UỶ BAN NHÂN DÂN **TỈNH SƠN LA**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1249/QĐ-UBND	*Sơn La, ngày 24 tháng 6 năm 2022*

QUYẾT ĐỊNH

Về việc phê duyệt Đề cương và dự toán chi tiết : Mua sắm thiết bị tường lửa phục vụ nâng cấp Trung tâm tích hợp dữ liệu thuộc dự toán: "Mua sắm, nâng cấp hệ thống máy chủ và thiết bị chuyên dùng"

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH

Căn cứ Luật Ngân sách nhà nước năm 2015;

Căn cứ Luật Công nghệ thông tin năm 2006;

Căn cứ Nghị định số 163/2016/NĐ-CP ngày 21/12/2016 của Chính phủ quy định chi tiết và hướng dẫn thi hành Luật Ngân sách nhà nước;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 73/2019/NĐ-CP ngày 05/9/2019 của Chính phủ quy định quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước;

Căn cứ Thông tư số 03/2020/TT-BTTTT ngày 24/02/2020 của Bộ Thông tin và Truyền thông về việc Quy định về lập đề cương và dự toán chi tiết đối với hoạt động ứng dụng công nghệ thông tin sử dụng kinh phí chi thường xuyên thuộc nguồn vốn ngân sách nhà nước;

Căn cứ Thông tư số 04/2020/TT-BTTTT ngày 24/02/2020 của Bộ Thông tin và Truyền thông về việc Quy định về lập và quản lý chi phí dự án đầu tư ứng dụng công nghệ thông tin;

Căn cứ Quyết định số 2378/QĐ-BTTTT ngày 30/12/2016 của Bộ Thông tin và Truyền thông về việc công bố định mức chi phí quản lý dự án, chi phí tư vấn đầu tư ứng dụng công nghệ thông tin sử dụng ngân sách nhà nước; Quyết định số 1688/QĐ-BTTTT ngày 11/10/2019 của Bộ Thông tin và Truyền thông về việc sửa đổi, bổ sung Quyết định số 2378/QĐ-BTTTT ngày 30/12/2016 của Bộ Trưởng Bộ Thông tin và Truyền thông công bố định mức chi phí quản lý dự án, chi phí tư vấn đầu tư ứng dụng công nghệ thông tin sử dụng ngân sách nhà nước;

Căn cứ Quyết định số 1184/QĐ-UBND ngày 11/6/2020 của UBND tỉnh Sơn La về việc ban hành quy định tiêu chuẩn, định mức sử dụng máy móc, thiết bị chuyên dùng của các cơ quan, tổ chức, đơn vị trên địa bàn tỉnh Sơn La;

Theo đề nghị của Sở Thông tin và Truyền thông tại Tờ trình số 63/TTr-STTTT ngày 23/6/2022 và Báo cáo thẩm định số 182/BCTĐ-STTTT ngày 23/5/2022.

QUYẾT ĐỊNH:

Điều 1. Phê duyệt đề cương và dự toán chi tiết: Mua sắm thiết bị tường lửa phục vụ nâng cấp Trung tâm tích hợp dữ liệu thuộc dự toán "mua sắm nâng cấp hệ thống máy chủ và thiết bị chuyên dùng" với các nội dung chủ yếu sau:

1. Đơn vị sử dụng ngân sách: Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông.

2. Tổ chức, đơn vị lập đề cương và dự toán chi tiết: Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông.

3. Mục tiêu, quy mô: Mua sắm thiết bị tường lửa của Trung tâm tích hợp dữ liệu tỉnh Sơn La để đáp ứng nhu cầu về vận hành, khai khác và bảo vệ ngăn chặn các cuộc tấn công từ bên ngoài có hiệu quả hơn.

4. Giải pháp kỹ thuật, công nghệ và các nội dung ứng dụng công nghệ thông tin chủ yếu

Thiết bị đầu tư và Phương án lắp đặt, cấu hình Hệ thống được đề xuất tuân thủ theo các tiêu chuẩn, quy chuẩn kỹ thuật, cụ thể như sau:

- Sự phù hợp của việc lựa chọn phương án công nghệ, kỹ thuật, thiết bị: Quy mô đầu tư bổ sung các thiết bị công nghệ thông tin của dự án gồm: 02 thiết bị tường lửa công nghệ đề xuất là giải pháp tường lửa Next-generation Firewall với các tính năng như: App-ID, IPS, antivirus, anti-spyware, DNS Sinkhole... Các thiết bị được lựa chọn trên cơ sở phân tích, hệ thống công nghệ mới tiên tiến, hiện đại và đang được sử dụng phổ biến trên thị trường. Phân tích các nhu cầu, tính năng của thiết bị để đưa ra phương án lựa chọn tối ưu, đảm bảo phù hợp với dự án, tương thích với các thiết bị hiện có tại Trung tâm tích hợp dữ liệu tỉnh Sơn La.

- Sự phù hợp của thiết kế với các tiêu chuẩn, quy chuẩn kỹ thuật và các yêu cầu cơ bản về chức năng, tính năng kỹ thuật: Tiêu chuẩn, quy chuẩn các hạng mục thiết bị đầu tư của dự án được thực hiện theo Thông tư 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ Thông tin và Truyền thông về việc Ban hành danh mục tiêu chuẩn về ứng dụng công nghệ thông tin trong cơ quan nhà nước.

Mô hình thiết kế phù hợp với nội dung, quy mô và danh mục thiết bị nâng cấp được đề xuất.

Giải pháp thiết kế mô hình bao gồm: "Modul Internet, Modul mạng Lan, Model Máy chủ" và phân tích các chức năng đảm bảo vai trò của thiết bị bảo mật cho từng Modul. Đưa ra cách thức vận hành, sơ đồ dự kiến lắp đặt trên Rack.

5. Dự toán chi tiết

Tổng cộng: 3.173.000.000 VNĐ (Bằng chữ: *Ba tỷ một trăm bảy mươi ba triệu đồng*).

Trong đó:

- Chi phí mua sắm thiết bị công nghệ thông tin: 3.151.660.000 đồng.
- Chi phí tư vấn: 13.340.000 đồng.
- Chi phí khác (thẩm định giá): 8.000.000 đồng.

6. Nguồn vốn: Quyết định số 2999/QĐ-UBND ngày 08/12/2021 của UBND tỉnh Sơn La về việc giao dự toán thu, chi ngân sách năm 2022.

7. Địa điểm thực hiện: Trung tâm tích hợp dữ liệu thuộc Trung tâm Công nghệ thông tin và Truyền thông tỉnh Sơn La.

8. Thời gian thực hiện: Năm 2022.

9. Đơn vị thực hiện: Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông.

10. Tên gói mua sắm: Mua sắm thiết bị tường lửa phục vụ nâng cấp Trung tâm tích hợp dữ liệu.

11. Đề cương và dự toán chi tiết: *(Có Đề cương, dự toán chi tiết gửi kèm theo).*

Điều 2. Tổ chức thực hiện

1. Sở Thông tin và Truyền thông chịu mọi trách nhiệm trước pháp luật, trước Chủ tịch UBND tỉnh về tính chuẩn xác, tính hợp pháp của các thông tin, số liệu về nội dung đề cương, dự toán thẩm định, trình duyệt, Có trách nhiệm hướng dẫn đơn vị tổ chức thực hiện quy trình mua sắm đảm bảo đúng theo pháp luật quy định hiện hành.

