Người ký: Sở Y tế
Cơ quan: Ủy ban Nhân dân tỉnh Thái Bình
Thời gian ký: 06.12.2018 08:56:12 +07:00

UBND TỈNH THÁI BÌNH
SỞ Y TẾ

Số: 112/KH-SYT

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

Thái Bình, ngày 30 tháng 11 năm 2018

KẾ HOẠCH
Xây dựng hệ thống an toàn, an ninh thông tin và lưu trữ dữ liệu cho hệ thống sever máy chủ dữ liệu Database house - Sở Y tế Thái Bình

I. Tính cấp thiết xây dựng hệ thống đảm bảo an toàn, an ninh thông tin và lưu trữ dữ liệu tại Sở Y tế Thái Bình

Công nghệ thông tin (CNTT) đang dần chứng tỏ tầm ảnh hưởng rất lớn đến mọi mặt của đời sống xã hội. Đối với hoạt động của ngành y tế, có thể thấy, CNTT ngày càng đóng vai trò quan trọng trong quá trình cải cách hành chính trong công tác quản lý, điều hành của cơ quan nhà nước.

Sở Y tế là cơ quan đầu ngành Y tế trong tỉnh, quản lý toàn bộ hệ thống y tế từ các đơn vị y tế xã, phường, thị trấn đến các đơn vị y tế tuyến huyện, tỉnh. Nhu cầu ngày càng cao trong công tác quản lý điều hành cũng như quản lý ngành trong công tác khám chữa bệnh (KCB) như chụp cắt lớp, phẫu thuật nội soi, hội chẩn trực tuyến...công tác giảng dạy, đào tạo, giám sát dịch bệnh, nghiên cứu phát triển trong lĩnh vực y tế...

Đối với công tác quản lý Nhà nước, từ đầu năm 2012 Sở Y tế Thái Bình là đơn vị sớm áp dụng, triển khai thực hiện nhân rộng việc quản lý văn bản đến và văn bản đi trên Mạng văn phòng điện tử liên thông của Uỷ ban nhân dân tỉnh; Đến nay 100% các đơn vị trong ngành đều sử dụng mạng văn phòng để thực hiện thông suốt việc chỉ đạo, trao đổi thông tin, báo cáo và gửi dữ liệu.

Đối với công tác quản lý ngành, đầu năm 2018, Sở Y tế đã xây dựng hệ thống kho dữ liệu chung (Database - House) nhằm chủ động được trong cập nhật dữ liệu, thông tin, báo cáo kịp thời, chính xác; giúp ngành có sự quản lý toàn diện các thông tin, số liệu từ tuyến xã đến tuyến tỉnh và cá nhân người dân trong tỉnh.

Hệ thống máy chủ tại Sở Y tế đã được mua sắm đáp ứng nhu cầu cho kho dữ liệu dùng chung, 9/21 đơn vị bệnh viện đã kết nối thành công đến hệ thống dữ liệu chung (Database - House) của Sở và trong năm 2018 100% các bệnh viện sẽ kết nối vào hệ thống. Tuy nhiên, một thách thức đặt ra trong quá trình kết nối là việc đảm bảo an toàn, an ninh thông tin cho hệ thống Database - House và hệ thống phần mềm quản lý tại các bệnh viện.

Đơn cử một ví dụ, ngày 15/9/2018, BVĐK Thành phố đã bị sự cố tấn công mạng gây mã hoá dữ liệu. Dữ liệu đã bị mã hóa không thể được khôi phục vì hacker sử dụng thuật mã hóa công khai và khóa bí mật dùng để giải mã chỉ được lưu giữ trên server của hacker. Bệnh viện đã phải nhập tay lại dữ liệu bị thiệt hại tuy nhiên dữ liệu được khôi phục lại không còn được toàn vẹn như ban

đầu, thiệt hại của bệnh viện là rất lớn. Khi bệnh viện kết nối hệ thống Database house không được bảo vệ an toàn, virut sẽ lây lan rất nhanh tới hệ thống phần mềm các bệnh viện khác, khi đó thiệt hại về dữ liệu trong ngành sẽ nhân lên gấp nhiều lần.

Hệ thống dữ liệu được lưu trữ tại Sở Y tế khi triển khai các phần mềm gồm các dữ liệu về khám chữa bệnh từ các bệnh viện, các trạm y tế xã phường thị trấn, các chương trình mục tiêu, bệnh lây nhiễm, không lây,... Ước trong 5 năm hoạt động đạt khoảng 10Tb, đây là hệ thống dữ liệu rất lớn và cần thiết được lưu trữ qua các năm để phục vụ công tác quản lý, đánh giá của ngành vì vậy cần có một hệ thống lưu trữ dữ liệu riêng, được đảm bảo an toàn.

Trước những thực trạng nêu trên, để thực hiện hiệu quả sự chỉ đạo của Bộ Y tế, Uỷ ban nhân dân tỉnh trong việc ứng dụng công nghệ thông tin, cải cách thủ tục hành chính, giám định khám chữa bệnh bảo hiểm y tế, công tác quản lý ngành và quản lý trực tiếp tại các đơn vị; Sở Y tế Thái Bình đã xây dựng Kế hoạch về hệ thống an toàn, an ninh thông tin và lưu trữ dữ liệu cho hệ thống sever máy chủ dữ liệu Database house - Sở Y tế Thái Bình, nội dung cụ thể như sau:

II. CĂN CỨ LẬP KẾ HOẠCH

1. Căn cứ pháp lý

- Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

- Luật an toàn thông tin mạng số 86/2015/QH13;

- Luật Khám bệnh, chữa bệnh ngày 23 tháng 11 năm 2009;

- Quyết định số 1819/2015/QĐ-TTg ngày 26 tháng 10 năm 2015 của Thủ tướng Chính phủ về việc phê duyệt Chương trình quốc gia về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước giai đoạn 2016 – 2020;

- Quyết định số 997/2009/QĐ-UB ngày 12 tháng 5 năm 2009 của Ủy ban nhân dân tỉnh Thái Bình về chức năng, quyền hạn và tổ chức bộ máy của Sở Y tế;

- Thông tư 54/2017/TT-BYT ngày 29/12/2017 của Bộ Y tế ban hành bộ tiêu chí ứng dụng CNTT tại các đơn vị khám chữa bệnh;

- Quyết định 2916/QĐ-UBND ngày 09/11/2017 của Ủy ban nhân dân tỉnh Thái Bình ban hành bộ tiêu chí ứng dụng CNTT trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Thái Bình.;

- Quyết định 268/QĐ-SYT ngày 02/3/2018 của Sở Y tế phê duyệt Kế hoạch ứng dụng và phát triển công nghệ thông tin của Sở Y tế Thái Bình giai đoạn 2018-2020;

