BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 50 /BTTTT-UDCNTT V/v hướng dẫn triển khai sử dụng dịch vụ kết nối từ xa vào Mạng truyền số liệu chuyên dùng	*Hà Nội, ngày 05 tháng 01 năm 2013*

Kính gửi:

- Đơn vị chuyên trách Công nghệ thông tin của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các các tỉnh, thành phố trực thuộc Trung ương;
- Tập đoàn Bưu chính Viễn thông Việt Nam.

Mạng truyền số liệu chuyên dùng của cơ quan Đảng, Nhà nước (sau đây gọi tắt là Mạng chuyên dùng) đã triển khai hoàn thiện giai đoạn I và II kết nối tới hơn ba nghìn điểm từ các cơ quan Trung ương đến địa phương tới cấp quận/huyện. Ngày 21/7/2008, Bộ Thông tin và Truyền thông đã có văn bản số 2336/BTTTT-UDCNTT hướng dẫn các đơn vị kết nối, sử dụng Mạng chuyên dùng. Để tiếp tục mở rộng năng lực phục vụ, nâng cao hiệu quả sử dụng Mạng chuyên dùng, Bộ Thông tin và Truyền thông ban hành hướng dẫn việc kết nối từ xa sử dụng phương thức mạng riêng ảo (VPN) vào Mạng chuyên dùng.

1. Tóm tắt về hiện trạng Mạng chuyên dùng

Mạng chuyên dùng được xây dựng với mục tiêu là cung cấp một hạ tầng mạng truyền dẫn tốc độ cao, công nghệ hiện đại, tiên tiến với mạng lõi sử dụng phương thức chuyển mạch nhãn đa giao thức (IP/MPLS), cho phép các mạng máy tính cục bộ (LAN) của các cơ quan Đảng, Nhà nước tại các cấp có thể kết nối được với nhau một cách an toàn, bảo mật và thông suốt, hoạt động liên tục, thông suốt 24 giờ/07 ngày (kể cả ngày nghỉ, ngày lễ).

Mạng chuyên dùng được đầu tư xây dựng theo hai giai đoạn. Kết thúc giai đoạn I đã có 220 đơn vị được kết nối vào Mạng chuyên dùng, bao gồm 92 cơ quan Đảng, Nhà nước tại Trung ương và cơ quan đại diện tại Đà Nẵng và Thành phố Hồ Chí Minh, 128 Uỷ ban nhân dân cấp tỉnh và Tỉnh ủy/Thành ủy của 64 tỉnh/thành (bao gồm cả Hà Tây cũ). Mạng chuyên dùng giai đoạn II thực hiện việc đầu tư xây dựng thêm đường trục kết nối Hà Nội, Đà Nẵng và Thành phố Hồ Chí Minh để hoạt động dự phòng cho đường truyền chính đã được xây dựng trong giai đoạn I. Triển khai mở rộng kết nối Mạng chuyên dùng đến tất cả các cơ quan quận/huyện, sở, ban, ngành thuộc tỉnh/thành trong phạm vi toàn bộ 63 tỉnh/thành trên cả nước.

Tính tới thời điểm hiện tại, Mạng chuyên dùng đã cơ bản hoàn thành kết nối cho 63 tỉnh/thành tới tận cấp quận/huyện với tổng số 3.517 điểm. Phương thức kết nối mạng cho các đơn vị sử dụng bao gồm hai phương thức cáp quang kết nối trực tiếp hoặc cáp đồng dựa trên công nghệ SHDSL đảm bảo cung cấp các dịch vụ tốt, chất lượng cao an toàn, an ninh, bảo mật và phục vụ tốt các Bộ, ngành, địa phương triển khai các giải pháp ứng dụng công nghệ thông tin trong việc chỉ đạo điều hành và hỗ trợ nghiệp vụ của mình.

Việc kết nối các hệ thống mạng nội bộ của các cơ quan vào Mạng chuyên dùng sẽ được thực hiện thống nhất đảm bảo tính liên thông giữa các cơ quan đơn vị, các cấp với nhau nhằm thúc đẩy, triển khai các phương thức trao đổi hồ sơ, văn bản điện tử và dữ liệu.