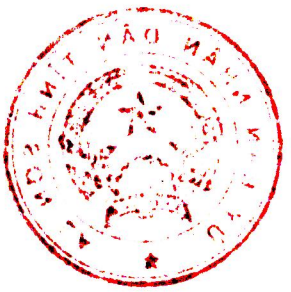
2. Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông chịu trách nhiệm toàn diện về các kết luận thanh tra, kiểm tra, kiểm toán và các cơ pháp luật nhà nước. Chủ động tự kiểm tra để kịp thời phát hiện những nội dung không đảm bảo theo quy định và sai phạm (nếu có) báo cáo UBND tỉnh kịp thời.

Điều 3. Chánh Văn phòng UBND tỉnh, Giám đốc Sở Tài chính, Giám đốc Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông và Thủ trưởng các cơ quan, đơn vị có liên quan chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Chủ tịch UBND tỉnh;
- Các PCT UBND tỉnh;
- Như Điều 3;
- Lưu: VT, KGVX.

KT.CHỦ TỊCH
PHÓ CHỦ TỊCH

Đặng Ngọc Hậu



SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH SƠN LA
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

CÔNG TY TNHH TƯ VẤN CÔNG NGHỆ HIẾU MINH
ĐÃ THẨM TRA
Số: 01.22/BC-HM
Ngày 23 tháng 05 năm 2022
Người thẩm tra:

ĐỀ CƯƠNG VÀ DỰ TOÁN

Mua sắm, nâng cấp thiết bị chuyên dùng thuộc dự toán: "Mua sắm, nâng cấp, hệ thống máy chủ và thiết bị chuyên dùng"

ĐẠI DIỆN ĐƠN VỊ THẨM TRA	ĐẠI DIỆN ĐƠN VỊ LẬP
GIÁM ĐỐC	PHÓ GIÁM ĐỐC
Đỗ Thị Thu Hà	Trần Đức Quang

Sơn La, tháng 3 năm 2022

SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH SƠN LA
TRUNG TÂM CNTTTT

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Sơn La, ngày 23 tháng 3 năm 2022

ĐỀ CƯƠNG VÀ DỰ TOÁN CHI TIẾT
Mua sắm, nâng cấp thiết bị chuyên dùng thuộc Dự toán "Mua sắm, nâng cấp, hệ thống máy chủ và thiết bị chuyên dùng"
Phần I
THÔNG TIN CHUNG

I. CƠ SỞ XÂY DỰNG

- Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/6/2006;

- Luật Viễn thông số 41/2009/QH12 ngày 23/11/2009;

- Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015;

- Nghị định số 73/2019/NĐ-CP ngày 05/9/2019 của Chính phủ v/v Quy định quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước;

- Thông tư 03/2020/TT-BTTTT ngày 24/02/2020 của Bộ Thông tin và Truyền thông v/v Quy định về lập đề cương và dự toán chi tiết đối với hoạt động ứng dụng công nghệ thông tin sử dụng kinh phí chi thường xuyên thuộc nguồn vốn ngân sách nhà nước;

- Thông tư số 58/2016/TT-BTC ngày 29/3/2016 của Bộ Tài chính về Quy định chi tiết việc sử dụng nguồn vốn nhà nước để mua sắm nhằm duy trì hoạt động thường xuyên của cơ quan nhà nước, đơn vị thuộc lực lượng vũ trang nhân dân, đơn vị sự nghiệp công lập tổ chức chính trị, tổ chức chính trị xã hội tổ chức chính trị xã hội – nghề nghiệp, tổ chức xã hội, tổ chức xã hội – nghề nghiệp;

- Tiêu chuẩn quốc gia TCVN 9250 : 2012 Trung tâm dữ liệu - yêu cầu về hạ tầng kỹ thuật viễn thông.

- Căn cứ Quyết định số 1162/QĐ-UBND ngày 10/5/2017 của UBND tỉnh Sơn La về việc phê duyệt quy hoạch hạ tầng kỹ thuật viễn thông thụ động tỉnh Sơn La đến năm 2020, định hướng đến năm 2025;

- Kế hoạch số 212/KH-UBND ngày 03/11/2020 v/v Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, phát triển Chính quyền số và bảo đảm an toàn thông tin mạng tỉnh Sơn La giai đoạn 2021-2025;

II. THÔNG TIN CHUNG

1. Tên dự án: Mua sắm, nâng cấp thiết bị chuyên dùng.

2. Thuộc dự toán: Mua sắm, nâng cấp, hệ thống máy chủ và thiết bị chuyên dùng.

3. Đơn vị sử dụng ngân sách: Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông tỉnh Sơn La.

4. Địa điểm thực hiện: Trung tâm tích hợp dữ liệu tỉnh Sơn La.

5. Thời gian thực hiện: năm 2022.

6. Tổ chức, đơn vị lập đề cương và dự toán chi tiết: Trung tâm Công nghệ thông tin và Truyền thông.

7. Nguồn vốn: Quyết định số 2999/QĐ-UBND ngày 08/12/2021 của UBND tỉnh Sơn La về việc giao dự toán thu, chi ngân sách năm 2022. Sở Thông tin và Truyền thông đã phân bổ tại Quyết định số 302/QĐ-STTTT ngày 30/12/2021.

III. DỰ KIẾN HIỆU QUẢ ĐẠT ĐƯỢC

Việc đầu tư mua sắm thiết bị công nghệ thông tin nhằm phục vụ nâng cấp thiết bị chuyên dùng là hệ thống tường lửa của trung tâm tích hợp dữ liệu tỉnh Sơn La để đáp ứng nhu cầu về vận hành, khai khác và bảo vệ ngăn chặn các cuộc tấn công từ bên ngoài có hiệu quả hơn, dự kiến sẽ mang lại những hiệu quả cụ thể như sau:

+ Cải thiện tốc độ, khả năng truy cập, tải dữ liệu của các máy chủ dịch vụ công của trung tâm tích hợp dữ liệu tỉnh Sơn La.

+ Hệ thống tường lửa (Firewall chạy chế độ HA dự phòng) nhằm tăng hiệu quả kiểm soát, ngăn chặn truy cập trái phép và phòng chống tấn công từ bên ngoài vào hệ thống trung tâm dữ liệu tích hợp trọng yếu của tỉnh.

+ Các thiết bị tưởng lửa phần cứng sẽ hỗ trợ, đảm bảo về hiệu năng, hiệu quả vận hành, tính an toàn và bảo mật thông tin, tạo môi trường để hình thành nên hệ thống có tính đồng bộ từ các cấp của cơ quan quản lý nhà nước, đảm bảo khả năng mở rộng cho các hệ thống dịch vụ công sẽ được xây dựng trong tương lai.

+ Cùng với các hệ thống thiết bị đang có, việc rà soát, bổ sung hệ thống tường lửa mới kết hợp với các hệ thống hiện có giúp tiết kiệm tối đa chi phí ngân sách nhà nước mà vẫn đảm bảo được nhu cầu sử dụng thực tiễn.

IV. ĐỀ XUẤT, KIẾN NGHỊ

Sau khi Đề cương và dự toán dự án được cấp có thẩm quyền phê duyệt Chủ đầu tư cần triển khai thực hiện một số nhiệm vụ sau:

1. Bố trí đủ kinh phí để thực hiện các nội dung của dự án.

2. Bố trí đủ nhân lực có năng lực, kinh nghiệm về quản lý dự án đầu tư, hiểu biết về lĩnh vực CNTT để thực hiện dự án.

3. Tổ chức triển khai thực hiện các bước tiếp theo của dự án theo quy định của pháp luật: Tổ chức lựa chọn nhà thầu thực hiện; kiểm tra, giám sát quá trình thực hiện dự án; nghiệm thu, bàn giao đưa vào hoạt động; hoàn tất các thủ tục theo quy định...

4. Phối hợp với các cơ quan chức năng đảm bảo lắp đặt đúng tiêu chuẩn và an toàn an ninh thông tin cho hệ thống thư điện tử nói riêng và trung tâm tích hợp dữ liệu nói chung.

