy chủ DNS để quản lý tên miền, máy chủ chính (Master) đặt tại TTDL, máy chủ phụ (secondary) đặt thuê tại ISP/Đơn vị cung cấp dịch vụ DNS Hosting. Hoạt động truy cập tên miền www.<abc>.gov.vn như sau:



Hình 16. Hoạt động truy cập tên miền www.<abc.gov.vn>

Chương trình trên máy người sử dụng (máy client) gửi yêu cầu tìm kiếm địa chỉ IP ứng với tên miền <abc>.gov.vn tới máy chủ quản lý tên miền cục bộ Local DNS Server (DNS Caching) thuộc mạng của nó. Máy chủ DNS Caching sẽ thực hiện quá trình truy vấn đệ quy tìm kiếm thông tin địa chỉ IP của tên miền và trả lời cho client để truy cập website www.<abc>.gov.vn.

c) Khai báo, quản lý tên miền ngược:

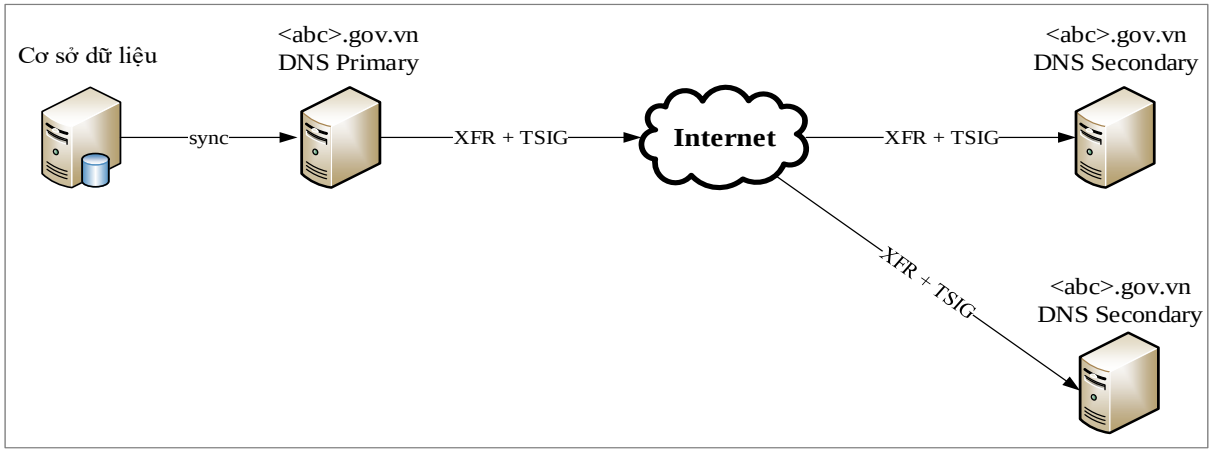
BNĐP được cấp phát địa chỉ IP từ VNNIC, khi đưa vào sử dụng cần khai báo tên miền ngược trên máy chủ DNS của mình, chi tiết tham khảo hướng dẫn tại địa chỉ sau: https://www.vnnic.vn/diachiip/hotro/thamkhao/.

d) Các yêu cầu cụ thể:

- Máy chủ DNS: tối thiểu 02 máy chủ DNS với địa chỉ IP khác nhau quản lý tên miền đặt ở 02 mạng độc lập khác nhau: tại TTDL của BNĐP và tại các đơn vị cung cấp dịch vụ như ISP, DNS Hosting hoặc nhà đăng ký tên miền .vn.

- 01 máy chủ DNS Primary (Master) quản lý dữ liệu chính, toàn bộ khai báo các bản ghi dịch vụ như <www, mail, edoc>.gov.vn được thực hiện trên máy chủ này.