2. Nhu cầu sử dụng dịch vụ kết nối từ xa

Mạng chuyên dùng đã bước đầu đóng góp vào công tác triển khai ứng dụng công nghệ thông tin phục vụ chỉ đạo điều hành, các ứng dụng nghiệp vụ và chuyên ngành khác của các cơ quan nhà nước đảm bảo các mức độ bảo mật khác nhau. Khác với các ứng dụng triển khai trên mạng Internet có thể được mọi người truy cập sử dụng với đường truyền Internet bất kỳ, các ứng dụng triển khai trên Mạng chuyên dùng cần giới hạn phạm vi kết nối, sử dụng để đảm bảo an toàn, an ninh và tính chất dùng riêng của mình. Tuy nhiên, trong quá trình khai thác Mạng chuyên dùng có thể xuất hiện những tình huống sau:

- Đơn vị sử dụng Mạng chuyên dùng khi mở rộng quy mô tổ chức hoặc thay đổi địa điểm làm việc nhưng chưa hoặc không được triển khai kết nối mở rộng đường truyền Mạng chuyên dùng. Khi đó, sẽ xuất hiện cụm máy tính biệt lập của đơn vị không thể kết nối vào trụ sở chính hoặc tới cơ quan khác;

- Cá nhân sử dụng Mạng chuyên dùng đi công tác ngoài địa điểm làm việc của mình khi có nhu cầu sẽ có thể gặp khó khăn khi kết nối vào Mạng chuyên dùng hoặc mạng nội bộ đã kết nối Mạng chuyên dùng để sử dụng các dịch vụ được triển khai nội bộ.

Để khắc phục các vướng mắc trên, cần có biện pháp thiết lập một đường truyền số liệu riêng ảo với phạm vi kết nối phù hợp để vừa đáp ứng nhu cầu của các đơn vị sử dụng Mạng chuyên dùng trên nền hạ tầng Mạng chuyên dùng, vừa giảm tối đa số lượng các ứng dụng, hệ thống thông tin sử dụng trong hoạt động của cơ quan nhà nước đang triển khai trên Internet có nguy cơ rủi ro cao về an toàn, an ninh.

3. Hướng dẫn chung

3.1. Mục tiêu của kết nối từ xa vào Mạng chuyên dùng nhằm thiết lập một kết nối từ mạng Intetnet vào Mạng chuyên dùng hoặc mạng nội bộ của các

cơ quan, đơn vị có kết nối Mạng chuyên dùng, đảm bảo tính an toàn, an ninh, bảo mật.

3.2. Tuỳ thuộc vào thực tế, đơn vị sử dụng Mạng chuyên dùng có thể lựa chọn các phương án kết nối phù hợp với mục đích và nhu cầu sử dụng.

3.3. Việc quản lý, đảm bảo an toàn, an ninh khi triển khai kết nối từ xa vào Mạng chuyên dùng được thực hiện theo Thông tư số 23/2011/TT-BTTTT ngày 11/8/2011 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về việc quản lý, vận hành, sử dụng và đảm bảo an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước, văn bản số 3240/BTTTT-UDCNTT ngày 26/11/2012 của Bộ Thông tin và Truyền thông về hướng dẫn việc đảm bảo an toàn mạng và thông tin trên Mạng truyền số liệu chuyên dùng.

3.4. Triển khai các biện pháp an toàn bảo mật bổ sung nếu cần thiết để truyền tải thông tin đòi hỏi độ bảo mật cao (sử dụng dịch vụ chứng thực và chữ ký số theo Thông tư 05/2010/TT-BNV ngày 01/7/2010 của Bộ trưởng Bộ Nội vụ hướng dẫn về cung cấp, quản lý sử dụng dịch vụ chứng thực chữ ký số chuyên dùng phục vụ các cơ quan thuộc hệ thống chính trị).