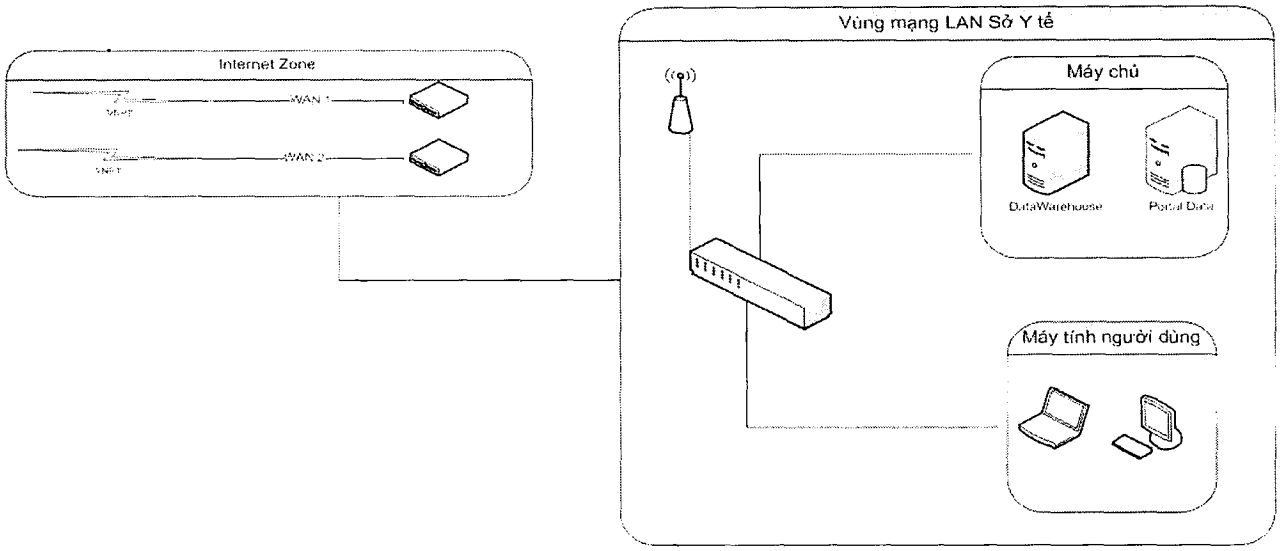
- Quyết định số 3232/QĐ-UBND ngày 12/12/2017 của Uỷ ban nhân dân tỉnh Thái Bình về việc giao dự toán thu chi ngân sách năm 2018;

- Thông báo số 210/TB-SYT ngày 5 tháng 10 năm 2017 của Sở Y tế Thái Bình về việc Thông báo Kết luận của Giám đốc Sở Y tế tại Hội nghị thông nhất

một số giải pháp ứng dụng công nghệ thông tin trong quản lý ngành, khám chữa bệnh BHYT và an ninh mạng trong ngành Y tế.

2. Căn cứ thực tiễn

1. *Sơ đồ kết nối hạ tầng mạng tại Sở Y tế*



2. *Hạ tầng mạng*
   - Hệ thống mạng của Sở Y tế như sau
     03 switch layer 2 3Com phân chia hệ thống mạng giữa các phòng ban
   - Sở chưa được trang bị thiết bị phát hiện và ngăn chặn tấn công mạng
3. *Hệ thống máy chủ*
   Sở Y tế được trang bị 2 máy chủ, trong đó:
   01 máy chủ cài đặp app của hệ thống Database house,
   01 máy chủ chứa dữ liệu hệ thống Database house.
4. *Hệ thống đường truyền*
   - Sở Y tế đang sử dụng 2 đường truyền Internet :
     02 đường truyền cáp quang tốc độ của VNPT
   - Các đơn vị trực thuộc chưa có đường truyền kết nối trực tiếp Sở Y tế mà kết nối qua mạng Internet
5. *Hệ thống các ứng dụng:*
   - Hệ thống dữ liệu dùng chung DataBase House kết nối trực tiếp với 20 bệnh viện và hệ thống y tế xã, phường, thị trấn
6. *Hệ thống sao lưu dữ liệu:*
   Sở Y tế đang thực hiện định kỳ việc sao lưu dữ liệu theo hình thức thủ công, cùng máy chủ hệ thống, chưa có hệ thống sao lưu theo tiêu chuẩn.
7. *Hệ thống máy trạm:*
   Sở Y tế có 60 máy trạm tại Sở Y tế và 21 máy trạm tại các đơn vị kết nối vào hệ thống.

III. MỤC TIÊU

1. Mục tiêu chung

Xây dựng hệ thống đảm bảo an toàn, an ninh thông tin cho cơ quan Sở Y tế và hệ thống sever máy chủ dữ liệu Database House.

2. Mục tiêu cụ thể:

- Xây dựng giải pháp cho các hệ thống:

+ Hệ thống giám sát và cảnh báo an ninh mạng

+ Thiết bị tường lửa và chống tấn công Firewal (BIF)

+ Hệ thống đảm bảo các chính sách an ninh được thực thi nghiêm túc và liên tục nhằm bảo vệ an ninh thông tin cho các hệ thống máy tính

+ Hệ thống cập nhật bản, lỗi hệ điều hành Windows Server Update Services

+ Hệ thống tổng thể phòng chống virus Bkav Endpoint Enterprise

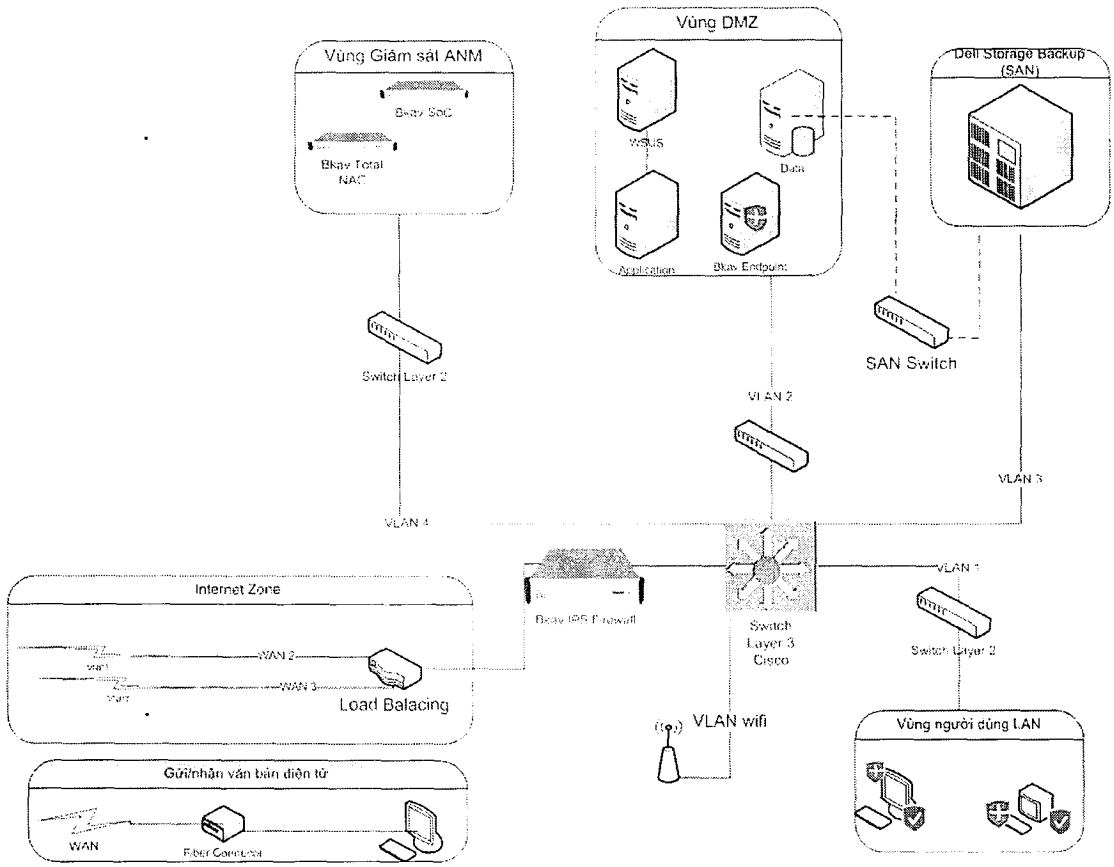
+ Hệ thống lưu trữ dữ liệu tiêu chuẩn SAN/NAS