Phần II
NỘI DUNG ĐỀ CƯƠNG

1. Sự cần thiết phải đầu tư

Hiện trạng hệ thống:

Thực trạng bảo mật tại Trung tâm tích hợp dữ liệu tỉnh rất thiếu và không đảm bảo đủ các tiêu chuẩn về trang thiết bị cần thiết để bảo vệ các hệ thống dùng chung, dịch vụ công của Tỉnh. Các giải pháp đang được trang bị như sau:

- Thiết bị tường lửa Cisco ASA với bản quyền (license) chỉ 100 Mbps đã được trang bị từ rất lâu, bản quyền không được hỗ trợ cho thiết bị này nên không có các tính năng bảo mật cần thiết như phát hiện và ngăn chặn tấn công.

- Một số thiết bị bộ định tuyến (Router) của nhà mạng như Virgo với các tính năng tường lửa rất cơ bản chỉ đảm bảo cho dịch vụ có thể hoạt động mà không có các năng lực bảo vệ cần thiết cho hệ thống ứng dụng, máy chủ khỏi các mối đe dọa từ mạng (internet).

- Toàn bộ lưu lượng truy cập của các máy chủ sẽ đi qua thiết bị Virgo 2912 không có các tính năng cân bằng tải, hay tính năng dự phòng song song, nên không có tính sẵn sàng cao khi có sự cố phải dừng hệ thống, vì thiết bị này chỉ làm nhiệm vụ như một bộ định tuyến (Router).

- Các truy cập từ bên ngoài vào dịch vụ một cửa được thông qua một thiết bị điều hướng (Proxy) mã nguồn mở với các tính năng bảo mật rất hạn chế.

- Những năm vừa qua tỉnh ký hợp đồng an ninh mạng với tập đoàn Viettel nhưng thuần túy chỉ là giám sát và cảnh báo sự cố, không có khả năng phòng chống tấn công có chủ đích vào hệ thống, và trong khuyến cáo của An ninh mạng Viettel cũng nêu rõ việc trang bị thiết bị thiết bị phòng chống tấn công là tỉnh cần phải đầu tư để đảm bảo cho việc phòng chống tấn công mạng

Sự cần thiết đầu tư:

Hệ thống mạng chưa có chức năng tường lửa và chưa có hệ thống chạy song song dự phòng. Hệ thống máy chủ và thiết bị lưu trữ hiện có cấu hình chưa đáp ứng được với nhu cầu xử lý, lưu trữ và sao lưu dữ liệu đối với các dịch vụ hành chính công, cụ thể như sau:

- Hệ thống tường lửa (Firewall chạy chế độ HA dự phòng) nhằm tăng hiệu quả kiểm soát, ngăn chặn truy cập trái phép và phòng chống tấn công từ bên ngoài vào hệ thống trung tâm dữ liệu tích hợp trọng yếu của Tỉnh.

- Hệ thống tường lửa bảo vệ là tiền đề, cơ sở tốt cho việc đầu tư nâng cấp hệ thống chuyển mạch chính (Core switch) và chuyển mạch nhánh (Access switch) sẽ tăng tốc việc chuyển mạch, gửi nhận dữ liệu giữa các phân vùng mạng cũng như chuẩn hoá kiến trúc hạ tầng mạng theo mô hình phổ biến 3 lớp Cốt lõi – Phân phối – Truy cập (Core – Distribution – Access). Hơn nữa, Firewall góp phần dễ dàng tích hợp với hệ thống cân bằng tải (Load Balancer) trong tương lai sẽ giúp Phân loại và định tuyến luồng dữ liệu WAN một cách tối ưu nhất, giúp giảm chi phí đầu tư đường truyền WAN cũng như có khả năng dự phòng khi một trong các đường truyền có sự cố, hệ thống sẽ tự động đẩy luồng dữ liệu qua các đường còn lại tránh thời gian chết (downtime) cho hệ thống, không ảnh hưởng đến hoạt động nghiệp vụ của các cơ quan, đơn vị trong tỉnh.

2. Giải pháp nâng cấp, đầu tư

a) Phương án kỹ thuật và các chỉ tiêu chung của hệ thống sau khi đầu tư thiết bị

- Sử dụng các thiết bị và phần mềm tiên tiến, hiện đại phù hợp với xu hướng phát triển hiện nay của công nghệ thông tin.
- Có khả năng mở rộng nâng cấp dễ dàng khi tăng cường thêm thiết bị, module mà không làm thay đổi logic hệ thống.
- Thuận tiện trong việc giao tiếp, kết nối với các hệ thống khác.
- Đảm bảo tuân thủ các chuẩn về công nghệ thông tin cũng như các chuẩn về thiết bị ngoại vi sử dụng trong hệ thống.

b) Công nghệ tường lửa

Phân tích theo công nghệ: Có khá nhiều công nghệ tường lửa nhưng chúng ta có thể thấy 4 loại công nghệ được sử dụng rất nhiều trong thực tế:

Công nghệ lọc gói tin (Packet Filter Firewall):

Cơ chế hoạt động

Hoạt động tại mức 3 (layer 3) trong mô hình kết nối OSI. Tường lửa này hoạt động trên cơ chế kiểm soát các luồng dữ liệu đi qua nó bằng cách so địa chỉ nguồn/đích và cổng nguồn/đích của gói tin với chính sách đã định sẵn.

Ưu điểm:

Tường lửa này cho tốc độ cao vì chúng thực hiện việc kiểm tra khá đơn giản tại lớp mạng;

Tích hợp được với hầu hết các thiết bị mạng như Router, Switch,….

Nhược điểm:

Có mức độ bảo mật kém vì cần phải mở các cổng lớn (>1023) để phục vụ các kết nối;

Không hiểu được trạng thái của các ứng dụng, dẫn đến mức độ bảo mật kém.

Công nghệ tường lửa kiểm soát trạng thái (Stateful Inspection Firewall):

Cơ chế hoạt động

Công nghệ tường lửa kiểm soát trạng thái hoạt động tại tầng 3 đến tầng 7 (layer 3 - 7) trong mô hình kết nối OSI. Tường lửa này hoạt động theo cơ chế kiểm soát các luồng dữ liệu đi qua nó bằng cách so sánh các thông tin như địa chỉ nguồn/đích, cổng, trạng thái kết nối, ứng dụng kết nối,… với chính sách bảo mật định trước và một bảng trạng thái động.

Ưu điểm

Tường lửa này cho tốc độ cũng như mức bảo mật cao với việc kiểm tra chi tiết các thông tin tại các tầng từ 3 – 7 trong mô hình OSI.

Nhược điểm

Đối với công nghệ này, kỹ thuật kiểm soát chủ yếu vẫn là lọc gói (packet filter), không nhận biết được dữ liệu của tầng 7.

Không còn phù hợp trong môi trường dữ liệu ứng dụng phức tạp hiện nay.

Công nghệ tường lửa UTM (Unified Threat Management):

Cơ chế hoạt động

Dựa trên công nghệ tường lửa Stateful Inspection, công nghệ tường lửa UTM hợp nhất các chức năng tường lửa, cổng truy cập VPN, Phòng chống tấn công (IDS/IPS), kiểm soát ứng dụng, phòng chống mã độc, lọc dữ liệu Web, chống mail spam, và có thể tích hợp các giải pháp giá trị gia tăng như tối ưu hóa dữ liệu WAN (WAN Optimization), Bộ quản lý truy cập không dây, cân bằng tải đường truyền… vào trong một thiết bị.

Ưu điểm:

Tường lửa này cho tốc độ cũng như mức bảo mật cao với việc kiểm tra chi tiết các thông tin tại các tầng từ 3 – 7 trong mô hình OSI.