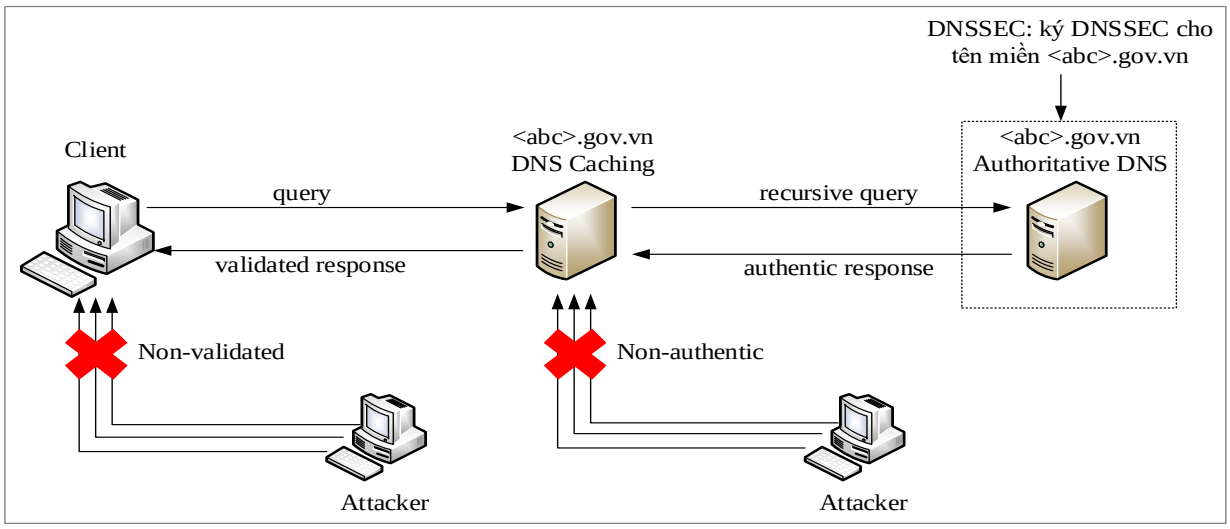
- 01- 02 máy chủ DNS Secondary (Slave): được đồng bộ với máy chủ master theo cơ chế zone transfer, sử dụng TSIG để đảm bảo an toàn (XFR + TSIG). Cơ chế TSIG (transaction signature) là quá trình sử dụng chung mã bảo mật chia sẻ giữa máy chủ DNS Primary và DNS Secondary để đảm bảo giao tiếp giữa các máy chủ DNS được xác thực.



Hình 17. Đồng bộ CSDL máy chủ DNS Primary và Secondary

- Ghi nhật ký hoạt động, phần mềm giám sát DNS, phân tích log DNS.

- Triển khai DNSSEC, đóng vai trò ký DNSSEC cho tên miền để đảm bảo an toàn tên miền. Các công việc thực hiện sẽ là tạo ra các khóa DNSSEC và ký lên zone tên miền <abc>.gov.vn. Gửi cập nhật đăng ký bản ghi chuyển giao (Deligation Signer - DS) lên hệ thống DNS quốc gia do VNNIC quản lý thông qua các nhà đăng ký tên miền .vn.



Hình 18. Triển khai DNSSec

Tham khảo hướng dẫn: https://vnnic.vn/sites/default/files/tailieu/VNNIC-TaiLieuHuongDanTrienKhaiDNSSEC-DHP-Final.pdf

