ĐẠI HỌC Y DƯỢC TPHCM
**BỆNH VIỆN ĐẠI HỌC Y DƯỢC**

Số: 1661.../BVĐHYD-CNTT

V/v mời chào giá

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

*Thành phố Hồ Chí Minh, ngày 09 tháng 04 năm 2026.*

Kính gửi: Quý nhà cung cấp

Bệnh viện Đại học Y Dược Thành phố Hồ Chí Minh kính mời các đơn vị có đủ năng lực và kinh nghiệm Cung cấp dịch vụ phòng chống tấn công DDoS (AntiDDoS) trên đường truyền FTTH theo yêu cầu dưới đây vui lòng gửi hồ sơ chào giá cho Bệnh viện theo nội dung cụ thể như sau:

1. Tên dự toán: Cung cấp dịch vụ phòng chống tấn công DDoS (AntiDDoS) trên đường truyền FTTH

2. Phạm vi cung cấp và yêu cầu kỹ thuật: chi tiết theo phụ lục đính kèm.

3. Thời gian cung cấp hàng hóa, dịch vụ: 36 tháng kể từ ngày hợp đồng có hiệu lực.

4. Loại hợp đồng: trọn gói

5. Địa điểm thực hiện: Bệnh viện Đại học Y Dược Thành phố Hồ Chí Minh - 201 Nguyễn Chí Thanh, Phường Chợ Lớn, Thành phố Hồ Chí Minh

6. Hiệu lực của hồ sơ chào giá: tối thiểu 06 tháng.

7. Yêu cầu về giá chào: giá chào đã bao gồm các loại thuế, phí, lệ phí theo luật định, chi phí vận chuyển, giao hàng và các yêu cầu khác của chủ đầu tư.

8. Thời gian nhận hồ sơ chào giá: trước 16 giờ, ngày 20./04./2026.

9. Quy định về tiếp nhận hồ sơ chào giá:

- Gửi báo giá online qua website: https://bvdaihoc.com.vn/Home/ViewList/31;
- Gửi bản giấy có ký tên, đóng dấu về địa chỉ sau đây: Phòng Công nghệ thông tin, Tầng 4, Khu A, Bệnh viện Đại học Y Dược Thành phố Hồ Chí Minh – Cơ sở 1, số 215 Hồng Bàng, Phường Chợ Lớn, Thành phố Hồ Chí Minh

Người liên hệ: Mai Thị Thủy Số điện thoại: 028.39525391

10. Yêu cầu khác:

Hồ sơ chào giá của nhà thầu bao gồm các tài liệu sau:

+ Thư chào giá, bảng báo giá của nhà thầu (có ký tên, đóng dấu);

+ Hợp đồng trúng thầu còn hiệu lực đối với các mặt hàng đã trúng thầu tại các cơ sở y tế (nếu có);

+ Tài liệu kỹ thuật của dịch vụ

Trân trọng./.

***Nơi nhận:***
- Như trên;
- Giám đốc (để báo cáo);
- Đơn vị Quản lý Đấu thầu (để đăng tin);
- Lưu: VT, CNTT (J23-137-mtthuy) (03).

**TUQ. GIÁM ĐỐC**
**TRƯỞNG PHÒNG CÔNG NGHỆ THÔNG TIN**

BỆNH VIỆN ĐẠI HỌC Y DƯỢC TP. HỒ CHÍ MINH

**Trần Văn Đức**

BM:CVĐT.01(1)

# PHỤ LỤC. PHẠM VI CUNG CẤP VÀ YÊU CẦU KỸ THUẬT

*(Đính kèm Công văn số 1661../BVĐHYD-CNTT ngày 09. tháng 04 năm 2026)*

## A. Phạm vi cung cấp

| STT | Tên danh mục | Đơn vị tính | Số lượng |
|---|---|---|---|
| 1 | Đường truyền Internet FTTH | Kênh | 01 |
| 2 | Dịch vụ phòng chống tấn công DDoS (AntiDDoS) | Gói | 01 |