Đơn giản hóa việc quản lý nhiều giải pháp bảo mật riêng biệt, đồng nhất công nghệ và kỹ thuật bảo mật.

Chi phí đầu tư thấp so với đầu tư các giải pháp bảo mật riêng lẻ.

Nhược điểm:

Năng lực xử lý của thiết bị tường lửa UTM thường sụt giảm nhiều khi bật nhiều tính năng bảo mật cùng lúc.

Nhiều nhà sản xuất không cung cấp các tính năng trong bộ giải pháp UTM mà dùng cách tích hợp với đối tác cung cấp khác, dẫn đến tính không đồng nhất trong kiến trúc và độ trễ xử lý dữ liệu mạng.

Không được lựa chọn ở các vị trí quan trọng, cần độ trễ xử lý thấp mà vẫn đảm bảo mức độ bảo mật cao như DMZ, Core, WAN.

Công nghệ tường lửa NGFW (Next Generation Firewall):

Cơ chế hoạt động:

Dựa trên công nghệ tường lửa Stateful Inspection, tường lửa NGFW cung cấp thêm một tầng kiểm soát ứng dụng, cho phép nhận diện, kiểm soát các ứng dụng trên mạng và máy trạm không phụ thuộc vào port, giao thức, địa chỉ IP. Công nghệ này cung cấp tầm nhìn và khả năng kiểm soát toàn vẹn dữ liệu liệu ứng dụng, kể cả qua những kênh dữ liệu mã hóa như SSH hay TLS/SSL. Ví dụ ta cho phép Facebook Chat hoạt động, tuy nhiên chặn Facebook Video (cả 02 ứng dụng này đều chạy trên giao thức HTTP). Ngoài ra, tường lửa NGFW phải có năng lực tổng hợp các thông tin ngữ cảnh (người dùng, ứng dụng, chính sách) để nhận định dữ liệu mạng hợp lệ và dữ liệu độc hại.

Ưu điểm:

Tường lửa này cho tốc độ cũng như mức bảo mật cao với việc kiểm tra chi tiết các thông tin tại các tầng từ 3 – 7 trong mô hình OSI.

Bằng cách xác định ứng dụng/ một số chức năng đặc trưng của ứng dụng, tường lửa NGFW cho phép người quản trị thiết lập các chính sách bảo mật theo cấp độ ứng dụng/ chức năng/ người dùng chặt chẽ hơn.

Bảo mật cho dữ liệu ứng dụng: quét virus, mã độc, spyware và các tấn công mạng.

Nhược điểm:

Do phải can thiệp vào dữ liệu ứng dụng, nên năng lực bảo mật của NGFW phụ thuộc vào cơ sở dữ liệu nhận diện ứng dụng và tấn công mạng.

Năng lực xử lý của các NGFW có thể sụt giảm rõ rệt nếu không được thiết kế phần cứng chuyên biệt để xử lý nhiều lớp tính năng bảo mật một lúc.

Chi phí đầu tư cao

Đề xuất lựa chọn giải pháp tường lửa NGFW cho mạng WAN:

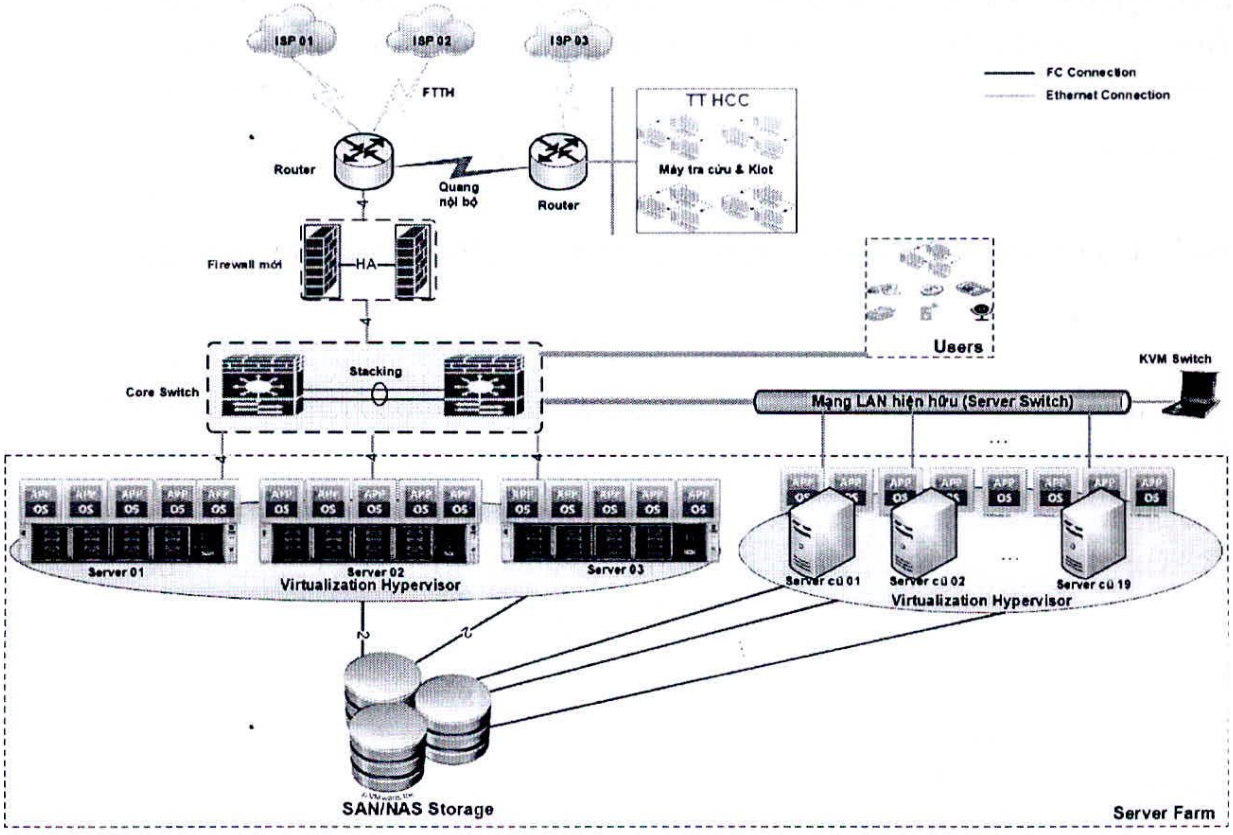
Tại vùng mạng này, cần kiểm soát lưu lượng từ vùng mạng WAN vào mạng bên trong để bảo vệ các vùng máy chủ publish website ra ngoài, có thể sử dụng thêm các tính năng kiểm soát ứng dụng và người dùng, IPS. Không cần sử dụng các tính năng khác như URL Filtering hay DLP, sẽ gây tốn chi phí và năng lực của thiết bị.

Khả năng kiểm soát và ra quyết định theo ngữ cảnh (ứng dụng, người dùng, chính sách).

Năng lực xử lý cao, độ trễ thấp theo đặt trưng yêu cầu của môi trường kết nối WAN.

c) Mô hình và thuyết minh thiết kế hệ thống

* Mô hình thiết kế chi tiết tích hợp tường lửa mới vào hạ tầng hiện hữu.



Hình 1. Hệ thống tường lửa bổ sung vào hệ thống hiện hữu

- Các thành phần và chức năng bao gồm:

+ Kết hợp với hệ thống Core network không thể thiếu hệ thống tường lửa (Firewall) nhằm tăng hiệu quả kiểm soát, ngăn chặn và phòng chống tấn công từ bên ngoài vào hệ thống trung tâm dữ liệu tích hợp trọng yếu của Tỉnh. Mức độ bao mật cao với việc kiểm tra chi tiết các thông tin tại các tầng từ 3 – 7 trong mô hình OSI.