- Đảm bảo năm 2018, có thể kết nối an toàn hệ thống Database House đến các đơn vị y tế theo đúng nội dung Quyết định 268/QĐ-SYT ngày 02/3/2018 của Sở Y tế phê duyệt Kế hoạch ứng dụng và phát triển CNTT của Sở Y tế Thái Bình giai đoạn 2018-2020.

III. NỘI DUNG KẾ HOẠCH

A. Hệ thống an toàn, an ninh mạng

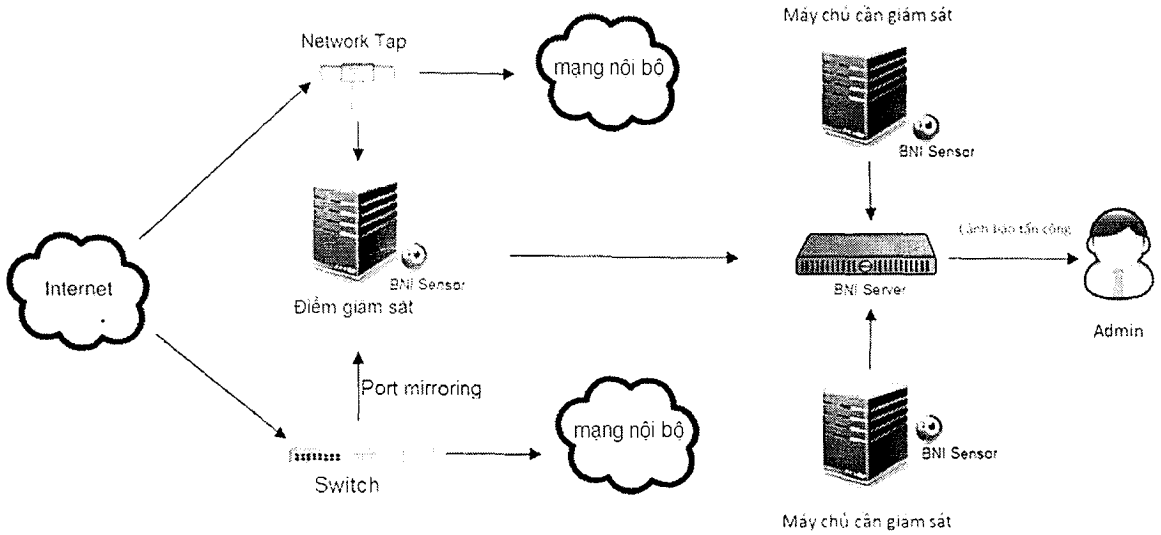
Mô hình triển khai giải pháp thiết bị và phần mềm ANM



1. Giải pháp về Thiết bị An ninh mạng

1.1 Thiết bị phát hiện và cảnh báo tấn công mạng Bkav Network Inspector SMB

- Bkav SoC – là thiết bị giám sát phát hiện, cảnh báo tấn công và các sự cố của hệ thống mạng sớm theo thời gian thực, dựa trên cơ chế phân tích các kết nối mạng và diễn biến sự kiện trên máy chủ, đường truyền mạng. Hệ thống bao gồm thiết bị xử lý trung tâm và các bộ cảm biến được cài đặt trên máy chủ và các điểm giám sát trên đường truyền.Mọi thông tin thay đổi trong hệ thống mạng đều được các cảm biến liên tục báo về thiết bị trung tâm. Từ đó, Bkav SoC phân tích và xác định dấu hiệu tấn công, các sự cố để cảnh báo cho đội ngũ quản trị qua SMS, email.
- Thực tế, các cuộc tấn công mạng vẫn âm thầm diễn ra khắp mọi nơi, cả Việt Nam và trên toàn thế giới. Tuy nhiên, hầu hết vụ việc không dễ bị phát hiện cho đến khi chúng gây ra những hậu quả rõ ràng như mất mát dữ liệu, làm tê liệt, thậm chí sụp đổ hệ thống. Hiện nay, hầu hết hệ thống mạng của các cơ quan doanh nghiệp Việt Nam chưa được trang bị các giải pháp phát hiện và cảnh báo tấn công. Đây chính là lỗ hổng lớn làm giảm khả năng ứng phó kịp thời với các sự cố về an ninh mạng. Với Bkav SoC việc phát hiện tấn công sẽ được cảnh báo tự động ngay từ khi có sự cố, thay vì phải chờ người sử dụng phát hiện ra.



Mô hình hoạt động của Bkav SoC

Chức năng:

Số TT	Chắc năng và đặc tính kỹ thuật
1.	Phát hiện sự thay đổi của các file hệ thống
2.	Cảnh báo khi dung lượng trống của ổ đĩa trên server dưới mức cho phép
3.	Cảnh báo khi các dịch vụ website không hoạt động (site down) hoặc dung lượng website có thay đổi vượt quá khoảng sai số cho phép
4.	Cảnh báo khi không có file backup dữ liệu tự động trên server
5.	Cảnh báo khi không kết nối được tới Server/Dịch vụ
6.	Cảnh báo khi hoạt động của tài nguyên (% CPU, % Ram, băng thông mạng) vượt quá giới hạn cho phép (giới hạn để tài nguyên hoạt động bình thường).
7.	Cảnh báo cập nhật bản vá cho server
8.	Phát hiện các cuộc tấn công Web: SQL Injection, XSS ...
9.	Phát hiện các cuộc tấn công DDoS
10.	Phát hiện nguy cơ từ việc phân tích event log

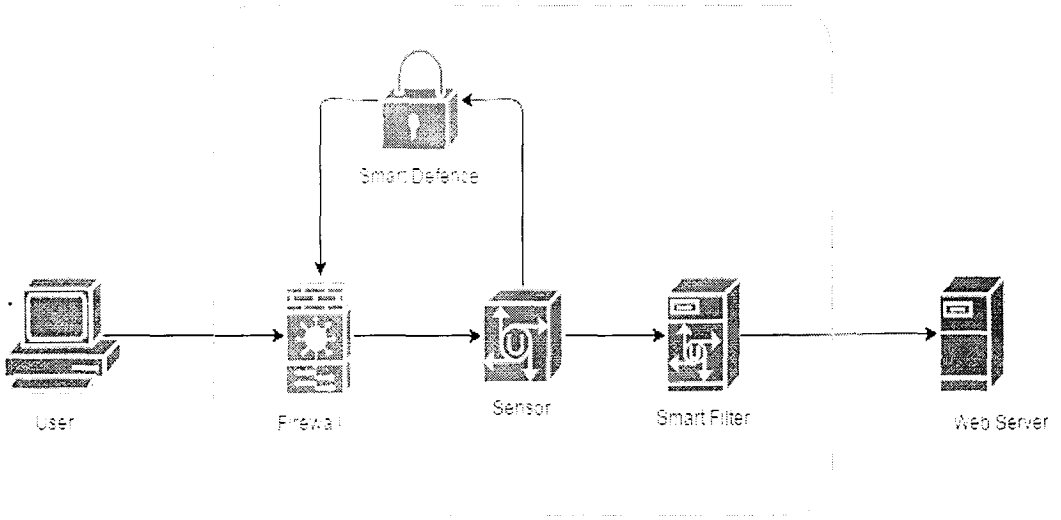
1.2 Thiết bị tường lửa và chống tấn công Bkav IPS Firewal (BIF)