## B. Yêu cầu kỹ thuật

| STT | Nội dung | Mô tả |
|---|---|---|
| **I** | **Đường truyền Internet FTTH** | |
| 1 | Băng thông/ tốc độ kênh truyền | - Băng thông trong nước ≥ 1000 Mbps<br>- Băng thông quốc tế ≥ 80 Mbps |
| 2 | IP tĩnh | - Số lượng IP tĩnh: ≥ 8 IP<br>- IP tĩnh (IP public) không nằm trong danh sách đen (Blacklist) của các tổ chức quản lý dịch vụ trên thế giới và được bên mời thầu kiểm tra qua công cụ MXToolBox.com |
| 3 | Chất lượng dịch vụ truyền dẫn | - Nhà thầu phải vẽ sơ đồ tuyến cáp quang thực tế theo 2 hướng khác nhau cho các đường truyền Internet; Cung cấp thông tin dữ liệu sơ đồ tuyến đối với các tuyến cáp quang, chú thích chủng loại cáp trên toàn tuyến.<br>- Nhà thầu phải độc lập về hạ tầng khi triển khai, không phải mua/thuê/mượn hạ tầng của đơn vị khác.<br>- Yêu cầu dịch vụ truyền dẫn như sau:<br>o Loại kết nối: Cáp quang.<br>o Tỷ lệ gây lỗi (Error Second Ratio -ESR) là tỉ lệ phần trăm của số giây mà lỗi được phát hiện trên tổng số giây đo được với khoảng cách truyền dẫn tiêu chuẩn là 27.500 km: Tỷ lệ gây lỗi (ESR) ≤ 1.<br>o Tỷ lệ mất gói là tỷ lệ giữa tổng số gói tin bị mất trên tổng số gói tin đã gửi trong quá trình truyền dữ liệu giữa hai thiết bị đầu cuối đặt tại đơn vị sử dụng dịch vụ: ping 1.000 ≤ 0,1%.<br>o Biến thiên độ trễ là độ lệch của độ trễ khi truyền dữ liệu thực tế so với độ trễ cam kết đối với đường internet. Đơn vị tính ms (Sử dụng công cụ Speedtest đo): Trong nước: ≤ 10 ms. Quốc tế: ≤ 50 ms.<br>- Yêu cầu thông tin liên hệ và xử lý sự cố<br>o Nhà cung cấp dịch vụ có cung cấp hotline xử lý sự cố (miễn phí). |