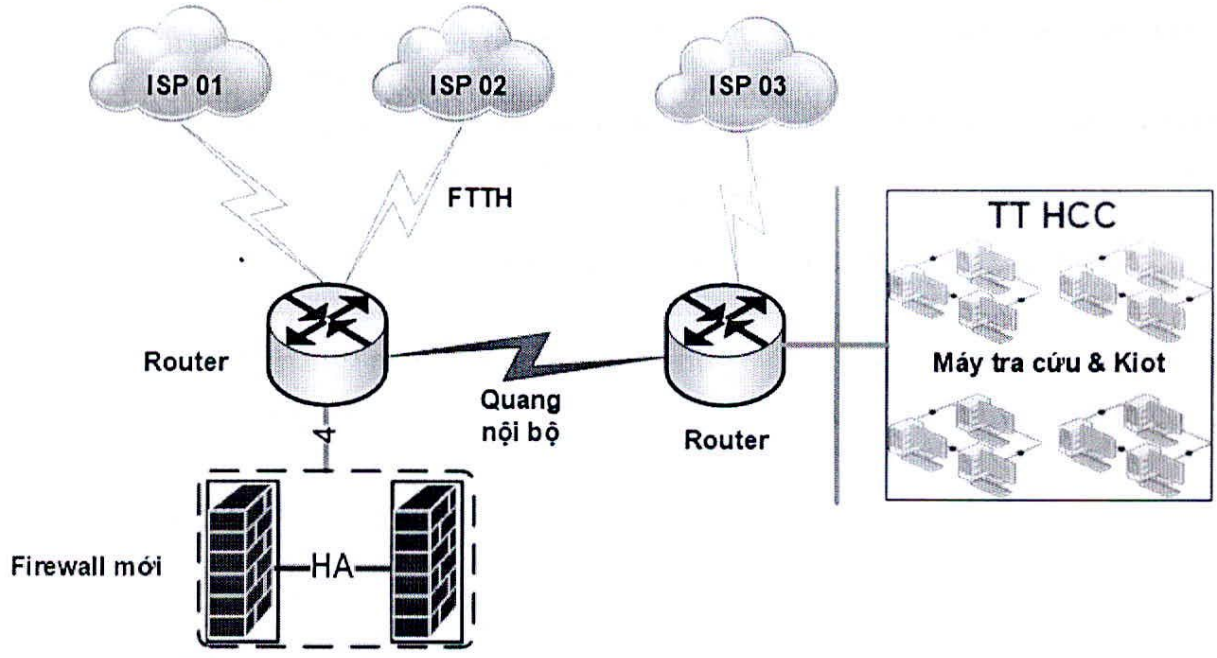
+ Firewall và Core Switch được trang bị một cặp thiết bị, triển khai cơ chế High Availability/Stacking nhằm tăng khả năng dự phòng và tính sẵn sàng của hệ thống khi một trong hai thiết bị gặp sự cố sẽ tự động failover gói tin qua thiết bị còn lại mà không ảnh hưởng đến quá trình nghiệp vụ liên tục.

+ Hỗ trợ cách xác định ứng dụng/ một số chức năng đặc trưng của ứng dụng, tường lửa NGFW cho phép người quản trị thiết lập các chính sách bảo mật theo cấp độ ứng dụng/ chức năng/ người dùng chặt chẽ hơn.

+ Bảo mật cho dữ liệu ứng dụng: quét virus, mã độc, spyware và các tấn công mạng.

- Diễn giải mô hình thiết kế:

+ Phân vùng Internet

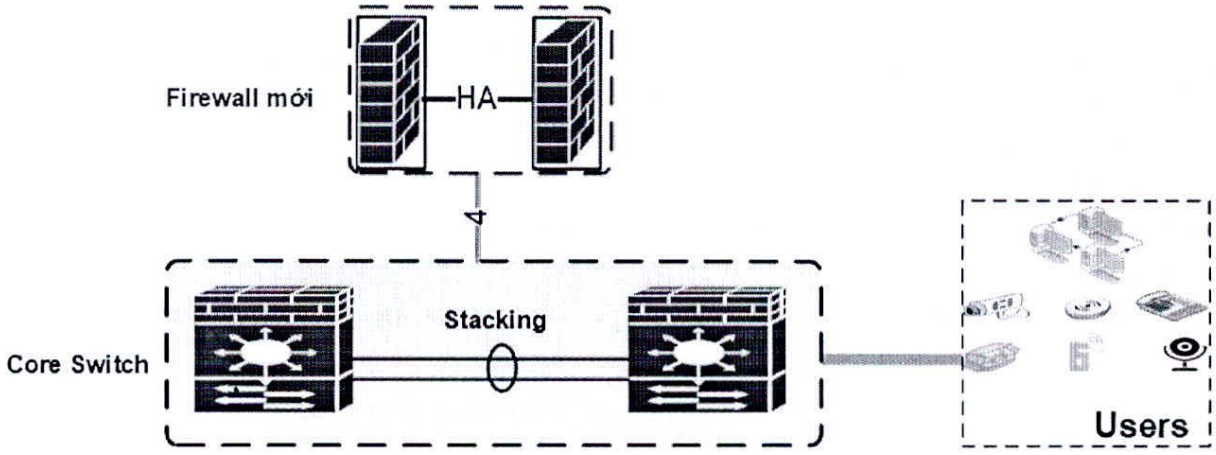


Vùng mạng WAN/Internet

- Hệ thống tại trung tâm có 02 đường truyền Internet FTTH kết nối đến hệ thống router đảm bảo băng thông, nâng cao tính ổn định, dự phòng đường truyền và phân chia lưu lượng băng thông khi truy xuất từ bên trong và bên ngoài. Đồng thời kết nối đến trung tâm hành chính công với đường quang nội bộ.
- Router sẽ kết nối đến hệ thống firewall mới được cấu hình port ở chế độ HA với chế độ (active-active hoặc active-standby), nhờ sự tách biệt khối điều khiển (control plane) / xử lý dữ liệu (data plane) trên kiến trúc phần cứng giúp firewall có tính sẵn sàng cao và không bị gián đoạn khi thông lượng qua khối xử lý dữ liệu tăng đột biến, nâng cao tính bảo mật thông tin, ngăn chặn các cuộc tấn công từ internet và các vùng khác vào bên trong vùng nội bộ (LAN) của hệ thống.

- Firewall với chức năng bảo vệ, ngăn chặn và phòng chống các virus, malware, spyware, ransomware, phishing,... từ Internet vào bên trong hệ thống nhờ hỗ trợ các tính năng Threat Prevention, IPS, Application Control, URL Filtering, DNS Security hay VPN với SSL giúp bảo mật các kết nối từ xa về hệ thống TTTHDL.
- Đồng thời cặc lưu lượng truy cập từ Internet vào hệ thống cũng được mã hoá toàn bộ nên dữ liệu đi vào hay đi ra đều được bảo vệ một cách nghiêm ngặt cho dù các mối nguy hay lỗ hỏng hệ thống đến từ bất cứ đâu bởi công nghệ zero trust.