- Làm thế nào để phát hiện và ngăn chặn khi bị tấn công vào hệ thống mạng một cách hiệu quả, khi mà các hình thức tấn công mạng ngày càng được thể hiện một cách tinh vi, liên tục thay đổi phương thức, cách thức khiến các quản trị mạng của các Cơ quan tổ chức thực sự gặp khó khăn. Đối tượng tấn công của hacker cũng rất đa dạng , không ngoại trừ ai và cơ quan nào với các nhiều mục đích khác nhau.
- Thiết bị tường lửa và chống tấn công Bkav IPS Firewall (BIF) được Bkav nghiên cứu và phát triển nhằm chống lại các cuộc tấn công trái phép trên. Thiết bị có nhiệm vụ ngăn chặn các nguy cơ tấn công vào các hệ thống trực truyến như tấn công web, đặc biệt là khả năng ngăn chặn hình thức tấn công DDoS vào các dịch vụ của cơ quan, tổ chức. Thông tin về thiết bị như sau:

- Bkav IPS Firewal (BIF) là Firewall thế hệ mới (Next-Generation Firewal), các cơ chế phân tích và ngăn chặn thông minh, mềm dẻo của BIF đảm bảo dịch Web luôn được bảo vệ trước các cuộc tấn công DDoS, tấn công ứng dụng Web như SQLi, XSS...một cách hiệu quả. Khi phát hiện tấn công BIF sẽ lập tức phân tích, ngăn chặn và cảnh báo tới người quản trị thông qua SMS, Email.

BIF bao gồm những tính năng nổi bật sau:

- **Smart Defence**
- **Smart Filter**
- **Web Accelerator**
- **Live Alert**



Bkav IPS Firewall

Hình 1. Mô hình triển khai

BIF có thể triển khai với 2 chế độ **Transparent** và **Proxy** tùy thuộc vào mô hình mạng triển khai :

- **Proxy**: Tất cả những domain cần được bảo vệ sẽ được trỏ tới địa chỉ IP của thiết bị BIF. Với chế độ này, BIF hỗ trợ thêm tính năng cân bằng tải, hỗ trợ tăng tốc Web (Web Accelerator).
- **Transparent**: Với chế độ này, việc triển khai thiết bị sẽ không ảnh hưởng gì tới mô hình mạng. Tuy nhiên, khi triển khai chế độ này, BIF không hỗ trợ 2 tính năng cân bằng tải và hỗ trợ tăng tốc Web.

Chi tiết chức năng:

STT	Chức năng	Đặc tính kĩ thuật
1.	**Smart Defence**	Công nghệ **Smart Defence** của **BIF** có khả năng tổng hợp, phân tích, tự học (machine learning) qua việc theo dõi lưu lượng mạng để phát hiện các dấu hiệu bất thường, đặc biệt là các dấu hiệu tấn công DoS/DDoS, từ đó điều khiển chức năng Firewall để bảo vệ cho các dịch vụ bên trong. - ICMP Flood - Ping Flood - SYN Flood - Spoof SYN Flood - SYN-ACK Flood - HTTP Slowloris - HTTP Slowbody - HTTP Slowread - HTTP Flood Khả năng phân tích, tự học của BIF được nâng cấp tự động từ các chuyên gia An ninh mạng của Bkav khi có các hình thức tấn công mới xuất hiện.
2.	**Smart Filter**	Công nghệ phòng chống tấn công ứng dụng web - **Smart Filter** đảm bảo cho các website được bảo vệ trước các cuộc tấn công khai thác thông qua lỗ hổng Website. Smart Filter của BIF có thể phát hiện và tự động ngăn chặn các dấu hiệu tấn công vào các lỗ hổng sau: - Command Injection - Cross Site Scripting - HTTP Pollution - LDAP Injection - PathTravesal and LFI, RFI - SQL Injection - XML Injection
3.	**Web Accelerator**	**BIF** có khả năng tự động tối ưu hóa tải Website và giảm tải cho webserver phía sau. Hỗ trợ việc tự động lưu lại trạng thái Website, khi Website gặp vấn đề kết nối hoặc dịch vụ không hoạt động, người dùng vẫn có thể duy trì việc truy

		cập Website với trạng thái đã được lưu trước đó.
4.	**Live Alert**	Khi hệ thống có dấu hiệu bất thường xảy ra, BIF có khả năng tự động gửi thông tin về các sự cố cho những người có trách nhiệm xử lý. Thông tin cảnh báo được gửi thông qua SMS và Email. Danh sách nhận cảnh báo có thể được cấu hình theo nhóm hoặc theo thứ tự ưu tiên tùy vai trò của người nhận (quản trị, quản lý).

1.3 Thiết bị quản lý chính sách an ninh thông tin Bkav Total NAC SMB

- Hiện nay, việc ứng dụng công nghệ thông tin trong các tổ chức, doanh nghiệp là xu thế tất yếu để cải thiện hiệu quả công việc và nâng cao năng suất lao động. Tuy nhiên đi kèm với điều đó là các nguy cơ về mất an ninh thông tin mà một phần xuất phát từ chính thói quen sử dụng các phần mềm, thiết bị của nhân viên. Để các hệ thống máy tính có thể tránh được các nguy cơ này, nhiều giải pháp, chính sách bảo mật đã được đưa ra và việc kiểm soát thực hiện chúng là điều hết sức cần thiết. Các chính sách bảo mật không chỉ đa dạng về cách thức thực hiện mà còn phải liên tục điều chỉnh để phù hợp với công việc của từng nhân viên, phòng ban trong các thời điểm khác nhau. Để các chính sách được thực hiện nghiêm túc sẽ cần một hệ thống giám sát liên tục để nhắc nhở nhân viên, đồng thời các vi phạm xảy ra trên các máy tính cũng cần được thống kê để quản trị viên của hệ thống có thể nắm được.
- Thiết bị Bkav Total Network Access Control (BTN) sẽ đảm bảo các chính sách an ninh được thực thi nghiêm túc và liên tục nhằm bảo vệ an ninh thông tin cho các hệ thống máy tính. BTN được thiết kế đơn giản, tiện dụng, khả năng tùy biến cao để đáp ứng được các nhu cầu của từng tổ chức, doanh nghiệp.