4. Phương án kết nối từ xa vào Mạng chuyên dùng

4.1. Phương án 1: Kết nối từ xa vào Mạng chuyên dùng từ Internet

a) Trường hợp sử dụng phương án

Phương án này được sử dụng đối với những trường hợp sau:

- Cá nhân sử dụng Mạng chuyên dùng khi đi công tác muốn sử dụng các dịch vụ được triển khai trong Mạng chuyên dùng từ mạng Internet;

- Đơn vị sử dụng Mạng chuyên dùng thay đổi địa điểm hoặc phát sinh một đơn vị trực thuộc mới muốn kết nối vào Mạng chuyên dùng tuy nhiên chưa triển khai được đường truyền dẫn riêng đến Mạng chuyên dùng.

b) Giải pháp thực hiện

- Hiện tại trên Mạng chuyên dùng đã có ba cổng kết nối ra Internet và được trang bị các thiết bị chấp nhận kết nối mạng riêng ảo (thiết bị ASA 5550). Thiết bị này có địa chỉ IP tĩnh của mạng Internet do Tập đoàn Bưu chính Viễn thông (Bưu điện Trung ương) hiện quản lý và vận hành.

- Cá nhân sử dụng/đơn vị sử dụng Mạng chuyên dùng kết nối từ xa cần có đường truyền Internet (có thể sử dụng đường truyền của các doanh nghiệp viễn thông).

- Thực hiện kết nối mạng riêng ảo (VPN) vào thiết bị chấp nhận kết nối mạng riêng ảo do Tập đoàn Bưu chính Viễn thông quản lý, vận hành.

- Sau khi xác thực thành công, thiết bị chấp nhận kết nối mạng riêng ảo sẽ tự động cấp địa chỉ IP và tạo một kênh kết nối ảo được bảo mật bằng công nghệ IPSec, định tuyến lưu lượng khách hàng đến Mạng chuyên dùng. Khi đó, mọi thông tin truyền từ máy tính ngoài mạng Internet đến Mạng chuyên dùng sẽ được lưu thông trong trong kết nối ảo được bảo vệ này.

- Đơn vị sử dụng Mạng chuyên dùng cần đăng ký dịch vụ kết nối từ xa nêu trên với Điểm đăng ký dịch vụ hoặc Bưu điện Trung ương (trong trường hợp Bưu điện Trung ương trực tiếp ký kết hợp đồng với đơn vị) để được cấp tài khoản truy cập thiết bị để tạo mạng riêng ảo.

c) Đánh giá phương án

- Phương án này không làm phát sinh các trang thiết bị mới dùng để thực hiện kết nối; cách thức thực hiện đơn giản, chỉ cần đăng ký với Điểm đăng ký dịch vụ để sử dụng dịch vụ.

- Phương án có giới hạn là địa chỉ IP được cấp nằm trong một vùng được quản lý chung của Mạng chuyên dùng mà không phải địa chỉ IP mạng nội bộ của đơn vị sử dụng Mạng chuyên dùng; tùy thuộc vào chính sách triển khai, bảo mật của đơn vị sử dụng Mạng chuyên dùng, có thể không sử dụng được các dịch vụ, hệ thống thông tin nội bộ.

4.2. Phương án 2: Kết nối từ xa vào mạng nội bộ của các đơn vị sử dụng Mạng chuyên dùng từ Internet.

a) Trường hợp sử dụng phương án

Phương án này được sử dụng đối với những trường hợp sau:

- Cá nhân sử dụng Mạng chuyên dùng đi công tác hoặc không có mặt tại trụ sở làm việc muốn sử dụng các dịch vụ được triển khai trong mạng nội bộ của cơ quan từ mạng Internet;

- Đơn vị sử dụng Mạng chuyên dùng có thêm trụ sở làm việc mới. Trụ sở mới này chưa có đường truyền kết nối Mạng chuyên dùng mà chỉ có đường kết nối Internet. Phương án 2 thực hiện kết nối liên thông các mạng LAN giữa hai trụ sở;

- Các trường hợp khác cần một kết nối mạng riêng ảo từ Internet đến mạng nội bộ và được cấp địa chỉ IP của mạng nội bộ.

b) Giải pháp thực hiện

- Đơn vị sử dụng Mạng chuyên dùng có nhu cầu triển khai đầu tư trang bị máy chủ đóng vai trò chấp nhận kết nối mạng riêng ảo tại đơn vị của mình trong Mạng chuyên dùng. Thiết bị được cấu hình dịch vụ IPSec Remote Access VPN.