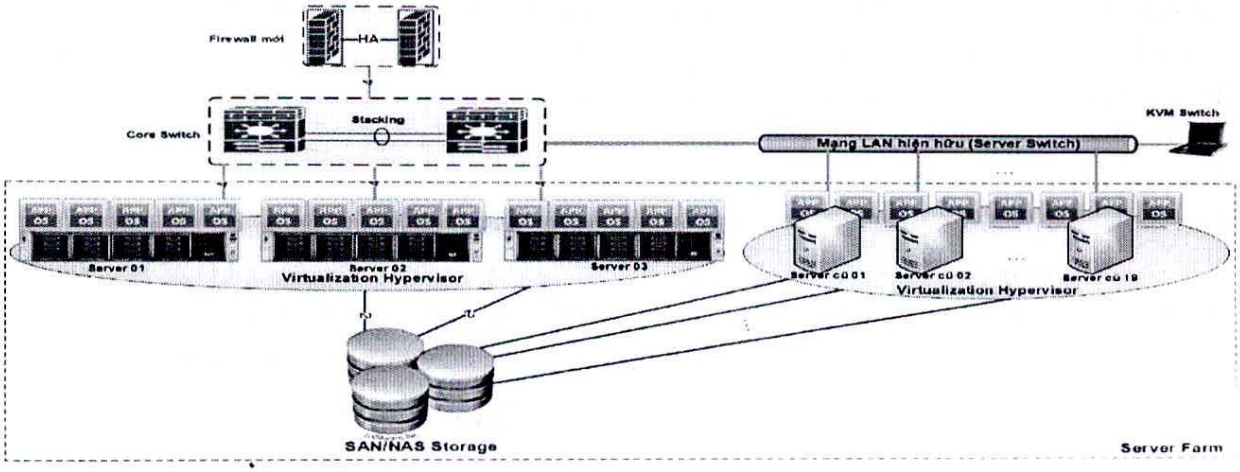
+ Phân vùng truy cập nội bộ (LAN)



Vùng người dùng (Users Access)

- Hệ thống Firewall bảo vệ mạng nội bộ và chịu trách nhiệm ngăn chặn sự tấn công từ internet vào lớp người dùng (Users).
- Firewall hỗ trợ khả năng kiểm soát người dùng, ứng dụng và nội dung với sự kết hợp sử dụng ba công nghệ nhận dạng tiên tiến: App-ID, User-ID and Content-ID nhằm bảo vệ đến mức tối đa các truy cập, hành vi, dữ liệu của user khi truy cập vào ra Internet, mạng botnet hay bên trong vùng server của TTTHDL tỉnh và sẽ cảnh báo ngay lập tức cho người quản trị hệ thống được tích hợp sẵn trong thiết bị.
- Hệ thống Firewall mới được nối với thiết bị chuyển mạch trung tâm bằng 04 port tốc độ 1/10Gbps và thiết bị trung tâm được stacking port với nhau chịu trách nhiệm định tuyến giữa các máy chủ trong hệ thống với nhau và định tuyến giữa mạng bên ngoài với các máy chủ trong hệ thống.

Vùng máy chủ (Server Farm)



- Tương tự như đối với vùng người dùng, hệ thống Firewall có khả năng kiểm soát ứng dụng, người dùng và dữ liệu nhờ công nghệ nhận dạng cao cấp App-ID, User-ID and Content-ID. Hơn nữa, các lưu lượng dữ liệu được truyền đi được mã hoá từ điểm đầu đến điểm cuối (end-to-end) cùng với việc dò tìm và ngăn chặn các lỗ hổng ứng dụng (zero day), file nhạy cảm, phần mềm độc hại, ransomware, APT bằng phân tích dự đoán dựa trên Machine Learning từ sandbox của thiết bị cho thấy sự tối ưu vượt bậc trong công nghệ cũng như kiến trúc, cách thức hoạt động của hệ thống tường lửa đề xuất cho TTTHDL tỉnh Sơn La là điều hết sức cần thiết và phù hợp nhất.
- Cặp thiết bị core switch trung tâm sẽ đấu nối xuống hệ thống máy chủ mới bằng 04 port tốc độ 1/10Gbps nhằm tăng cường băng thông truy xuất các máy chủ bên trong phục vụ việc truy xuất dữ liệu từ người dùng bên trong và người dùng truy xuất dữ liệu từ bên ngoài, kết nối với hệ thống máy chủ cũ qua các switch layer 2 (server switch) được tận dụng một cách triệt để.
- Trên hệ thống server được sử dụng toàn bộ trên nền tảng ảo hoá giúp việc quản trị và cấp phát tài nguyên chạy các ứng dụng cũng nhanh chóng và thuận tiện. Ngoài ra còn có hệ thống lưu trữ tập trung SAN/NAS Storage cho việc tập trung hoá dữ liệu và dễ dàng mở rộng trong tương lai.

- Cách thức vận hành hệ thống tường lửa:

+ Hệ thống tường lửa lớp 7 được trang bị mới để hình thành mô hình phòng thủ theo chiều sâu (2 lớp tường lửa – Defense in Depth) cho hệ thống mạng Internet và mạng LAN.

+ Bảo vệ và ngăn chặn các tấn công từ vùng mạng Internet vào ra vùng mạng nội bộ, vùng mạng DMZ (nếu có).

+ Hỗ trợ thiết lập kết nối bảo mật, an toàn và ổn định giữa các đơn vị.

+ Cung cấp hệ thống an ninh ảo toàn diện với Firewall, VPN, Application Control, IPS

+ Hỗ trợ khả năng cập nhật động cơ phòng chống xâm nhập mạng trái phép (IPS) trực tuyến hoặc cập nhật từ hệ thống Signature server đặt tại vùng mạng nội bộ hoặc cập nhật bằng tay

+ Kiểm soát người dùng truy cập internet thông qua tên người dùng xác thực bằng hệ thống LDAP/Active directory

+ Đảm bảo hỗ trợ chuẩn Ipv6

+ Giao diện điều khiển tiếng Anh

+ Vận hành đạt tính sẵn sàng cao

+ Báo cáo kiểm soát người dung truy cập internet:

- Hiển thị trạng thái truy cập thời gian thực cho từng người dùng
- Hiển thị đồ thị top người dùng truy cập web nhiều nhất
- Hiển thị đồ thị top người dùng có dung lượng truy cập nhiều nhất
- Hiển thị đồ thị top người dùng có thời lượng truy cập nhiều nhất

- Hiển thị đồ thị mật độ người dùng truy cập web trong 24 giờ vừa qua
- Báo cáo chi tiết truy cập web theo ngày: Người dùng, dung lượng, thời lượng, trang web truy cập

d) Sơ đồ lắp đặt thiết bị trên tủ rack

Sơ đồ chỉ thể hiện vị trí lắp đặt trên tủ rack cho thiết bị tường lửa (mới) sẽ đầu tư, các thiết bị khác không thể hiện. Tuy nhiên, có thể điều chỉnh vị trí theo tình hình thực tế trong quá trình triển khai.

e) Danh sách thiết bị, thống số kỹ thuật đề xuất

TT	Thống số kỹ thuật đề xuất (sản phẩm tương đương hoặc cao hơn)
I	**Thiết bị tường lửa**
1.1	Hiệu năng: - Firewall throughput (App-ID): 4.8Gbps - Threat Prevention throughput (appmix): 2.6Gbps - IPsec VPN throughput: 2.6Gbps - New session per second: 52800 - Max session: 1M
1.2	Tính năng: Có sẵn các tính năng: App-ID, IPS, antivirus, anti-spyware, DNS Sinkhole
1.3	Cổng kết nối: - 12 cổng 10/100/1000 - 4 cổng 1G/10G SFP/SFP+ - 4 cổng 1G SFP (4) - 2 cổng HA 10/100/1000 high availability - 1 cổng 10G SFP+ high availability
1.4	Ổ cứng: 240GB SSD

TT	Thống số kỹ thuật đề xuất (sản phẩm tương đương hoặc cao hơn)
I	**Thiết bị tường lửa**
1.5	Kiến trúc phần cứng: Tách biệt phần cứng quản trị (Management) và phần cứng xử lý dữ liệu (Data plane)
1.6	Bộ xử lý: 14 vCPU (core)
1.7	Tính sẵn sàng cao: - Active/active, active/passive, HA clustering - Failure detection: Path monitoring, interface monitoring
1.8	Nguồn cung cấp: Nguồn dự phòng và có thể thay thế nóng khi đang chạy
1.9	Bảo hành và dịch vụ hỗ trợ kỹ thuật: 36 tháng
1.10	Kiểu dáng: Rackmount

3. Danh mục quy chuẩn, tiêu chuẩn kỹ thuật được áp dụng

Hệ thống khi thiết kế, triển khai đảm bảo tuân thủ danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nước công bố kèm theo Thông tư số 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ trưởng Bộ Thông tin và Truyền thông:

- Các tiêu chuẩn kết nối;
- Các tiêu chuẩn tích hợp dữ liệu;
- Các tiêu chuẩn truy cập thông tin;
- Các tiêu chuẩn an toàn thông tin.