MÔ HÌNH SỐ 11: ***Hệ thống máy chủ tên miền đệm (DNS Caching)***

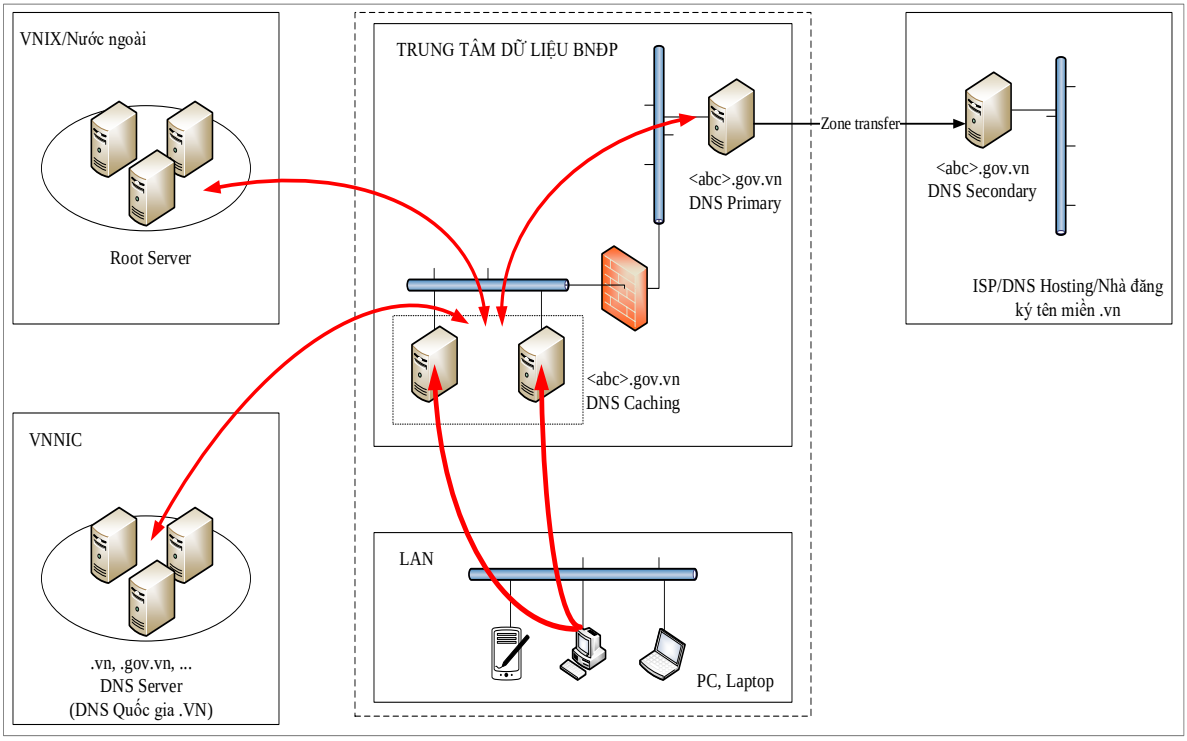
a) Sự cần thiết:

Phục vụ truy cập các dịch vụ Internet sử dụng tên miền, truy vấn tên miền .VN và tên miền quốc tế của các thiết bị (máy tính để bàn, máy tính xách tay, thiết bị di động…) trong mạng của các đơn vị (BNĐP).

Quản lý thiết lập chính sách truy cập tên miền tập trung, hệ thống DNS Caching có thể kết hợp với các hệ thống ATTT khác để bảo vệ chống mã độc, botnet….

b) Mô hình khuyến nghị:

Khuyến nghị mô hình tổng thể về DNS Caching cho BNĐP như sau:



Hình 19. Mô hình tổng thể DNS Caching cho BNĐP

- Các thiết bị (máy tính để bàn, máy tính xách tay, thiết bị di động, …) trong mạng của các đơn vị (BNĐP) trước khi kết nối sử dụng dịch vụ (nội bộ hoặc trên Internet) thì việc đầu tiên là phải kết nối, truy vấn tên miền để tìm kiếm thông tin địa chỉ IP của dịch vụ cần kết nối đến.

- Hệ thống DNS Caching sẽ đi tìm kiếm và trả lời các thông tin về tên miền cho các thiết bị trong mạng của các đơn vị đang yêu cầu như hình vẽ trên.

c) Các yêu cầu cụ thể:

- Máy chủ DNS: tối thiểu 02 máy chủ DNS Caching với địa chỉ IP khác nhau đặt tại trung tâm TTDL của BNĐP. 02 máy chủ hoạt động Active-Active, đảm bảo

khả năng dự phòng nóng, khi 01 máy chủ bị lỗi hoặc hỏng hóc vẫn còn 01 máy chủ còn lại hoạt động, đảm bảo không bị gián đoạn.