- Đăng ký sử dụng dịch vụ với Điểm đăng ký dịch vụ để được cấp một địa chỉ IP tĩnh của mạng Internet đồng thời được cấp một kênh bảo vệ từ các điểm truy cập Internet của Mạng chuyên dùng đến máy chủ của đơn vị sử dụng Mạng chuyên dùng.

- Đơn vị sử dụng Mạng chuyên dùng tự cấu hình, quản lý và cấp tài khoản cho cán bộ của mình. Số lượng tài khoản kết nối không bị giới hạn.

- Cá nhân sử dụng/đơn vị sử dụng Mạng chuyên dùng kết nối từ xa cần có đường truyền Internet (có thể sử dụng đường truyền của các doanh nghiệp viễn thông).

- Thiết bị của cá nhân sử dụng/đơn vị sử dụng Mạng chuyên dùng từ mạng Internet muốn kết nối từ xa sẽ thực hiện kết nối mạng riêng ảo tới địa chỉ IP tĩnh được cấp. Thiết bị đó sẽ được cấp phát địa chỉ mạng nội bộ của đơn vị sử dụng Mạng chuyên dùng. Một mạng riêng ảo được thiết lập giữa thiết bị ngoài Internet đến mạng nội bộ của đơn vị và mọi thông tin lưu thông sẽ được bảo vệ bởi mạng riêng ảo này.

c) Đánh giá phương án

- Phương án này đòi hỏi đơn vị sử dụng Mạng chuyên dùng phải trang bị thiết bị máy chủ Remote Access VPN.

- Đơn vị sử dụng Mạng chuyên dùng chỉ cần đăng ký một lần với Điểm đăng ký dịch vụ và toàn quyền kiểm soát cấp tài khoản kết nối mạng VPN vào mạng nội bộ; khi thiết lập kết nối, máy kết nối được cấp địa chỉ IP của mạng nội bộ, do đó có thể sử dụng tất cả các dịch vụ được triển khai trong mạng nội bộ.

5. Tổ chức thực hiện

5.1. Các đơn vị sử dụng Mạng chuyên dùng có trách nhiệm:

a) Lựa chọn phương án phù hợp với nhu cầu về triển khai các dịch vụ truy cập từ xa vào Mạng chuyên dùng;

b) Liên hệ với Điểm đăng ký dịch vụ Mạng chuyên dùng (được hướng dẫn theo văn bản số 944/BTTTT-UDCNTT ngày 19/4/2012 của Bộ Thông tin và Truyền thông) hoặc Bưu điện Trung ương để được trợ giúp về mặt kỹ thuật, cách thức triển khai và cung cấp dịch vụ;

c) Cấp phát và quản lý tài khoản và giám sát các kết nối từ xa vào Mạng chuyên dùng, mạng nội bộ của đơn vị, triển khai các giải pháp, chính sách đảm bảo an toàn, an ninh, bảo mật đối với các kết nối từ xa vào Mạng chuyên dùng.

5.2. Đơn vị chuyên trách công nghệ thông tin của các Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, các Sở Thông tin và Truyền thông các tỉnh/thành phố trực thuộc Trung ương có trách nhiệm:

a) Phối hợp với Viễn thông tỉnh, Bưu điện Trung ương xây dựng các phương án kỹ thuật phù hợp, áp dụng cho Bộ, ngành, địa phương thuộc phạm vi quản lý của mình;

b) Chủ trì tổ chức hướng dẫn, lựa chọn phương án triển khai kết nối từ xa, phương án khai thác đường truyền từ xa cho các đơn vị sử dụng Mạng chuyên dùng tại Bộ, ngành, địa phương mình;

c) Giám sát triển khai các phương án kết nối của các đơn vị sử dụng Mạng chuyên dùng đồng thời phối hợp xử lý các trường hợp sự cố phát sinh liên quan đến dịch vụ kết nối từ xa vào Mạng chuyên dùng.