Chức năng:

STT	Chức năng
1.	Kiểm soát các phần mềm được cài đặt trên máy tính (không cho phép cài/sử dụng phần mềm có thể mang virus, chưa mua bản quyền, phần mềm remote máy tính từ xa).
2	Kiểm soát việc sử dụng thiết bị kết nối (USB, ổ đĩa CD…) và chia sẻ dữ liệu để tránh sao chép thông tin nội bộ.
3	Kiểm soát việc truy cập mạng internet của các máy: Kiểm soát truy cập web, Kiểm soát lượng dữ liệu ra khỏi máy tính
4	Thiết lập cấu hình bảo mật của hệ điều hành (tường lửa, chế độ mật khẩu, khóa màn hình khi không làm việc,…).
5.	Kiểm soát chia sẻ thư mục: Kiểm soát chặt chẽ việc chia sẻ thư mục ổ đĩa tránh bị sao chép lộ lọt thông tin.
6	Lưu trữ, thống kê thông tin vi phạm: Toàn bộ thông tin cảnh báo, vi phạm được BTN phát hiện tại các máy tính trong hệ thống sẽ được lưu trữ và gửi về máy chủ BTN để người quản trị kiểm soát và có biện pháp xử lý

2. Giải pháp về phần mềm An ninh mạng

2.1 Giải pháp cập nhật bản vá lỗi hệ điều hành Windows Server Update Services

Thông tin và dữ liệu đóng vai trò quan trọng trong hoạt động sản xuất kinh doanh cũng như sự phát triển của doanh nghiệp. Một trong những phương pháp quan trọng để bảo mật thông tin và dữ liệu là cập nhật thường xuyên các bản vá lỗi hệ điều hành Windows, các phần mềm của Microsoft trên các PC và Server. Tuy nhiên, với số lượng PC và Server tại các cơ quan tương đối lớn, việc thực hiện cập nhật (update) các bản vá lỗi (hotfixes), các bản nâng cấp cho các hệ điều hành, các phần mềm của Microsoft là một điều đáng được quan tâm. Hiện tại, việc cập nhật cho các PC và Server tại các cơ quan phần lớn được thực hiện một cách thủ công (từng người dùng thực hiện cập nhật riêng lẻ). Điều này dẫn đến các vấn đề như sau:

- Người dùng không thực hiện cập nhật các bản vá lỗi hoặc thực hiện cập nhật các bản vá lỗi không đầy đủ, dẫn đến nguy cơ bị tấn công vào các lỗ hổng bảo mật.

- Người quản trị chưa kiểm soát được tình trạng cập nhật các bản vá lỗi, các bản nâng cấp các hệ điều hành, các ứng dụng Microsoft của người dùng.
- Mỗi người dùng cập nhật một cách riêng lẻ các chương trình, hệ điều hành của Microsoft sẽ dẫn đến việc tiêu tốn băng thông, đặc biệt là băng thông quốc tế.
- Trong trường hợp đường truyền Internet bị chậm hoặc gián đoạn sẽ dẫn đến việc cập nhật các hệ điều hành, các chương trình của Microsoft cho PC và Server diễn ra lâu hơn, làm cho PC và Server chạy chậm hơn. Do đó, giải pháp chính là cài đặt một Server trung gian (WSUS Server) thực hiện cập nhật các bản vá lỗi từ Internet về, sau đó các máy PC trong mạng LAN kết nối đến Server này để cập nhật các bản vá lỗi. Sau khi triển khai giải pháp này sẽ đạt được các mục tiêu sau:
- Tất cả các máy tính Client trong mạng LAN đều được cập nhật các bản vá lỗi kịp thời, nâng cao khả năng bảo mật, an toàn cho máy tính người dùng (Client).
- Thời điểm cập nhật của các Client được đặt lịch phù hợp với hiệu suất hoạt động mạng LAN.
- Tiết kiệm được băng thông truy cập Internet: trước đây tất cả các Client đều phải truy cập Internet để cập nhật (mỗi lần cập nhật phải tải về từ vài chục đến vài trăm Mega byte dữ liệu), nhưng bây giờ chỉ có 1 Server kết nối Internet để cập nhật online còn các Client thực hiện cập nhật bên trong mạng LAN.

2.2 Giải pháp tổng thể phòng chống virus Bkav Endpoint Enterprise

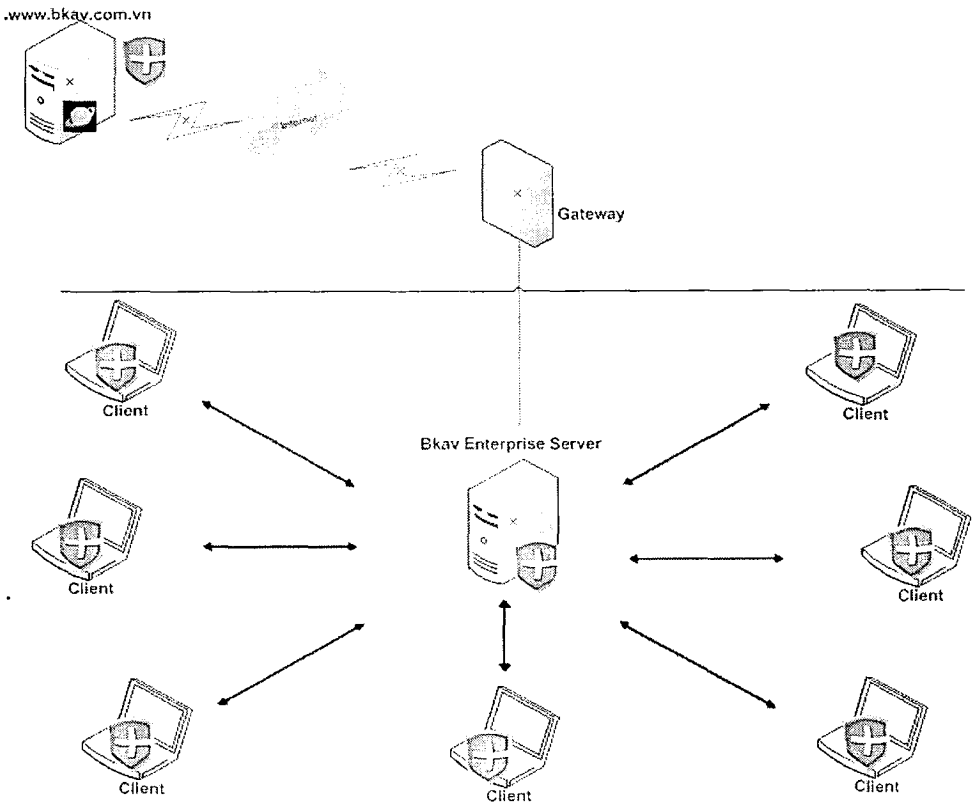
Bkạv Endpoint Enterprise là giải pháp tổng thể phòng chống virus, phiên bản dành cho các doanh nghiệp, cơ quan có hệ thống mạng nội bộ. Giải pháp này hoạt động theo mô hình quản lý tập trung trên Server, giúp cho người quản trị hệ thống mạng có thể nắm được tình hình virus trong toàn mạng, biết được máy nào trong mạng nhiễm virus, loại virus gì. Với Bkav Endpoint Enterprise, người quản trị có thể đặt lịch, ra lệnh cho các máy tính trong mạng đồng thời xử lý virus vào 1 thời điểm.