| STT | Nội dung | Mô tả |
|---|---|---|
| | | o Nhà cung cấp dịch vụ có cung cấp số điện thoại liên hệ với bộ phận kinh doanh. |
| 4 | Yêu cầu về hệ thống giám sát kênh truyền | - Có cung cấp hệ thống giám sát kênh truyền, có thể theo dõi theo thời gian thực và tra cứu dữ liệu lịch sử băng thông trong nước, băng thông quốc tế của từng đường truyền. |
| 5 | Năng lực nhà cung cấp dịch vụ | - Nhà cung cấp dịch vụ có các đường kết nối Internet đi quốc tế theo nhiều hướng khác nhau như đường biển, đường bộ và vệ tinh; Cung cấp thông tin sở hữu tối thiểu 2 tuyến cáp đất liền và 3 tuyến cáp quang biển đi quốc tế.<br>- Nhà cung cấp dịch vụ có kết nối trực tiếp đến Trạm trung chuyển Internet Quốc gia (VNIX) với tổng băng thông ≥ 50Gbps.<br>- Có phương án kỹ thuật (Online và onsite) đảm bảo chất lượng kết nối Internet đến người dùng đầu cuối tính từ cổng kết nối Internet đến tận người sử dụng.<br>- Có khả năng hỗ trợ ứng cứu traffic quốc tế thông qua đường IPTransit trong nước qua các nhà mạng tại Việt Nam |
| **II** | **Dịch vụ phòng chống tấn công DDoS (AntiDDoS)** | |
| 1 | Yêu cầu chung | - Giải pháp cung cấp nằm trong nhóm các giải pháp dẫn đầu về chống tấn công DDoS (DDoS Mitigation Solutions) của một trong các bảng xếp hạng giải pháp công nghệ Gartner, Forrester, IDC trong khoảng thời gian từ 2019 đến nay. |
| | | - Giải pháp có khả năng phát hiện, cảnh báo và phản ứng/ chặn được các cuộc tấn công DDoS, chi tiết yêu cầu như sau:<br>+ Tấn công Layer 3:<br>Location-based IP Addresses, Spoofed/ Non- spoofed DoS AttacksTấn công Layer 4: TCP (SYN, etc), ICMP, UDP Floods<br>+ Tấn công hỗn hợp:<br>Đối với các dịch vụ tấn công có kết hợp nhiều yếu tố: Đơn vị cung cấp dịch vụ hỗ trợ cung cấp các thông tin liên quan đến lưu lượng mạng và phân tích gói tin của cuộc tấn công |
| | | - Giải pháp có đầy đủ các nhóm tính năng:<br>- Phân tích, thống kê lưu lượng<br>- Cảnh báo cuộc tấn công<br>- Phản ứng trước cuộc tấn công từ chối dịch vụ |
| | | Giải pháp hỗ trợ công nghệ phân tích lưu lượng mạng (Flow) và phân tích sâu bên trong gói tin mạng (Deep packet inspection) |

| STT | Nội dung | Mô tả |
|---|---|---|
| | | Có khả năng phòng chống các loại tấn công DDoS ngập lụt băng thông (Volumetric) lên đến 100Gbps |
| | | Có khả năng tích hợp giám sát đường truyền và không cần lắp đặt thêm thiết bị. |
| | | Giải pháp/dịch vụ cung cấp đáp ứng tiêu chuẩn quản lý an toàn thông tin ISO 27001:2013 |
| | | Thời gian triển khai dịch vụ: <= 2 ngày |
| 2 | Yêu cầu về tính sẵn sàng và độ khả dụng của dịch vụ | - Có khả năng phát hiện các cuộc tấn công từ các nguồn IP nước ngoài, của các Nhà cung cấp khác và của các nguồn liên tỉnh. |
| | | - Đảm bảo băng thông sạch trả về với dịch vụ 24x7x365 |
| | | - Đảm bảo độ khả dụng - Uptime của dịch vụ DDoS ≥ 99,5% |
| | | - Đảm bảo tỉ lệ mất gói tin khi bị tấn công là ≤ 0.3% |
| 3 | Yêu cầu về tính năng của giải pháp | |
| 3.1 | Khả năng phát hiện các cuộc tấn công | Cho phép cấu hình chung để phát hiện các cuộc tấn công vào các host |
| | | Cho phép cấu hình giám sát trên đối tượng (Objects) |
| | | Có khả năng giám sát lưu lượng mạng (Traffics) IPv4 và IPv6, cho phép giám sát theo đối tượng, dịch vụ; Phát hiện dấu hiệu tấn công nhắm vào thiết bị (Host) hỗ trợ phản ứng nhanh để tự động giảm thiểu nguy cơ cho hệ thống. |
| | | Cho phép thiết lập cảnh báo với các Host theo thông số: Total traffic; DNS, DNS Amplification; ICMP; IP Fragment; NTP Amplification; SNMP Amplification; SSDP Amplification; TCP: ACK, Null, RST, SYN; UDP |
| | | Cho phép cấu hình giám sát lưu lượng mạng vượt ngưỡng cho phép đối với đối tượng và dịch vụ. Khi có cảnh báo, hệ thống có khả năng thu thập thông tin liên quan trên toàn bộ hệ thống mạng, tổng hợp các giao thức có liên quan và hiển thị nguồn tấn công ASN |
| 3.2 | Khả năng cảnh báo các cuộc tấn công | Cho phép cấu hình cảnh báo các sự kiện bất thường |
| | | Cho phép cảnh báo hoạt động dưới dạng đồ thị, bảng tương quan sự kiện, hiển thị các thông tin liên quan: Mức độ nghiêm trọng, tham số, ảnh hưởng, tỉ lệ ảnh hưởng |
| | | Cho phép cấu hình cảnh báo vượt ngưỡng theo dịch vụ và theo lưu lượng |
| | | Cho phép cảnh báo tấn công DDoS, cung cấp các thông tin có liên quan đến cuộc tấn công: Lưu lượng, dấu hiệu một cuộc tấn công, chú thích cảnh báo, phương án giảm nhẹ ban đầu |