5.3. Tập đoàn Bưu chính Viễn thông (Bưu điện Trung ương) có trách nhiệm:

a) Xây dựng các phương án kỹ thuật chi tiết của các phương án áp dụng cho các Bộ, ngành, địa phương;

b) Tổ chức hỗ trợ triển khai, tiếp nhận yêu cầu và cung cấp dịch vụ cho các đơn vị có nhu cầu;

c) Giám sát các kết nối từ xa vào Mạng chuyên dùng, đảm bảo điều kiện an toàn, an ninh, bảo mật tránh các mối nguy hiểm từ việc kết nối từ Internet vào Mạng chuyên dùng phát sinh khi triển khai giải pháp kết nối từ xa bằng công nghệ VPN.

Trong quá trình thực hiện, nếu có gì vướng mắc, đề nghị Quý Cơ quan báo cáo về Bộ Thông tin và Truyền thông (Cục Ứng dụng công nghệ thông tin) để có hướng dẫn giải quyết./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Minh Hồng (để b/c);
- Bưu điện Trung ương;
- Lưu: VT, UDCNTT.

TL. BỘ TRƯỞNG
CỤC TRƯỞNG CỤC ỨNG DỤNG CÔNG NGHỆ THÔNG TIN

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

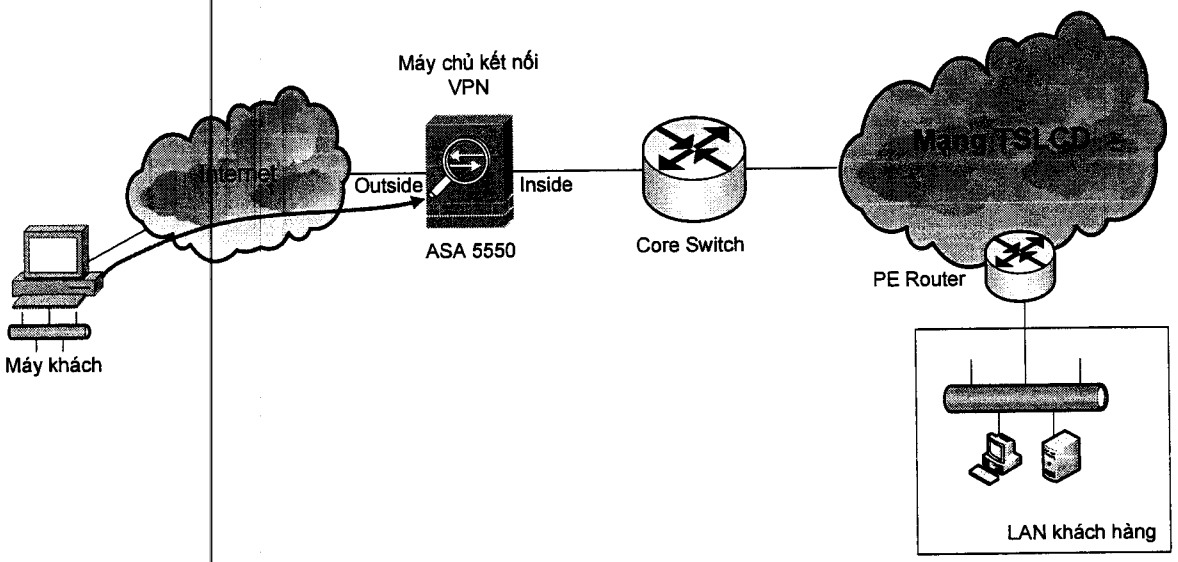
Nguyễn Thành Phúc

Phụ lục

MÔ HÌNH KẾT TRUY CẬP TỪ XA VÀO MẠNG CHUYÊN DÙNG BẰNG CÔNG NGHỆ MẠNG RIÊNG ẢO

(Ban hành kèm theo công văn số 50./BTTTT-UDCNTT ngày 05/11/2013)

1. Phương án 1: Mô hình kết nối từ xa vào Mạng chuyên dùng từ Internet



2. Phương án 2: Mô hình kết nối từ xa vào Mạng nội bộ của các cơ quan đơn vị từ Internet