Bkav Endpoint Enterprise hoạt động theo mô hình quản lý tập trung trên Server:

- Chương trình diệt virus Bkav trên máy trạm sẽ tự động phát hiện và xử lý (Realtime Auto Protect) các virus, trojan ngay khi chúng xâm nhập. Xử lý các virus lây lan qua copy File, qua đĩa mềm, USB, CD..., các virus lây qua lỗ hổng của phần mềm cũng như các Trojan. Gửi báo cáo tình hình diệt virus về cho Server.
- Bkav Endpoint Enterprise Server giúp cho người quản trị hệ thống có

thể nắm được tình hình virus trong toàn mạng, biết được máy nào trong mạng nhiễm virus, loại virus gì. Người quản trị có thể đặt lịch, ra lệnh cho các máy tính trong mạng đồng thời xử lý virus vào 1 thời điểm. Cập nhật tự động, thống nhất các mẫu virus mới nhất xuống các máy trạm.

- Khi có virus mới xuất hiện và Bkav cập nhật mẫu virus mới nhất trên mạng thì Bkav Endpoint Enterprise sẽ tự động phát hiện và tải về. Sau đó Server sẽ tự động cập nhật xuống các máy trạm.



Hình: Mô hình quản lý tập trung với Bkav Endpoint Enterprise

Các chức năng của Bkav Endpoint Enterprise:

- BCOS (Bkav Community-based protection Online System) - Công nghệ Phòng vệ dựa trên cộng đồng
- Real-time Rootkit Detection – Hệ thống phòng thủ chống rootkit
- Virtual Keyboard - Bàn phím ảo
- Host Intrusion Prevention System - Hệ thống đánh chặn theo hành vi
- Share-full Protection - Bảo vệ các ổ đĩa chia sẻ trong mạng LAN
- Real-time Protection - Bảo vệ thời gian thực
- Safe Run – Thực thi an toàn

- Safe Facebook – Bảo vệ truy cập mạng xã hội
- Anti Ransombase - Chống các loại mã độc mã hóa dữ liệu
- Kiểm soát truy cập thiết bị lưu trữ di động (USB, ổ đĩa cứng di động,…)
- Anti Keylogger - Chống phần mềm gián điệp
- Safe Removing
- Site Advisor - Giám sát truy cập
- Diệt virus, worm, trojan, spybase, adbase, backdoor...
- Diệt rootkit
- Diệt virus siêu đa hình
- Sửa chữa file Exel
- Hiện file ẩn
- Tích hợp tường lửa cá nhân (Firewall)
- Chống bùng nổ (Proactive Protection)
- Quét virus theo hành vi (Heuristic Scan)
- Bảo vệ truy nhập web và diệt virus mạng (Web Protection)
- Tự phòng vệ trước sự tấn công của malbase (Self-Defense).
- Nhận diện mã độc dựa trên độ tín nhiệm (Reputation Based Detection)
- Kiểm soát truy cập web đen (Parental Control).
- Hỗ trợ các chế độ quét: Quét thông thường, Quick Scan - Quét nhanh, Smart Scan - Quét thông minh, Deep Scan - Quét sâu toàn bộ máy, Quét các file nén.
- Cập nhật mẫu nhận diện từng phần
- Quản lý tình hình virus trên các máy trạm tại Server
- Quản lý tập trung theo mô hình phân cấp nhiều máy chủ
- Quản lý, theo dõi trạng thái, phiên bản của Bkav Endpoint Enterprise Client trên các máy trạm
- Tự động cài đặt máy trạm thông qua máy chủ
- Thống kê và báo cáo tình hình virus trên toàn hệ thống
- Đặt lịch quét định kì thống nhất cho tất cả các máy trạm trong hệ thống
- Ra lệnh từ xa cho từng nhóm hay tất cả các máy trạm trong hệ thống quét virus vào một thời điểm bất kì
- Phân chia và quản lý máy trạm theo nhóm

- Hoạt động ở chế độ nền của hệ điều hành (Kernel Mode)

3. Giải pháp về cơ sở hạ tầng và thiết bị lưu trữ dữ liệu, lưu điện

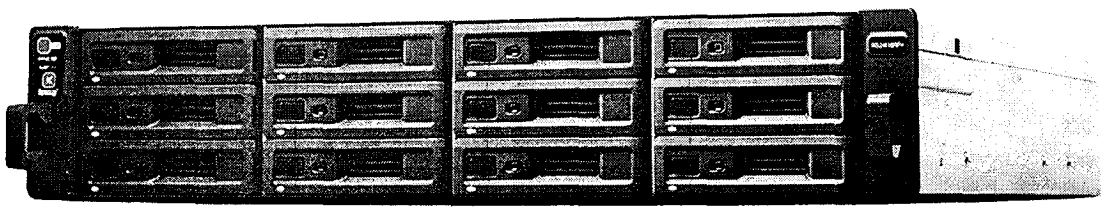
3.1. Thiết bị lưu trữ NAS Synology RackStation RS2418+

Thiết bị lưu trữ NAS (Network-attached storage) là bộ lưu trữ tệp chuyên dụng cho phép nhiều người dùng và các thiết bị khách không đồng nhất truy cập và lấy dữ liệu từ ổ đĩa tập trung thông qua mạng LAN (local area network).

Thiết bị lưu trữ NAS nằm trên mạng LAN dưới dạng một nút mạng độc lập và có địa chỉ IP riêng.

NAS Synology RackStation RS2418+ sử dụng CPU Intel Atom C3538 Quad-core 2.1 GHz, RAM DDR4 UDIMM có thể mở rộng tối đa 64GB (Thiết bị có 4 khe cắm Ram và có thể cắm tối đa 4 ram 16GB), ổ cứng có thể mở rộng lên đến 24 ổ cứng, hỗ trợ tối đa 288TB dung lượng (Thiết bị có sẵn 12 khay ổ cứng và có thể lắp thêm 12 khay ổ cứng để cắm được 24 ổ cứng).

NAS Synology RackStation RS2418+ thích hợp cho việc quản lý dữ liệu tập trung và là nơi sao lưu cho các server khác.



Thiết bị NAS Synology RackStation RS2418+ có 4 cổng Lan RJ-45 1GbE, đáp ứng nhu cầu tăng băng thông và load balancing cho thiết bị. Ngoài ra, RS2418+ tích hợp 1 khe PCIe 3.0 phục vụ cho nhu cầu mở rộng, có thể gắn thêm M.2 SSD SATA hay card NIC 10GbE tuỳ theo ý muốn để tăng cường tốc độ truy xuất dữ liệu của thiết bị.

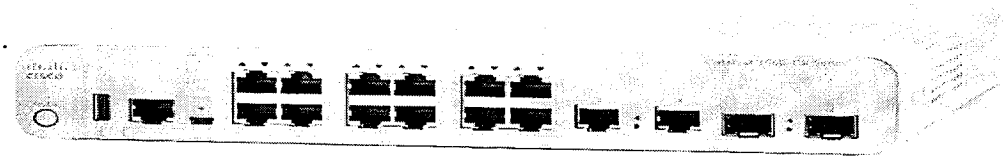
NAS Synology RackStation RS2418+ hỗ trợ tất cả các ứng dụng backup và đồng bộ của Synology, giúp bảo vệ dữ liệu trên hầu hết hệ điều hành, từ Windows, Linux, MacOS đến Android, iOS.