| STT | Nội dung | Mô tả |
|---|---|---|
| | | Hiển thị bảng tổng hợp thông tin liên quan đến cuộc tấn công với các tham số: Mức độ nghiêm trọng (Serverity level), mức độ ảnh hưởng đến băng thông (Max impact of alert traffic), hướng tấn công (Direction), tham số của cuộc tấn công (Misusc types), đối tượng (Object) |
| 3.3 | Khả năng phản ứng khi có tấn công từ chối dịch vụ | Giải pháp hỗ trợ lọc chặn các cuộc tấn công theo thời gian thực, kết hợp với các tính năng tự phát hiện tấn công, cảnh báo |
| | | Giải pháp có khả năng phản ứng nhanh trước cuộc tấn công DDoS theo đa dạng các bộ countermeasure |
| | | Giải pháp cho phép cấu hình Blacklist (Bỏ qua) đối với các sự kiện bất thường |
| | | Giải pháp cho phép cấu hình các kịch bản giảm thiểu thiệt hại tấn công |
| 3.4 | Báo cáo thống kê | Hỗ trợ hiển thị dữ liệu báo cáo dưới các hình thức biểu đồ khác nhau: Stacked, bar, pie, line |
| | | Cho phép tùy chỉnh các thành phần của báo cáo theo các nhóm: Ứng dụng (applications), đối tượng (managed objects), dịch vụ (services) |
| 4 | Yêu cầu về SLA và báo cáo | Khi phát hiện các dấu hiệu cuộc tấn công DDoS vào hệ thống/ dịch vụ của khách hàng, hệ thống tự động gửi cảnh báo ngay tức thời qua Email cho đầu mối của khách hàng và phối hợp khách hàng để xử lý tiếp theo |
| | | Thời gian tối đa xử lý xong cuộc tấn công DDoS ≤ 1 giờ kể từ khi xảy ra |
| | | Việc xử lý chống tấn công phải trong suốt với khách hàng, không gây bất kỳ gián đoạn hay ảnh hưởng nào khác (ngoài ảnh hưởng do cuộc tấn công DDoS trực tiếp gây ra) đến tất cả các ứng dụng/ dịch vụ đang chạy trên chính đường truyền Internet của ISP cung cấp. |
| | | Cung cấp trang portal riêng cho khách hàng để theo dõi các thông tin sau:<br>- Thông tin về cuộc tấn công: Hình thức tấn công, thời điểm phát hiện, mức độ nghiêm trọng, thông tin khuyến nghị<br>- Thông tin chi tiết với các yếu tố có liên quan đến cuộc tấn công:<br>+ Phân loại hình thức tấn công, xác định cấp độ cuộc tấn công<br>+ IP tham gia / mục tiêu của cuộc tấn công<br>+ Bảng phân tích lưu lượng mạng tham gia vào cuộc tấn công<br>+ Các giao thức, port có liên quan đến quá trình tấn công |
| | | Nhà cung cấp hỗ trợ gửi báo cáo định kỳ, tối thiểu bao gồm các thông tin sau nếu chủ đầu tư yêu cầu:<br>+ Báo cáo Top lưu lượng sử dụng trên hệ thống |