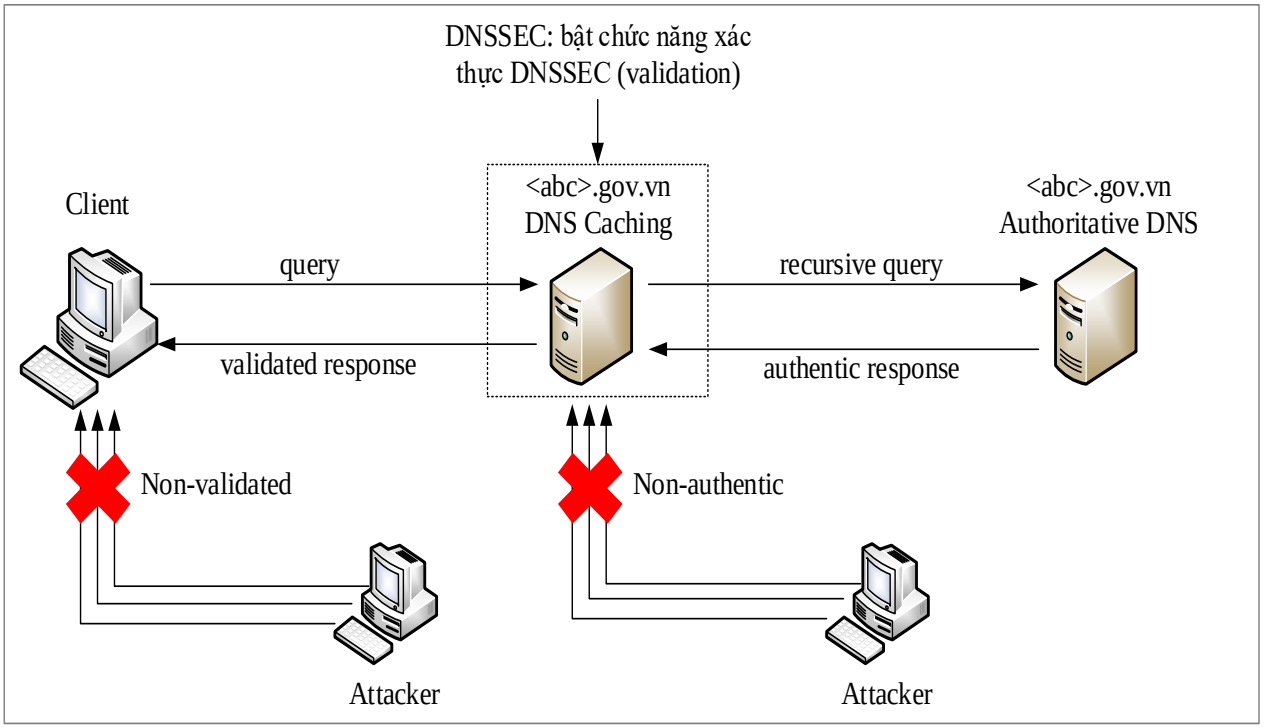
- Hệ thống có thể được thiết lập theo cơ chế đệ quy (recursive), tức là sẽ đi tìm kiếm câu trả lời từ các máy chủ DNS khác để trả lời cho máy trạm (client). Hoặc hệ thống có thể được thiết lập theo cơ chế caching forwarder (chuyển tiếp) để chuyển tiếp toàn bộ kết nối, truy vấn tên miền đến hệ thống DNS Caching khác.

- Hệ thống chỉ phục vụ các truy vấn tên miền từ các thiết bị (máy tính để bàn, máy tính xách tay, thiết bị di động, …) trong mạng của các đơn vị, không tiếp nhận phục vụ các truy vấn tên miền từ bên ngoài.

- Toàn bộ các thiết bị (máy tính để bàn, máy tính xách tay, thiết bị động, …) trong mạng của đơn vị phải được cấu hình để sử dụng hệ thống DNS Caching này.

- Ghi nhật ký hoạt động, phần mềm giám sát DNS, phân tích log DNS.