NAS Synology RackStation RS2418+ hỗ trợ Btrfs file system, sử dụng các công nghệ lưu trữ tiên tiến và snapshot để tối ưu hoá và ngăn chặn việc hỏng dữ liệu, giúp giảm chi phí bảo trì. Btrfs đảm bảo tính toàn vẹn dữ liệu mức độ cao, nó cũng cung cấp các công cụ khôi phục và bảo vệ dữ liệu hiệu quả, linh hoạt.

3.2.Thiết bị chuyển mạch Cisco Catalyst WS-C3560CX-8TC-S 8 Port Data IP Base:

Thiết bị chuyển mạch Switch Cisco WS-C3560CX-8TC-S là sản phẩm được sử dụng nhiều với các thiết bị chuyển mạch quản lý Multigigabit trong các

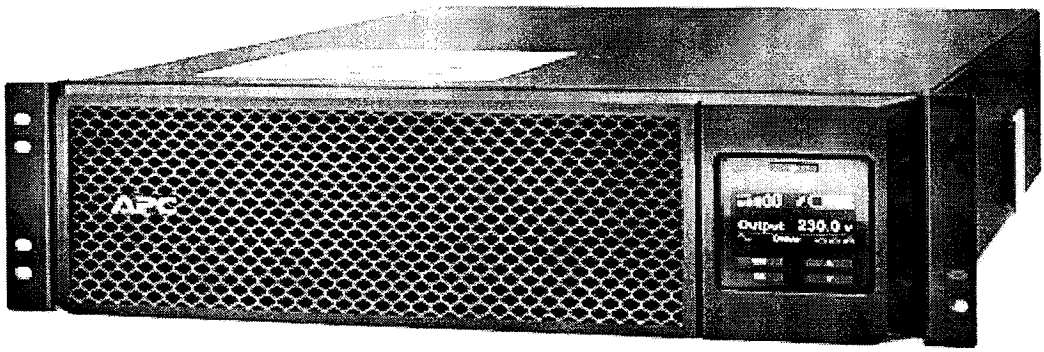
kết nối tốc độ cao, các kết nối Wifi Backhaul và kết nối PoE ở những không gian cao.



WS-C3560CX-8TC-S bao gồm 8 cổng Gigabit Ethernet, 2 cổng uplink RJ-45 Gigabit Ethernet, 2 x SFP.

3.3.Thiết bị lưu điện UPS APC Smart-UPS SRT5KRMXLI 5000VA 230V:

Bộ lưu điện UPS APC Smart-UPS SRT5KRMXLI 5000VA 230V là UPS online và là thiết bị tiếp nhận điện từ lưới điện và trực tiếp cung cấp điện cho các thiết bị sử dụng với điện áp đầu ra phù hợp với thiết bị sử dụng.



Các tính năng của Bộ lưu điện UPS APC Smart-UPS SRT5KRMXLI 5000VA 230V

- Thông báo lỗi pin: Cung cấp phân tích lỗi cảnh báo sớm về pin cho phép bảo trì kịp thời phòng ngừa

- Chế độ tiết kiệm: Chế độ hoạt động bằng cách vượt qua các thành phần điện không sử dụng trong điều kiện năng lượng tốt để đạt được hiệu quả hoạt động cao mà không phải hy sinh bảo vệ

- Chế độ màu xanh lục: Chế độ hoạt động đang chờ cấp bằng sáng chế bỏ qua các thành phần điện không sử dụng trong điều kiện nguồn điện tốt để đạt được hiệu quả hoạt động rất cao mà không phải hy sinh bất kỳ sự bảo vệ nào.

- Hiển thị đồ họa LCD: Văn bản và biểu đồ bắt chước hiển thị các chế độ hoạt động, thông số hệ thống và báo thức.

- Các tính năng & lợi ích trực tuyến Smart-UPS

+ Quản lý

Mạng có thể quản lý: Cung cấp quản lý nguồn điện từ xa của UPS qua mạng.

Kết nối nối tiếp: Cung cấp quản lý UPS thông qua cổng nối tiếp.

Chỉ báo trạng thái LED: Nhanh chóng hiểu trạng thái đơn vị và nguồn điện với các chỉ báo trực quan.

+ Khả dụng

Tự động bỏ qua nội bộ: Cung cấp nguồn điện cho các tải kết nối trong trường hợp quá tải hoặc lỗi nguồn UPS.

Sạc pin được bù nhiệt độ: Kéo dài tuổi thọ pin bằng cách điều chỉnh điện áp sạc theo nhiệt độ pin.

Thời gian chạy có thể mở rộng: Cho phép thêm thời gian chạy khi cần thiết.

Quản lý pin thông minh: Tối đa hóa hiệu suất pin, tuổi thọ và độ tin cậy thông qua tính năng sạc thông minh, chính xác.

Tự động khởi động lại tải sau khi tắt UPS: Tự động khởi động thiết bị được kết nối khi trả lại nguồn điện.

Pin có thể thay thế nóng: Đảm bảo năng lượng sạch, không bị gián đoạn cho thiết bị được bảo vệ trong khi pin đang được thay thế

+ Tính năng tiếp thị

Tiết kiệm thời gian với khả năng truy cập từ xa / mạng dễ dàng và thuận tiện

Chi phí vận hành và bảo dưỡng thấp với độ tin cậy đã được chứng minh và quản lý pin thông minh.

Quản lý pin thông minh, được tiên phong bởi APC, tối đa hóa hiệu suất pin và tuổi thọ thông qua sạc pin chính xác, thông minh. Tự động kiểm tra tự bảo đảm độ tin cậy của pin và cảnh báo khách hàng trước khi thay pin. Các mô-đun pin tiện lợi, dễ kết nối, có thể thay thế nóng cung cấp sự thay thế pin mà không cần tắt nguồn.

Tránh các vấn đề về điện năng tốn kém bằng cách giữ cho thiết bị và dữ liệu CNTT của bạn được bảo vệ và có sẵn.

Điều hòa công suất cấp mạng bảo vệ khỏi các chấn động và gây ra tiếng ồn gây hại. Kiến trúc chuyển đổi kép cung cấp quy định điện áp chặt chẽ, điều chỉnh tần số và thời gian truyền bằng không cho pin trong các sự kiện nguồn.

Yên tâm rằng đi kèm với thiết bị tương thích đầy đủ và độ tin cậy của một nhà lãnh đạo

+ Khả năng phục vụ

Báo thức âm thanh: Cung cấp thông báo về việc thay đổi điều kiện nguồn điện và nguồn điện UPS

Thông báo pin đã ngắt kết nối: Cảnh báo khi pin không có sẵn để cung cấp nguồn dự phòng.

Thông báo thất bại dự phòng:Cung cấp phân tích lỗi cảnh báo sớm đảm bảo thay thế thành phần chủ động.

Tự kiểm tra tự động: Tự kiểm tra pin định kỳ đảm bảo phát hiện sớm pin cần được thay thế.