| STT | Nội dung | Mô tả |
|---|---|---|
| | | + Báo cáo thống kê các cuộc tấn công<br>+ Báo cáo tình trạng tuân thủ sử dụng dịch vụ (SLAs) |
| | | Nhà cung cấp cung cấp giao diện đầy đủ liên quan đến DDoS quản trị hệ thống ở chế độ Audit/ Monitor để nhân viên quản trị của khách hàng có thể truy cập bất cứ thời gian nào thông qua Internet |
| | | Nhà cung cấp dịch vụ phòng chống tấn công DDoS (AntiDDoS) đồng thời là nhà cung cấp đường truyền Internet Leased line (ILL) |
| **III** | **Các yêu cầu khác** | |
| 1 | Kế hoạch triển khai | Có kế hoạch chi tiết triển khai lắp đặt kênh Cung cấp dịch vụ trong vòng 07 ngày kể từ khi hợp đồng có hiệu lực |
| 2 | Cam kết thời gian tiếp nhận, xử lý sự cố | Thời gian xác nhận sự cố: ≤ 15 phút, thời gian onsite ≤ 30 phút Thời gian xử lý sự cố: ≤ 4h . Thời gian tiếp nhận sự cố: 24/7/365. Có quy trình tiếp nhận và xử lý sự cố. Phương thức tiếp nhận thông tin: Tổng đài hỗ trợ kỹ thuật 24/7; Hotline kỹ thuật; Email |
| 3 | Quy định về kiểm tra, nghiệm thu sản phẩm: | Về quy trình kiểm tra, nghiệm thu sản phẩm, trình tự giao nộp sản phẩm… để phục vụ công tác thanh, quyết toán hợp đồng được thực hiện trên cơ sở quy định của pháp luật hiện hành có liên quan và nội dung công việc của gói thầu.<br>Trước khi bàn giao sản phẩm Nhà thầu phối hợp với Chủ đầu tư kiểm tra, nghiệm thu mọi sản phẩm có liên quan |
| 4 | Nhân sự chủ chốt | |
| 4.1 | Cán bộ phụ trách chung dự án | ≥ 1 nhân sự tốt nghiệp đại học chuyên ngành bảo mật thông tin<br>* Có chứng chỉ CCNP và CHFI<br>** Yêu cầu về kinh nghiệm và tài liệu kèm theo:*<br>- Tối thiểu 5 năm hoặc đã thực hiện tối thiểu 5 hợp đồng tương tự<br>- Tổng số năm kinh nghiệm (căn cứ theo từ thời điểm nhân sự bắt đầu thực hiện công việc tương tự đó đến thời điểm đóng thầu); Kinh nghiệm trong các công việc tương tự |
| 4.2 | Cán bộ triển khai đường truyền | ≥ 1 nhân sự tốt nghiệp đại học chuyên ngành điện tử viễn thông<br>* Có chứng chỉ CCNP<br>** Yêu cầu về kinh nghiệm và tài liệu kèm theo:*<br>- Tối thiểu 3 năm hoặc đã thực hiện tối thiểu 3 hợp đồng tương tự |

| STT | Nội dung | Mô tả |
|---|---|---|
| | | - Tổng số năm kinh nghiệm (căn cứ theo từ thời điểm nhân sự bắt đầu thực hiện công việc tương tự đó đến thời điểm đóng thầu); Kinh nghiệm trong các công việc tương tự |
| 4.3 | Cán bộ triển khai an toàn thông tin | ≥ 1 nhân sự tốt nghiệp đại học chuyên ngành công nghệ thông tin<br>* Có chứng chỉ CEH<br>** Yêu cầu về kinh nghiệm và tài liệu kèm theo:*<br>- Tối thiểu 3 năm hoặc đã thực hiện tối thiểu 3 hợp đồng tương tự<br>- Tổng số năm kinh nghiệm (căn cứ theo từ thời điểm nhân sự bắt đầu thực hiện công việc tương tự đó đến thời điểm đóng thầu); Kinh nghiệm trong các công việc tương tự |