4. Thuyết minh nội dung đào tạo hướng dẫn khai thác

a) Mục tiêu đào tạo

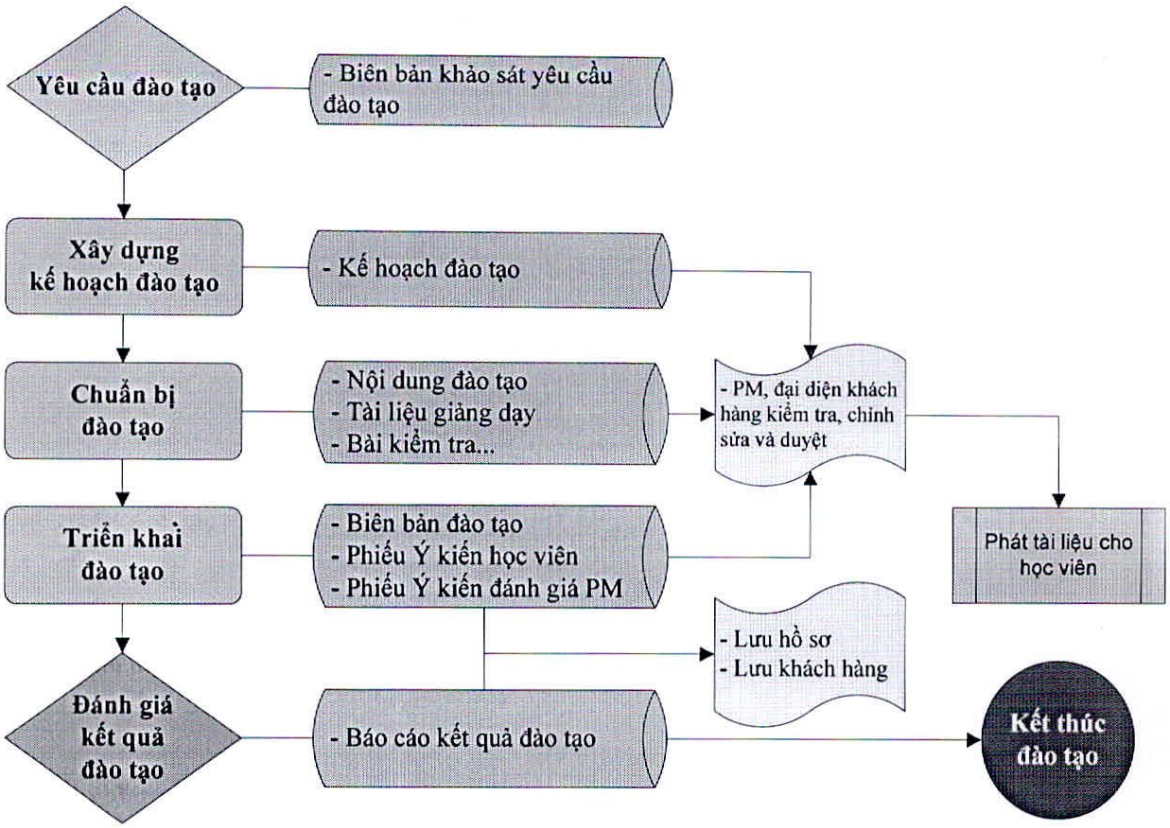
Đào tạo hướng dẫn sử dụng với mục đích cung cấp đầy đủ các kiến thức cơ bản và nâng cao về các bước triển khai, khai thác và hướng sử dụng nhằm hỗ trợ cán bộ, công chức thực hiện tốt các nhiệm vụ sau:

- Thực hiện các thao tác cơ bản trong quy trình vận hành xử lý phát sinh sau khi dự án kết thúc;

- Khai thác, sử dụng thiết bị một cách an toàn, bảo mật và có hiệu quả.

b) Quy trình đào tạo

Quy trình đào tạo được thực hiện cụ thể theo các bước sau:



Hình: Quy trình đào tạo

c) Phạm vi và địa điểm đào tạo

- Địa điểm: Trụ sở Trung tâm Công nghệ thông tin và Truyền thông.

- Đối tượng tham gia: cán bộ kỹ thuật thuộc Trung tâm Công nghệ thông tin và Truyền thông.

- Số lượng học viên: Dự kiến số lượng học viên cho lớp Quản trị hệ thống là 06 học viên; Số lượng học viên cho lớp Vận hành, khai thác là 06 học viên;

- Thời gian: Dự kiến mỗi lớp đào tạo diễn ra trong vòng 1 ngày.

d) Nội dung đào tạo

- Đào tạo quản trị hệ thống:

  o Cài đặt, cấu hình hệ thống;

  o Thiết lập các thông số (thời gian kết nối, mức độ an ninh, mức độ truy cập, mức độ thực hiện, nhật ký (Logging);

  o Các thông báo lỗi của ứng dụng;

- Đào tạo hướng dẫn sử dụng nghiệp vụ hệ thống:

  o Giới thiệu quy trình, quy tắc vận hành hệ thống;

  o Đào tạo hướng dẫn sử dụng từng chức năng nghiệp vụ tính năng trên thiết bị;

  o Giới thiệu những lỗi người sử dụng thường gặp trong quá trình vận hành, khai thác hệ thống...;

PHẦN III
DỰ TOÁN KINH PHÍ

1. Căn cứ lập dự toán

- Luật thuế giá trị gia tăng (GTGT) số 13/2008/QH12 của Quốc hội;

- Thông tư 03/2020/TT-BTTTT ngày 24/02/2020 của Bộ Thông tin và Truyền thông v/v Quy định về lập đề cương và dự toán chi tiết đối với hoạt động ứng dụng công nghệ thông tin sử dụng kinh phí chi thường xuyên thuộc nguồn vốn ngân sách nhà nước;

- Nghị định số 63/2014/NĐ-CP ngày 26/6/2014 của Chính phủ quy định chi tiết thi hành một số điều của Luật đấu thầu về lựa chọn nhà thầu;

- Quyết định số 2378/QĐ-BTTTT ngày 30/12/2016 của Bộ Thông tin và Truyền thông về công bố định mức về chi phí quản lý dự án, chi phí tư vấn đầu tư ứng dụng CNTT sử dụng nguồn vốn ngân sách nhà nước;

- Quyết định số 1688/QĐ-BTTTT ngày 11/10/2019 của Bộ Thông tin và Truyền thông về việc sửa đổi, bổ sung Quyết định số 2378/QĐ-BTTTT ngày 30 tháng 12 năm 2016 của Bộ Trưởng Bộ Thông tin và Truyền thông công bố định mức chi phí quản lý dự án, chi phí tư vấn đầu tư ứng dụng công nghệ thông tin sử dụng ngân sách nhà nước;

- Báo giá tham khảo.