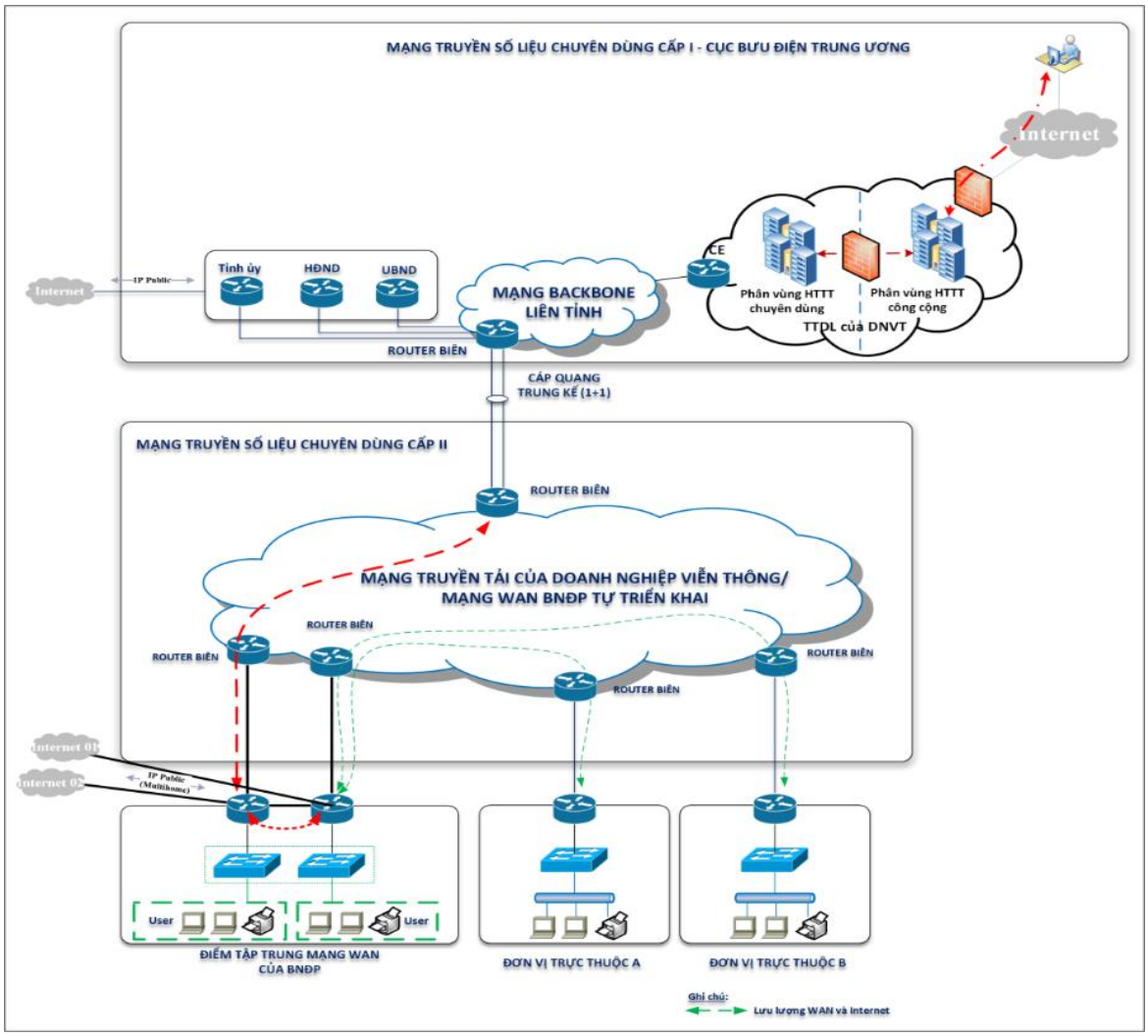
- Triển khai DNSSEC, đóng vai trò xác thực (validation) để đảm bảo an toàn tên miền: DNS Caching hỗ trợ DNSSEC có vai trò rất quan trọng, giúp bảo vệ người sử dụng, chống lại việc giả mạo các phản hồi truy vấn tên miền thông quan việc xác thực chữ ký số trên các bản ghi DNS có trong câu trả lời truy vấn tên miền.



Hình 20. Triển khai DNSSec

Tham khảo hướng dẫn: https://vnnic.vn/sites/default/files/tailieu/VNNIC-TaiLieuHuongDanTrienKhaiDNSSEC-ISP-Final.pdf

VII. Mô hình mục tiêu



Hình 21. Mô hình mục tiêu

Mô hình mục tiêu là mô hình chuẩn, đáp ứng các yêu cầu về ATTT, được sử dụng trong trường hợp các BNĐP có đầy đủ các điều kiện, trang thiết bị để triển khai.

Các yêu cầu cơ bản:

- Trên hạ tầng mạng TSLCD cấp II (trong trường hợp BNĐP và các đơn vị trực thuộc có kết nối mạng TSLCD cấp II) hoặc hạ tầng mạng WAN của BNĐP (trong trường hợp BNĐP tự triển khai hạ tầng mạng WAN riêng): tạo kết nối điểm – đa điểm từ các đơn vị trực thuộc về điểm tập trung mạng WAN của BNĐP.

- Tại điểm tập trung mạng WAN của BNĐP thực hiện:

+ Chuyển tiếp lưu lượng từ các đơn vị trực thuộc đến các ứng dụng tại HTTT chuyên dùng của BNĐP đặt tại TTDL của DNVT.

+ Chuyển tiếp lưu lượng kết nối Internet của các đơn vị trực thuộc qua kênh kết nối Internet tại điểm tập trung.