Pin người dùng có thể thay thế: Tăng tính khả dụng bằng cách cho phép người dùng được đào tạo thực hiện nâng cấp và thay thế pin giảm Thời gian trung bình để sửa chữa (MTTR)

+ Khả năng thích ứng

Phần mềm nâng cấp Flash: Cài đặt bản phát hành bảo trì của phần mềm từ xa bằng FTP.

Pin ngoài cắm và chạy: Đảm bảo năng lượng sạch, liên tục cho các tải khi thêm thời gian chạy bổ sung cho UPS.

Rack / Tower convertible: Bảo vệ đầu tư ban đầu trong UPS khi di chuyển từ tháp đến môi trường gắn kết.

+ Sự bảo vệ

Bộ ngắt mạch có thể reset: Dễ dàng phục hồi từ quá tải; không cần phải thay thế cầu chì.

Tần số và điều chỉnh điện áp: Cung cấp khả năng ứng dụng cao hơn bằng cách điều chỉnh tần số và điều kiện điện áp kém mà không cần sử dụng pin.

Cung cấp nguồn pin tạm thời khi tắt nguồn điện.

Cơ quan an toàn đã được phê duyệt:Đảm bảo sản phẩm đã được kiểm tra và phê duyệt để hoạt động an toàn với thiết bị của nhà cung cấp dịch vụ được kết nối và trong môi trường được chỉ định.

Hiệu chỉnh hệ số công suất đầu vào: Giảm thiểu chi phí lắp đặt bằng cách cho phép sử dụng máy phát và cáp nhỏ hơn.

Máy phát điện tương thích: Đảm bảo năng lượng sạch, không bị gián đoạn cho thiết bị được bảo vệ khi sử dụng nguồn máy phát điện.

Điều hòa điện: Bảo vệ các tải được kết nối từ các vụ nổ, đột biến, sét và các nhiễu điện khác.

IV. TIẾN ĐỘ DỰ KIẾN THỰC HIỆN:

STT	Nội dung	Thời gian	Ghi chú
1	Xây dựng các bước tiến hành Gói thầu được áp dụng hình thức Chào hàng cạnh tranh theo quy trình rút gọn cho các gói thầu	Tháng 11/2018 - Đầu tháng 12/2018	
2	Tiếp nhận và bàn giao, nghiệm thu thiết bị, phần mềm	Tháng 12/2018	

V. TỔ CHỨC THỰC HIỆN

- Giao phòng Kế hoạch – tài chính làm đầu mối tham mưu, chỉ đạo việc triển khai thực hiện đảm bảo an toàn, an ninh thông tin cho cơ quan Sở Y tế và hệ thống sever máy chủ dữ liệu Database house .

- Văn phòng Sở Y tế: Phối hợp với phòng Kế hoạch trong công tác quản lý, lắp đặt, bảo vệ tài sản hệ thống đảm bảo an toàn, an ninh thông tin được triển khai tại Sở Y tế.

- Các phòng chức năng trong Sở Y tế có trách nhiệm phối hợp, tuân thủ quy chế sử dụng thiết bị, hệ thống mạng của Sở Y tế.

VI. KINH PHÍ THỰC HIỆN

1. Kinh phí: 769.771.000 đồng *(Bảy trăm sáu mươi chín triệu, bảy trăm bảy mươi mốt ngàn đồng chẵn).*

2. Nguồn kinh phí: Được bố trí tại Mục 3. Mua sắm trang thiết bị thực hiện đồng bộ công nghệ thông tin ngành y tế, phần mềm khám chữa bệnh tại trạm y tế xã, phần mềm hồ sơ sức khoẻ cá nhân.. 1.900 triệu đồng (trong mục IV. Kinh phí hỗ trợ mua sắm trang thiết bị y tế phục vụ công tác khám chữa bệnh các đơn vị quản lý ngành, phụ lục 19 Quyết định số 3232/QĐ-UBND ngày 12/12/2017)

Nơi nhận:
- Phòng KHTC, VP SYT ;
- Giám đốc, các PGĐ Sở Y tế ;
- Lưu: VT, KHTC.

GIÁM ĐỐC

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ Y TẾ
THÁI BÌNH

Phạm Văn Dịu

DỰ TOÁN KINH PHÍ

Stt	Danh mục hàng hóa	Đơn vị tính	Số lượng	Xuất xứ	Đơn giá trước thuế	Thành tiền trước thuế	Thuế VAT	Thành tiền sau thuế	Ghi chú
I	**Gói 1: Thiết bị an ninh mạng**							**377.500.000**	
1	Thiết bị tường lửa Bkav IPS Firewall SMB license 1 year	Bộ	1	Việt Nam	80.000.000	80.000.000	8.000.000	88.000.000	
2	Thiết bị phát hiện và cảnh báo tấn công mạng Bkav Network Inspector SMB license 1 year	Bộ	1	Việt Nam	150.000.000	150.000.000	15.000.000	165.000.000	
3	Thiết bị quản lý chính sách an ninh thông tin Bkav Total NAC SMB license 1 year	Bộ	1	Việt Nam	95.000.000	95.000.000	9.500.000	104.500.000	
4	Dịch vụ thiết lập hệ thống Firewall	Gói	1		20.000.000	20.000.000	0	20.000.000	
II	**Gói 2: Phần mềm**							**151.800.000**	
1	Bản quyền HĐH máy chủ Window Server cho 02 máy chủ	License	2	Microsoft	25.000.000	50.000.000	5.000.000	55.000.000	(19/11/2018 USD: 22,721; WSV Standard[2]: 972USD)
2	Dịch vụ thiết lập hệ thống WSUS		1	Microsoft	20.000.000	20.000.000	2.000.000	22.000.000	
3	WinSvrCAL 2019 SNGL OLP NL DvcCAL	License	50	Microsoft	760.000	38.000.000	3.800.000	41.800.000	(19/11/2018 USD: 22,721;37USD)
4	Bản quyền phần mềm phòng chống phần mềm độc hại, mã độc Bkav Endpoint AI license 1 year	License	50	Việt Nam	600.000	30.000.000	3.000.000	33.000.000	

Stt	Danh mục hàng hóa	Đơn vị tính	Số lượng	Xuất xứ	Đơn giá trước thuế	Thành tiền trước thuế	Thuế VAT	Thành tiền sau thuế	Ghi chú
III	**Gói 3: Hạ tầng và thiết bị lưu trữ**							**240.471.000**	
1	Thiết bị lưu trữ NAS Synology RackStation RS2418+	Bộ	1	Taiwan	82.290.000	82.290.000	8.229.000	90.519.000	Thiết bị lưu trữ chính
2	Thiết bị chuyển mạch Cisco Catalyst WS-C3560CX-8TC-S 8 Port Data IP Base	Bộ	1	China	57.450.000	57.450.000	5.745.000	63.195.000	Switch layer 3 8 cổng (Dùng chung cho hệ thống firewall và lưu trữ dữ liệu
3	Thiết bị Lưu Điện UPS APC Smart-UPS SRT5KRMXLI 5000VA 230V	Bộ	1	China	60.870.000	60.870.000	6.087.000	66.957.000	UPS Online 5KVA (Dùng chung cho Hệ thống máy chủ và lưu trữ)
4	Dịch vụ thiết lập hệ thống lưu trữ NAS	Gói	1		18.000.000	18.000.000	1.800.000	19.800.000	
Tổng cộng								**769.771.000**	