2. Dự toán kinh phí thực hiện

Tổng kinh phí: 3.173.000.000 VNĐ (Bằng chữ: *Ba tỷ một trăm bảy mươi ba triệu đồng*). Trong đó:

+ Chi phí mua sắm thiết bị, nâng cấp: 3.151.660.000 đồng.

+ Chi phí tư vấn: 13.340.000 đồng.

+ Chi phí khác (Thẩm định giá): 8.000.000 đồng.

PHẦN IV
DỰ KIẾN TIẾN ĐỘ THỰC HIỆN

Tổng hợp thời gian triển khai theo bảng như sau:

1. Tiến độ triển khai

Tiến độ chi tiết như sau:

STT	HẠNG MỤC CÔNG VIỆC	THỜI GIAN THỰC HIỆN					
		Tháng 03/2022	Tháng 04/202	Tháng 05/202	Tháng 6/2022	...	Tháng 12/2022
1	Lập đề cương và dự toán chi tiết						
2	Tổ chức đấu thầu, lựa chọn các nhà thầu						
3	Triển khai hợp đồng						
4	Nghiệm thu, Báo cáo, tổng kết, vận hành hệ thống						

Ghi chú: Các công việc có thể được thực hiện nối tiếp hoặc song song.

2. Tổ chức duy trì, vận hành sau đầu tư:

Sau khi đơn vị thi công, đào tạo chuyển và đưa vào khai thác, Trung tâm Công nghệ thông tin và Truyền thông chủ động quản lý hệ thống và phân quyền sử dụng cho các Sở, ban ngành trên địa bàn tỉnh

3. Trách nhiệm các cơ quan, đơn vị

a) Trách nhiệm của Trung tâm Công nghệ thông tin và Truyền thông thuộc Sở Thông tin và Truyền thông

- Chủ đầu tư, tổ chức quản lý, lựa chọn đối tác thực hiện các công việc theo đúng nội dung được cơ quan chủ quản phê duyệt, theo đúng quy định nhà nước về triển khai đầu tư ứng dụng CNTT;

- Quản lý tốt hợp đồng về tiến độ, chất lượng, giải ngân và nghiệm thu, thanh lý hợp đồng theo các quy định hiện hành;

- Tổ chức tiếp nhận, vận hành, khai thác và sử dụng hệ thống;

b) Trách nhiệm của đơn vị thi công

- Đơn vị thi công cung cấp sản phẩm đảm bảo theo như thiết kế, đáp ứng đầy đủ năng lực vận hành. Bàn giao và đào tạo chuyển giao theo các yêu cầu của hợp đồng đã ký;

- Đảm bảo thực hiện đúng theo kế hoạch của dự án/hạng mục, báo cáo với chủ đầu tư kịp thời những vướng mắc, khó khăn trong quá trình thực hiện để tránh ảnh hưởng đến tiến độ, chất lượng hạng mục.

- Chấp hành nghiêm chỉnh quy trình, quy phạm Nhà nước về quản lý chất lượng đối với dự án/hạng mục đầu tư công nghệ thông tin

- Đảm bảo các quy trình về bảo hành, bảo trì và nâng cấp hệ thống theo đúng thời gian trong yêu cầu của dự án, nhiệm vụ…

- Nhà thầu có trách nhiệm giải trình chi tiết phần Chi phí chung khi thực hiện các thủ tục thanh quyết toán.

PHẦN V
KIẾN NGHỊ VÀ ĐỀ XUẤT

Việc triển khai nâng cấp thiết bị tường lửa cho Trung tâm tích hợp dữ liệu sẽ mang lại các kết quả nhìn thấy như đảm bảo sự an toàn và ổn định cho các vùng mạng như LAN,. WAN và vùng Máy chủ vì thế việc nâng cấp là rất cần thiết trong giai đoạn hiện nay, Trung tâm Công nghệ thông tin và Truyền thông kính đề nghị Sở Thông tin và Truyền thông tỉnh thẩm định trình cấp có thẩm quyền phê duyệt, để Trung tâm có căn cứ triển khai các bước tiếp theo.

Phụ lục I
TỔNG HỢP DỰ TOÁN

Đvt: Đồng

STT	Khoản mục chi phí	Ký hiệu	Cách tính	Chi phí trước thuế	Thuế	Chi phí làm tròn	Tham chiếu cách tính
1	**Mua sắm thiết bị, nâng cấp**	**Gtb**		**2.865.145.455**	**286.514.545**	**3.151.660.000**	
1.1	Mua sắm, nâng cấp thiết bị chuyên dùng	Gtb1	*Dự toán chi tiết*	2.865.145.455	286.514.545	3.151.660.000	
2	**Chi phí tư vấn**	**Gtv**	**Gtv1+Gtv2**	**12.343.175**	**987.454**	**13.340.000**	
2.1	*Chi phí lập hồ sơ mời thầu, đánh giá hồ sơ dự thầu*	*Gtv1*	*Gtb*0,283%*	8.108.362	648.669	8.760.000	Quyết định 1688/QĐ-BTTTT ngày 11/10/2019)
2.2	*Chi phí thẩm định hồ sơ mời thầu và thẩm định kết quả lựa chọn nhà thầu*	*Gtv2*	*Mức tối thiểu*	*2.000.000*	160.000	*2.160.000*	(Nghị định 63/2014/NĐ-CP ngày 26/6/2014)
2.3	*Chi phí thẩm tra đề cương và dự toán chi tiết*	*Gtv3*	*0.078%*	*2.234.813*	178.785	*2.420.000*	Quyết định 1688/QĐ-BTTTT ngày 11/10/2019)
3	**Chi phí khác**	**Gk**		**7.407.407**	**592.593**	**8.000.000**	
3.1	*Chi phí thẩm định giá*	*Gk1*	*Theo HĐ*	*7.407.407*	*592.593*	*8.000.000*	Thực tế
	TỔNG CỘNG	**TM**	**Gtb+Gqlda+Gk**	**2.884.896.037**	**288.094.592**	**3.173.000.000**	

Bằng chữ: Ba tỷ một trăm bảy mươi ba triệu đồng

Phụ lục II
DANH MỤC, CHỦNG LOẠI CÁC THIẾT BỊ

TT	Danh mục vật tư	Đơn giá (VNĐ)	Số lượng (Bộ)	Thành tiền (VNĐ)
1	**Thiết bị tường lửa**	1.575.830.000	2	**3.151.660.000**
1.1	Hiệu năng: - Firewall throughput (App-ID): 4.8Gbps - Threat Prevention throughput (appmix): 2.6Gbps - IPsec VPN throughput: 2.6Gbps - New session per second: 52800 - Max session: 1M			
1.2	Tính năng: Có sẵn các tính năng: App-ID, IPS, antivirus, anti-spyware, DNS Sinkhole			
1.3	Cổng kết nối: - 12 cổng 10/100/1000 - 4 cổng 1G/10G SFP/SFP+ - 4 cổng 1G SFP (4) - 2 cổng HA 10/100/1000 high availability - 1 cổng 10G SFP+ high availability			
1.4	Ổ cứng: 240GB SSD			
1.5	Kiến trúc phần cứng: Tách biệt phần cứng quản trị (Management) và phần cứng xử lý dữ liệu (Data plane)			
1.6	Bộ xử lý: 14 vCPU (core)			
1.7	Tính sẵn sàng cao: - Active/active, active/passive, HA clustering - Failure detection: Path monitoring, interface monitoring			
1.8	Nguồn cung cấp: Nguồn dự phòng và có thể thay thế nóng khi đang chạy			
1.9	Bảo hành và dịch vụ hỗ trợ kỹ thuật: 36 tháng			
1.10	Kiểu dáng: Rackmount			